Tema 2. El Sistema Operativo. Seguridad.

1. EL SOFTWARE Y EL SISTEMA OPERATIVO

    1.1. Concepto y clasificación del Software.

    1.2. El Sistema Operativo. Funciones. Estructura. Tipos.

    1.3. El concepto de propiedad. Ley de propiedad intelectual. Materiales libres y privativos en la web

    1.4. Formas de distribución del software. Licencias de software

    1.5. Windows7

2. SEGURIDAD INFORMÁTICA

    2.1. Principios de la seguridad informática.

    2.2. Seguridad activa y pasiva. Seguridad física y lógica. Seguridad de contraseñas.

    2.3. Actualización de sistemas operativos y aplicaciones.

    2.4. Copias de seguridad.

    2.5. Software malicioso, herramientas antimalware y antivirus, protección y desinfección.

    2.6. Cortafuegos. Seguridad en redes inalámbricas. Ciberseguridad.

    2.7. Criptografía. Certificados digitales. Agencia española de Protección de datos.

    2.8. Seguridad en redes sociales, acoso y convivencia en la red.

1. EL SOFTWARE Y EL SISTEMA OPERATIVO

1.1. CONCEPTO Y CLASIFICACIÓN DEL SOFTWARE.

El hardware no puede funcionar sin un programa o software que lo controle y le indique las instrucciones a ejecutar. Los programas se clasifican en base a su utilidad en cuatro categorías.

A. SOFTWARE DE BASE: Sistemas operativos y controladores

El sistema operativo es el programa o conjunto de programas que hacen posible el funcionamiento del ordenador. Sus funciones principales son:

- Arranca el sistema
- Configura los periféricos
- Mantiene el sistema
- Permite el funcionamiento de las aplicaciones

Ofrece al programador una abstracción de alto nivel y administra los recursos hardware.

Se diferencian dos tipos principales de sistemas operativos: modo grafico (WINDOWS, Macintosh... es la tendencia actual) y modo texto (MS-DOS, Linux, UNIX).

Los controladores (drivers) son programas que sirven para configurar los periféricos y asegurar su correcto funcionamiento.

Guadalinex es una distribución de Linux que la Junta de Andalucía ha creado como sistema operativo de código abierto (software libre). Guadalinex es un sistema operativo multiusuario, multitarea y multiplataforma basado en Ubuntu, una distribución de Linux basada en Debian.

B. SOFTWARE DE APLICACIÓN

Son programas de propósito específico, como los paquetes integrados (suites ofimáticas como Microsoft Office o Star Office), juegos, software de diagnóstico, herramientas (Norton Ghost), programas de contabilidad como ContaPlus, de estadística (Statgraphic)s, edición de imagen digital (Photoshop, The Gimp), utilidades (PartitionMagic, antivirus...)…

C. SOFTWARE DE DESARROLLO

Lo usan los programadores para desarrollar otros programas nuevos. Son los compiladores, intérpretes y entornos de desarrollo. Ejemplos: Visual Basic, Pascal, TurboC, VisualC++, VisualJava, PowerBuilder,...

D. SOFTWARE DE COMUNICACIONES

Son programas para comunicación por Internet, como navegadores web (Google Chrome, Mozilla Firefox, Opera, Safari…), clientes de correo electrónico (Eudora, OutlookExpress, Evolution, Outlook) , protocolos de Internet (TCP/IP), chats IRC, clientes FTP (WS-FTP), Messenger, software de videoconferencias (como Skipe, Hangouts, Line…)…

1.2. El Sistema Operativo y sus funciones.

El Sistema Operativo. Concepto

El sistema operativo es el programa principal del ordenador, el primero que debemos instalar para que todo funcione, junto con los drivers o controladores de dispositivos. Sin el sistema operativo nada funcionaría.

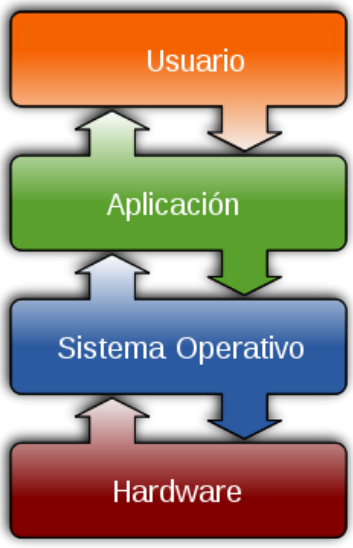
Software de base = Sistema Operativo + Drivers

Definición 1: El **sistema operativo** es un conjunto de programas que **gestionan los recursos de hardware (procesador, memoria, periféricos) y provee servicios a los programas de aplicación** .

Definición 2: Un **sistema operativo** es un programa que actúa como **intermediario entre el usuario y el hardware de un ordenador y su propósito es proporcionar un entorno en el cual el usuario pueda ejecutar programas.** El objetivo principal de un Sistema Operativo es lograr que el sistema se utilice de manera cómoda y que el hardware del computador se emplee de manera eficiente.

El Sistema Operativo es una parte importante de cualquier sistema de computación. Un sistema de computación puede dividirse en cuatro componentes:

- Usuarios
- Los programas de aplicación
- Sistema Operativo
- Hardware



Funciones del Sistema Operativo.

Las funciones principales de un Sistema Operativo podríamos resumirlas en las siguientes:

- **Administración del procesador:** el sistema operativo administra la distribución del procesador entre los distintos programas en ejecución (procesos).
- **Gestión de la memoria:** el sistema operativo se encarga de gestionar el espacio de memoria RAM asignado para cada programa y para cada usuario.
- **Gestión de entradas/salidas:** el sistema operativo permite unificar y controlar el acceso de los programas a los periféricos a través de los *drivers* o controladores de dispositivo.

- **Gestión de las aplicaciones (instalación, ejecución y desinstalación):** el sistema operativo se encarga de que las aplicaciones se ejecuten sin problemas asignándoles los recursos que éstas necesitan para funcionar. Esto significa que si una aplicación no responde correctamente, el sistema puede finalizar ese proceso.

- **Administración de autorizaciones (usuarios):** el sistema operativo se encarga de la seguridad en relación con la ejecución de programas garantizando que los recursos sean utilizados sólo por programas y usuarios que posean las autorizaciones correspondientes.

- **Gestión de archivos:** el sistema operativo gestiona la lectura y escritura en el sistema de archivos, y las autorizaciones de acceso a archivos de aplicaciones y usuarios.

- **Gestión de la información:** el sistema operativo proporciona cierta cantidad de indicadores que pueden utilizarse para diagnosticar el funcionamiento correcto del equipo.

- **Gestión de red:** el sistema operativo permite utilizar los recursos de otras máquinas, así como compartir carpetas, archivos y periféricos locales, y conectar el sistema a internet.

- **Gestión de errores:** el sistema operativo garantiza que el sistema se recupere tras un error y de un mensaje de error al usuario.

- **Gestión de la Interfaz Grafia de usuario (GUI)**

Estructura de un Sistema Operativo.

Los elementos principales de un sistema operativo son:

- **NÚCLEO (Kernel)** Es el módulo de más bajo nivel de un sistema operativo, pues descansa directamente sobre el hardware de la computadora. En general, el núcleo se encarga de controlar el resto de los módulos y sincronizar su ejecución. Entre las tareas que desempeña se incluyen:

  a. El manejo de las interrupciones que llegan de los periféricos (ratón, teclado…)

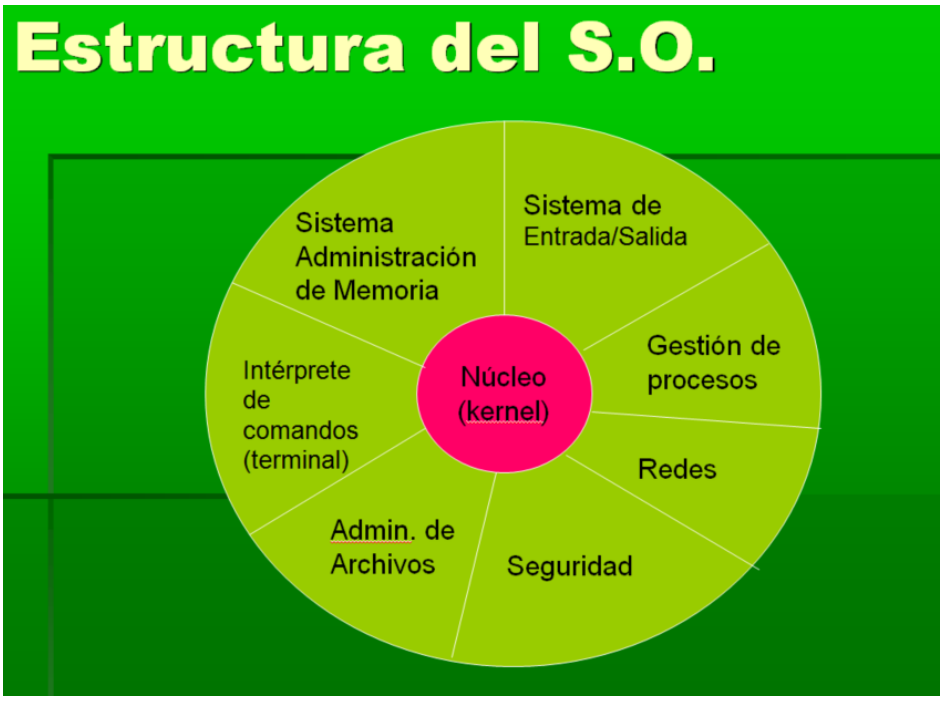
  b. la asignación de trabajo al procesador: . El núcleo contiene un submódulo denominado "**planificador**", el cual se encarga de asignar tiempo del procesador a los programas, de acuerdo a una cierta política de planificación que varía de un sistema operativo a otro. Normalmente se utiliza una jerarquía de prioridades que determinan cómo se asignará el tiempo del CPU a cada programa. Una política de planificación muy común en los sistemas de multiprogramación y multiproceso son las técnicas de "time slicing" (fracción de tiempo). Se asigna a cada programa un corto intervalo de tiempo del procesador. Si el programa no ha terminado durante este intervalo de tiempo, vuelve a la cola de programas.

  c. Proporcionar una vía de comunicación entre los distintos programas.

b) **ADMINISTRADOR DE MEMORIA.** Este módulo se encarga de asignar ciertas porciones de la memoria principal (RAM) a los diferentes programas que la necesiten, mientras el resto de los datos y los programas se mantienen en los dispositivos de almacenamiento masivo (disco). De este modo, cuando se asigna una parte de la memoria principal se hace de una forma estructurada, siguiendo un determinado orden. La forma más común de administración de la memoria supone crear una **memoria virtual**; con este sistema, la memoria de la computadora aparece, para cualquier usuario del sistema, mucho mayor de lo que en realidad es.

c) **SISTEMA DE ENTRADA/SALIDA.** El sistema operativo es el encargado de atender las particularidades de cada uno de los periféricos (como su velocidad de operación). Una técnica muy común, especialmente en salida en impresoras, es el uso de "spoolers". Los datos de salida se almacenan de forma temporal en una cola situada en un dispositivo de almacenamiento masivo (el spool de impresión), hasta que la impresora se encuentre libre; de este modo se evita que un programa quede retenido porque la impresora no esté disponible. El sistema operativo dispone de llamadas para añadir y eliminar archivos del spool.

d) **ADMINISTRADOR DE ARCHIVOS.** El sistema de archivos **gestiona y establece la forma en que se almacenan los archivos y carpetas en el disco y en las memorias externas** (pendrives, CDs, DVD…). Se encarga de mantener la estructura de los datos y los programas del sistema y de los diferentes usuarios (que se mantienen en archivos) y de asegurar el uso eficiente de los medios de almacenamiento masivo. El administrador de archivos también **supervisa la creación, actualización y eliminación de los archivos,** manteniendo un directorio con todos los archivos que existen en el sistema en cada momento y coopera con el módulo administrador de memoria durante las transferencias de datos desde y hacia la memoria principal. Si se dispone de un sistema de **memoria virtual**, existen transferencias entre la memoria principal y los medios de almacenamiento masivo para mantener la estructura de la misma. Cada archivo está dotado de un conjunto de **privilegios de acceso**, que indican quién puede acceder a ese archivo y con qué permisos. El sistema operativo **comprueba que estos privilegios no sean violados.**



Algunos sistemas de archivos:

- En Windows: FAT, FAT32, NTFS.
- En Linux: ext2, ext3, ext4, ReiserFS.

Estructura jerárquica de carpetas del sistema de archivos de Windows →

Esquema de un sistema operativo

Tipos de sistemas operativos

Los sistemas operativos se clasifican atendiendo a varios aspectos:

Según la interfaz de usuario:

- **S.O. de Modo Gráfico:** tienen una interfaz grafica de usuario (GUI: *Graphic User Interface*), con ventanas, iconos, barras de tareas… En estos entornos es importante el ratón. Ejemplos: Windows, OS X de Apple... ,es la tendencia actual) y
- **S.O. en Modo Texto:** sin GUI,solo tienen la línea de comandos. Ejemplo: MS-DOS

Según el número de usuarios:

- **Monousuario**: solo distingue a un usuario. Ejemplo: MS-DOS
- **Multiusuario:** reconocen varios usuarios. Los sistemas operativos multiusuario son capaces de dar servicio a más de un usuario a la vez, ya sea por medio de varias terminales conectadas a la computadora o por medio de sesiones remotas en una red de comunicaciones. Ejemplos: Linux, Windows, MacOS, Unix…

Según el número de tareas que es capaz de procesar a la vez:

- **Monotarea:** solo pueden procesar una tarea en cada momento por usuario**.** Ejemplo: MS-DOS
- **Multitarea:** permiten la ejecución simultánea de varias tareas por un mismo usuario.

Según el manejo de recursos:

- **Centralizado:** Si permite usar los recursos de una sola computadora.
- **Distribuido o en Red:** Si permite utilizar los recursos (memoria, CPU, disco, periféricos...) de más de una computadora al mismo tiempo.

Según el **número de procesadores** que es capaz de soportar:

- **Sistema Operativo Uniproceso:** es aquél que es capaz de manejar solamente un procesador de la computadora, de manera que si la computadora tuviese más de uno le sería inútil. El ejemplo más típico de este tipo de sistemas es el DOS y MacOS.
- **Sistema Operativo Multiproceso:** permite usar más de un procesador, y el S.O. es capaz de usar todos los procesadores para distribuir su carga de trabajo.

1.3. El concepto de propiedad. Materiales libres .

La mayoría de los programas que usamos a diario son desarrollados por empresas de software con un objetivo comercial, o tienen derechos de autor, por lo que su copia o modificación están prohibidos o limitados. Pero en la década de los 70 surgió el **movimiento del software libre** liderado por **Richard Stallman**, que abanderaba una causa. Los miembros del movimiento de software libre creen que todo el software debería venir acompañado con las 4 libertades declaradas en la definición de software libre (uso, copia, modificación y redistribución). Muchos sostienen que el software privativo es prohibir o impedir a las personas que hagan efectivas esas libertades y que éstas son necesarias para crear una sociedad decente donde los usuarios puedan ayudarse mutuamente y tomar el control sobre el uso de un ordenador.

El movimiento del software libre también cree que todo software necesita **documentación libre**, pero esto no se posiciona firmemente en otros tipos de trabajos. Algunos defensores del software libre apoyan que los trabajos que sirven para un fin práctico también deberían ser libres.

LEY DE LA PROPIEDAD INTELECTUAL Y DERECHOS DE AUTOR

En la web hay materiales protegidos con derechos de autor, que si los descargamos, copiamos y usamos en nuestros videos, presentaciones… podemos infringir la Ley. Por tanto, lo mejor es descargar materiales de bancos de imágenes., sonidos, videos libres de patentes.

¿Qué son los derechos de autor?

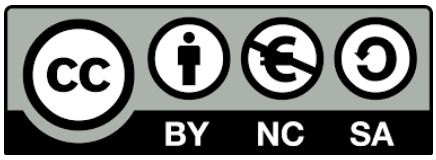
El derecho de autor son el conjunto de derechos de una persona natural sobre su obra de naturaleza literaria, artística o científica, las personas jurídicas también pueden ser titulares de los derechos. La legislación quiere que el trabajo del autor sea siempre reconocido y favorece que pueda obtener unos beneficios por su trabajo intelectual y por su aportación a la cultura o a la ciencia, beneficios que se reconocen durante un tiempo limitado.

BANCOS DE RECURSOS LIBRES DE PANTENTES

Para no infringir la ley de la propiedad intelectual usando obras con derechos de autor, debemos descargar de internet para nuestras producciones **materiales libres de derechos.** Algunos bancos de materiales libres son:

- Bancos de imágenes libres: Pixbay, Pexels, Morguefile ,imgur.com, Picjumbo, Freepick, OpenPhoto, https://search.creativecommons.org/...
- Bancos de sonidos libres: Jamendo, Audionity, SoundCloud, Audionautix, FreeMusicArchive, dig.ccmixer.org ….
- Bancos de videos libres: Videezy, Pexels Videos, Videvo, Mazwai, Pond5 …

LICENCIAS CREATIVE COMMONS



Las licencias Creative Commons (CC) son una herramienta legal de carácter gratuito que permite a los usuarios (licenciatarios) usar obras protegidas por derecho de autor sin solicitar el permiso del autor de la obra. Inicialmente, estas licencias se crearon con base en la legislación estadounidense y fueron portadas (adaptadas) a varias jurisdicciones en todo el mundo.1 Sin embargo, la última versión disponible armoniza las licencias a nivel internacional y se pueden utilizar en diferentes países y entre países.

1.4. Formas de distribución del software. Licencias de sw

En la actualidad hay diferentes categorías de aplicaciones para el ordenador atendiendo a su forma de distribución; las más usuales son:

- **SOFTWARE PRIVATIVO o PROPIETARIO:** software del cual no existe una forma libre de acceso a su código fuente, el cual solo se encuentra a disposición de su desarrollador y no se permite su libre modificación, adaptación o incluso lectura por parte de terceros. El término ha sido creado para designar al antónimo del concepto de software libre. Ejemplo: Microsoft, Adobe Photosohop, Autocad….
- **SOFTWARE LIBRE**. Es aquel que **da el código fuente y 4 libertades:**
  - puede ser **usado,**
  - **copiado**
  - **modificado,** por tanto debe venir **acompañado del código fuente**
  - **y redistribuído,** ; por lo tanto, debe venir acompañado del código fuente para hacer efectivas las libertades que lo caracterizan.

  Ejemplos de software libre: Linux, Guadalines, LibreOffice, THe Gimp, Audacity, FileRoller… y todos los programas que puedes descargar de Sourceforge.

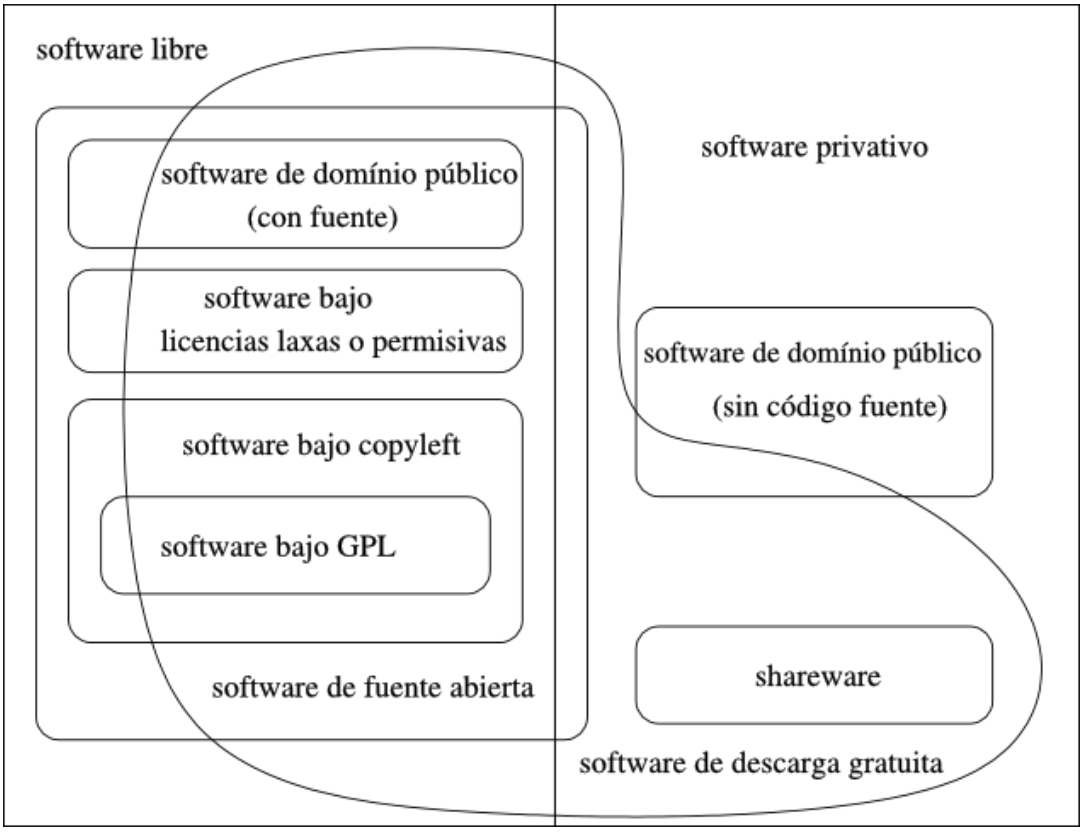
  El software libre protegido con ***copyleft*** impide a los redistribuidores incluir algún tipo de restricción a las libertades propias del software así concebido, es decir, garantiza que las modificaciones seguirán siendo software libre.

  Dentro de software libre hay, a su vez, matices que es necesario tener en cuenta. Por ejemplo, **el software de dominio público** significa que no está protegido por el copyright, por lo tanto, podrían generarse versiones no libres del mismo.

  También es conveniente no confundir el **software libre** con el **software gratuito**, éste no cuesta nada, hecho que no lo convierte en software libre, porque **no es una cuestión de precio, sino de libertad.**

- **Software de dominio público:** es un software libre que no tiene un propietario, por lo tanto no existen derechos de autor, licencias o restricciones de distribución. Por este concepto, el software de dominio público se diferencia de un freeware, el cual conserva los derechos de autor. significa que cualquiera puede obtener las fuentes, modificarlo e incluso publicar sus modificaciones bajo una licencia diferente. Tal es el caso del gestor de bases de datos relacional *SQLite*, ampliamente utilizado sobre todo en dispositivos móviles.
- **Freeware**. es software **privativo** que puede redistribuirse libremente pero no modificarse, entre otras cosas, porque no está disponible su código fuente. El freeware no es software libre. Por ejemplo: programas que descargamos de internet, pero no son libres, como los compresores *WinZip y WinRar*

- **Shareware**. Es un software **privativo** que permite su redistribución, sin embargo no viene acompañado de su código fuente y, por tanto, no puede ser modificado. Además, **pasado un periodo de tiempo nos pide registrarnos y** normalmente es necesario **pagar una licencia** para continuar usándolo, luego tampoco es software libre. Ejemplos: PHPEdit, algunos antivirus.



Licencias de Software

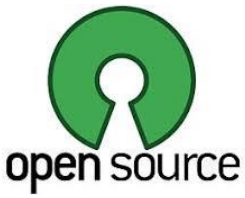
Una **licencia de software** es un contrato entre el **creador del programa** (autor/titular de los derechos de explotación/distribuidor) y el **usuario** que adquiere el programa (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Las licencias de software pueden **establecer en sus cláusulas** entre otras cosas:

- la cesión de determinados derechos del propietario al usuario final sobre una o varias copias del programa,
- los límites en la responsabilidad por fallos,
- el plazo de cesión de los derechos,
- el ámbito geográfico de validez del contrato e incluso
- pueden establecer determinados compromisos del usuario final hacia el propietario, tales como la no cesión del programa a terceros o la no reinstalación del programa en equipos distintos al que se instaló originalmente.

Las licencias de software se clasifican en varios grupos:

A) <u>Licencias de Código Abierto</u>: se puede acceder al ***<u>código fuente</u>*** (programa escrito en un lenguaje de programación). Se dividen en 2 grupos:



- **Permisivas:** permiten al software derivado no tener protección alguna (sin restricciones). Ej: PHP, Apache, Perl
- **Robustas:** aplican algunas restricciones a la obra derivada. Según sean:
  - **Fuertes: <u>Licencia GPL</u>** (todo el software derivado debe estar bajo la misma licencia)
  - **Débiles** o con Copyleft Débil: obliga a que las modificaciones del sw. original se deben licenciar bajo los mismos términos y condiciones que la licencia original, pero las obras derivadas (2ª modificación) pueden ser licenciadas bajo otros términos y condiciones distintas (LGPL)

    Sw. Original:GPL→ Derivado GPL→Sw derivado 2º vez no impone restricciones

B) <u>Licencias de Código Cerrado</u>:

Estas licencias también se conocen con el nombre de *software propietario* o *privativo*. En ellas los propietarios establecen los derechos de uso, distribución, redistribución, copia, modificación, cesión y en general cualquier otra consideración que se estime necesaria. Este tipo de licencias, por lo general, no permiten que el software sea modificado, desensamblado, copiado o distribuido de formas no especificadas en la propia licencia (piratería), regula el número de copias que pueden ser instaladas e incluso los fines concretos para los cuales puede ser utilizado. La mayoría de estas licencias limitan fuertemente la responsabilidad derivada de fallos en el programa. Los fabricantes de programas sometidos a este tipo de licencias por lo general ofrecen servicios de soporte técnico y actualizaciones durante el tiempo de vida del producto.

C) <u>Software de dominio público (sin licencia)</u>.

El Software con dominio público es software sin copyright. Se permite uso, copia, modificación o redistribución con o sin fines de lucro. Algunos tipos de copia o versiones modificadas pueden no ser libres si el autor impone restricciones adicionales en la redistribución del original o de trabajos derivados.

LA LICENCIA GNU GPL (General Public License) y LGPL

La Licencia Pública General de GNU es la licencia más ampliamente usada1 en el mundo del software y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios. Esta licencia fue creada originalmente por *Richard Stallman* fundador de la *Free Software Foundation (FSF)* para el proyecto GNU.

La licencia LGPL

LGPL es prácticamente igual a la GPL, pero permite que software con esta licencia esté integrado en programas privativos. Por ejemplo, la biblioteca C de Linux posee este tipo de licencia, porque si solo fuera GPL, inevitablemente solo se podrían crear aplicaciones para Linux u otros sistemas que manejen la filosofía de software libre, pero como es LGPL, está adaptada para poder crear también

aplicaciones privativas.La licencia LGPL obliga a que los trabajos DERIVADOS del producto que tenga dicha licencia a liberar su codigo fuente, PERO no obliga a los trabajos que USEN dicho productos a hacerlo.
La licencia GPL obliga a que tanto los trabajos derivados como los que usen un productos con dicha licencia liberen su codigo fuente. Lo importante es diferenciar entre un software que USA otro software y el software que DERIVA de otro software. En esos conceptos se apoyan las diferencias entre la LGPL y la GPL. NOTA: la LGPL se suele usar con bibliotecas de funciones como las .DLL por ejemplo, para permitir que programas comerciales las usen, pero en el caso de que modifiquen el código fuente de dichas .DLL deberán liberar solo el código fuente derivado de las mismas (no el de tu software).

Web sobre la licencia GPL:

https://www.gnu.org/licenses/licenses.es.html

Web del proyecto GNU:

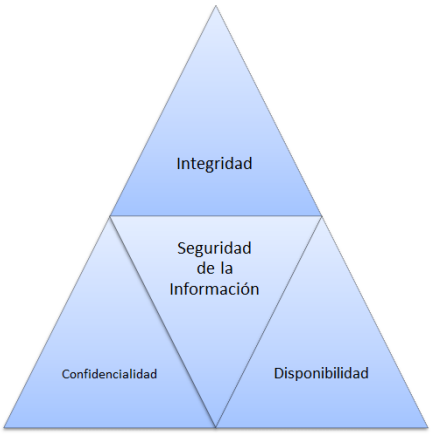
https://fsfe.org/freesoftware/basics/gnuproject.es.html

2. SEGURIDAD INFORMÁTICA

2.1. Principios de la seguridad informática.

Un **sistema seguro** consiste en garantizar los principios de seguridad informática son (**CIDAN**):

- **Confidencialidad:** garantizar que la información solamente será accesible al personal autorizado.
- **Integridad**: propiedad que busca mantener los datos libres de actualizaciones no autorizadas
- **Disponibilidad:** la información debe encontrarse accesible a quien debe acceder a ella.
- **Autenticación**: confirmación de la identidad de un usuario, comprobando que es quien dice ser.
- **No repudio:** permite comprobar la participación de las partes en una comunicación.



ALTA DISPONIBILIDAD: se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todomomento y sin interrupciones, debido a su carácter crítico. El objetivo es mantener el sistema funcionando las 24horas del día, 7 dias a la semana, 365 dias al año, manteniéndolo

a salvo de interrupciones previstas (paralizamos el sistema para realizar cambios o mejoras) o imprevistas (apagón, error del hw/sw, problemas de seguridad, desasatre natural, virtus , accidentes, caída involuntaria del sistema).

2.2. Seguridad activa y pasiva, física y lógica. Seguridad de contraseñas.

Seguridad física: son todos aquellos mecanismos -generalmente de prevención y detección- destinados a **proteger físicamente cualquier recurso hardware** del sistema; estos recursos son desde un simple teclado hasta una cinta de backup (copias de seguridad) con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos, que solo se permita acceder a ellos a las personas autorizadas para hacerlo.
La seguridad lógica se basa, en gran medida, en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de los accesos.
El control de acceso lógico incluye:

- Política de contraseñas. Seguridad de contraseñas.
- Control de acceso a la BIOS,
- Control de acceso al sistema: a la cuenta de usuario, a las carpetas…
- Política de usuarios y grupos

CONTRASEÑAS SEGURAS
Para conseguir que la contraseña sea segura tomemos en cuenta los siguientes criterios:

- Que no sea corta: Mínimo de 8 caracteres
- Combina letras, números y símbolos (.,-…)
- Mientras menos tipos de caracterese haya más larga debe ser
- Si no contiene ningún tipo de símbolos debe ser más larga
- No limitarse a caracteres comunes

La seguridad activa es el conjunto de acciones encaminadas a proteger el ordenador y su contenido (contraseñas seguras, antivirus actuaqlizados…). Se trata de reducir las vulnerabilidades todo lo posible, prevenir ataques o errores, es **preventiva**. Medidas: Antivirus, firewall, encriptación de datos, actualización de sistemas operativos y aplicaciones…

La seguridad pasiva es la que intenta minimizar el impacto y los efectos causados por un posible daño, accidentes (hacer copias de seguridad de los datos, SAI frente a cortes de luz…). Es decir, se consideran acciones posteriores a un ataque o incidente (es paliativa). Comprende:

- **Copias de seguridad periódicas de datos del servidor. Imágenes y restauración**
- **Seguridad física y ambiental**
- **Sistemas de alimentación ininterrumpida (SAI)**

2.3. Actualización de sistemas operativos y aplicaciones.

Dentro de la seguridad Activa, es muy importante mantener el sistema operativo actualizado con los packs de seguridad periódicos y las aplicaciones actualizadas. Los ciberdelicuentes se aprovechan de las vulnerabilidades que requieren una actualización inmediata de los sistemas. Los fabricantes de software actualizan sus sistemas cada vez que encuentran agujeros de seguridad.

2.4. Copias de seguridad.

Una **copia de seguridad, respaldo, copia de respaldo, copia de reserva (del inglés backup**) es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc.

El proceso de copia de seguridad se complementa con otro conocido como restauración de los datos, que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos. La pérdida de datos es muy común, el 66 % de los usuarios de Internet han sufrido una seria pérdida de datos en algún momento

2.5. Software malicioso, herramientas antimalware y antivirus, protección y desinfección.

El malware o software malicioso son programas diseñados para causar problemas y/o errores en nuestro ordenador. Dentro de esta categoría existen muchos tipos, como:

VIRUS: programa que se instala sin el permiso del usuario con le objetivo de causar daños. Puede autorreplicarse e infectar a otros ordenadores. Para propagarse puede valerse de memorias portátiles, software , correo electrónico, internet…

GUSANO: programa malicioso cuya finalidad es desbordar la memoria del sistema reproduciéndose a si mismo.

TROYANO: tipo de virus en el que se han introducido, camufladas en otro programa, instrucciones encaminadas a destruir la información almacenada en los discos o bien a recabar información. Suelen estar alojados en archivos aparentemente inofensivos, como una imagen o un archivo de música, y se instalan al abrir el archivo que los contiene.

KEYLOGER: es un tipo de programa que se encarga de obtener y memorizar las pulsaciones que se realizan en el teclado. Puede usarse para espiar de forma remota, con el objetivo de obtener contraseñas del usuario.

SPYWARE: o software espía, se puede considerar que son los troyanos, el adware y los hijackers.

ADWARE: (de **ad**vertisement soft**ware**) es software de publicidad incluida en programas que la muestran despues de instalarse. El problema viene cuando estos programas actúan como spyware, incluyendo código para recoger información personal del usuario.

HIJACKERS O SECUESTRADORES: son programas que secuestran a otros programas para usar sus derechos o para modificar su comportamiento. El caso más habitual es el ataque a un navegador,

modificando la página de inicio y redireccionando las páginas de búsqueda sin el consentimiento del usuario.

HACKERS Y CRACKERS

Los **hackers** son expertos informáticos que, en principio, solo se plantean retos intelectuales. El hacker no tiene por qué pretender causar daños; de hecho existen empresas de **hacking ético (white hacking)** que ayudan a las personas y empresas a saber cuál es su nivel de seguridad frente a hackers maliciosos. A veces se confunde a los hackers con **piratas informáticos (black hackers)** , que intentan atentar contra la seguridad de sistemas en la red y lucrarse con ello.

Los **crackers** son personas que se dedican a cambiar el funcionamiento de un programa comercial o bien a realizar aplicaciones que obtengan números de serie validos para usarlos sin licencia (piratearlos).

Visitar: https://latam.kaspersky.com/resource-center/threats/malware-classifications

OTRAS TÉCNICAS Y CONCEPTOS

SPAM O CORREO BASURA: son mensajes de correo electrónico que inundan la red con l finalidad de anunciar productos, a veces de dudosa legalidad, para que los usuarios los compren. Se envían de forma masiva porque está demostrado que uno de cada 12 millones de coreos enviados obtiene una respuesta positiva.

HOAXES: son cadenas de correo iniciadas por empresas para poder recopilar las direcciones de correo de muchos usuarios y posteriormente hacer mailing (spam). Se aprovechan de la bondad, la credulidad y la superstición de las personas. Es u na práctica no ilegal en la actualidad.

PHARMING: es una práctica que consisten en redirigir un nombre de dominio a otra máquina distinta, de forma que un usuario que introduzca una URL acceda a la página web del atacante. De este modo se puede, por ejemplo, suplantar la pagina web de un banco para obtener claves de la víctima.

COOKIES: son archivos de texto que se almacenan en el ordenador a través del navegador cuando visitamos una página web, para que esta web los lea en visitas posteriores. No son un riesgo ni una amenaza mientras solo pretendan facilitarnos el acceso al sitio. Se puede considerar spyware no malicioso. Borrar el historial y las cookies es una buena práctica cuando usamos un pc compartido.

HERRAMIENTAS ANTIMALWARE: ANTIVIRUS

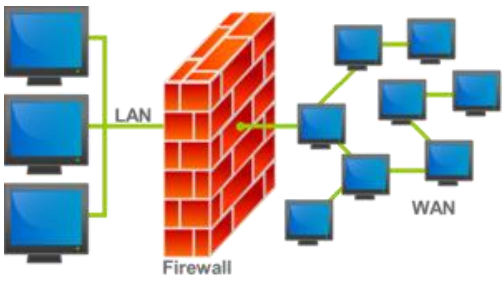
Un **antivirus** es un software que analiza las distintas unidades y dispositivos del PC, así como el flujo de datos entrante y saliente, revisando el código de los archivos, para buscar y eliminar malware. Emplea una base de datos con distintos virus. El antivirus puede detectar virus y solo a veces identificarlos. Podemos estar tranquilos si tenemos un antivirus instalado y actualizado. Existen antivirus gratuitos (Avast, Avira, Avg…)

2.6. Cortafuegos. Seguridad en redes inalámbricas. Ciberseguridad.

CORTAFUEGOS O FIREWALL

Cortafuegos (Firewall)

Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.



Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuegos a una tercera red, llamada *zona desmilitarizada o* DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

SEGURIDAD EN REDES INALAMBRICAS:

Las redes inalámbricas, al funcionar con ondas electromagnéticas, tienen el inconveniente de que cualquier intruso con un dispositivo móvil puede intentar acceder a la red. Debemos por tanto configurarla de forma que sólo puedan acceder a ella los usuarios acreditados. A continuación figuran algunas opciones de seguridad de redes inalámbricas:

Acceso protegido WiFi (WPA2)

WPA2, W*i-Fi* ***P****rotected* ***A****ccess*, es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo, *Wired Equivalent Privacy* (WEP). **WPA** adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una **clave** precompartida, que de un modo similar al WEP, **requiere introducir la misma clave en todos los equipos de la red. WPA2**, creado para corregir las deficiencias del sistema previo (WPA), utiliza el algoritmo de cifrado AES (Advanced Encryption Standard), que es más seguro que el de WPA.

Filtrado MAC

Una **dirección MAC** es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particulalar. Una dirección MAC consiste en seis grupos de dos caracteres, cada uno de ellos separados por dos puntos. 00:1B:44:11:3A:B7 es un ejemplo de dirección MAC.

CIBERSEGURIDAD

La **ciberseguridad** es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica

2.7. Criptografía. Certificados digitales. Agencia española de Protección de datos.

CRIPTOGRAFÍA

La criptografía es una parte de las matemáticas que se encarga del estudio de los algoritmos, protocolos (protocolos criptográficos), y sistemas que se utilizan **para cifrar (enmascarar) la información y así protegerla y dotar de seguridad a las comunicaciones y a las entidades que se comunican.**

Para ello los criptógrafos investigan, desarrollan y aprovechan técnicas matemáticas que les sirven como herramientas para conseguir sus objetivos. Por ejemplo, aplicando funciones matemáticas a las secuencias de bits, se consigue encriptar mensajes. Ejemplos de métodos criptográficos son: la firma digital, mensajes de correo encriptados, protocolos seguros como TransportLayer Security (TLS), HTTPS, WPA2…

CERTIFICADO DIGITAL

Un **certificado digital** o certificado electrónico es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido principalmente para autenticar a un usuario o sitio web en internet por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet.

El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información delicada entre las partes.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

La **Agencia Española de Protección de Datos (AEPD),** creada en 1993, es el organismo público encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España. Tiene su sede en Madrid y su ámbito de actuación se extiende al conjunto de España.

Es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de la Administración pública en el ejercicio de sus funciones. Su principal misión es velar por el cumplimiento de la legislación de protección de datos por parte de los responsables de los ficheros (entidades públicas, empresas privadas, asociaciones, etc.) y controlar su aplicación a fin de garantizar el derecho fundamental a la protección de datos personales de los ciudadanos. La AEPD lleva a cabo sus potestades de investigación fundamentalmente a instancias de los ciudadanos, aunque también está facultada para actuar de oficio. La Agencia es estatutaria y jerárquicamente independiente y se relaciona con el Gobierno a través del Ministerio de Justicia.

Web de la Agencia Española de Protección de Datos: https://www.agpd.es

2.8. Seguridad en redes sociales, acoso y convivencia en la red.

Las redes sociales son estupendas herramientas de comunicación con otras personas, pero debemos utilizarlas de forma segura. Para ello:

- Configura adecuadamente la privacidad de tu perfil.
- Filtra la información que subes a Internet. Ten en cuenta que una vez subida pierdes el control de la misma.
- Piensa antes de publicar algo, ya que una vez publicado no sabes si saldrá de la red social. Podrán utilizar esa información en tu contra.
- Revisa las aplicaciones instaladas y ten cuidado con publicaciones sospechosas, aunque provengan de contactos conocidos.
- Las principales redes sociales se toman muy en serio los problemas de seguridad de sus usuarios. Si tienes problemas, contacta con ellos a través de los mecanismos de contacto o de denuncia que facilitan.

- Asegúrate de que tus contactos en las redes sociales son realmente quienes crees que son. No nos conformemos con ver la foto, el nombre o que es amigo de nuestros amigos.
- Al igual que en la vida real, en las redes sociales también debemos ser respetuosos y tratar con educación a nuestros contactos. No envíes mensajes ofensivos a ningún contacto. Debes ser respetuoso y tratar con educación a tus contactos.
- No compartas fotos ni vídeos en los que aparezcas en situaciones comprometidas (sexting).
- No te olvides de leer la política de privacidad y las condiciones del servicio antes de usarlo.

DIRECCIONES WEB:

Web sobre la licencia GPL:

https://www.gnu.org/licenses/licenses.es.html

Web del proyecto GNU:

https://fsfe.org/freesoftware/basics/gnuproject.es.html

Malware:

https://latam.kaspersky.com/resource-center/threats/malware-classifications

Ciberseguridad: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Criptografía: https://tecnologia-informatica.com/que-es-la-criptografia/

Qué es un certificado digital: http://www.upv.es/contenidos/CD/info/711545normalc.html

Antivirus gratuitos:

https://www.avast.com/es-es/free-antivirus-download

https://www.avira.com/es/downloads

https://www.avg.com/es-es/free-antivirus-download

Mapa de ciberamenazas Kasperski: https://cybermap.kaspersky.com/