# TEMA 1 - SEGURIDAD INFORMÁTICA

## 1.1 Definición de Seguridad Informática

La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

## 1.2 Fiabilidad, Confidencialidad, Integridad y Disponibilidad

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque, son los datos y la información los sujetos **principales** de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y la disponibilidad de la información, por tanto, actualmente se considera que la seguridad de los datos y la información comprende 3 aspectos fundamentales:

1. *Confidencialidad*
2. *Integridad (seguridad de la información)*
3. *Disponibilidad*

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarla suelen afectar a estas 3 características de forma conjunta por tanto un fallo del sistema que haga que la información no sea accesible puede llevar consigo una pérdida de integridad. Generalmente tiene que existir los 3 aspectos descritos para que haya seguridad. Dependiendo del entorno en el que trabaje un sistema, a sus responsables les interesara dar prioridad a un cierto aspecto de la seguridad. Junto a estos 3 conceptos fundamentales se suele estudiar conjuntamente la *autenticación* y el *no repudio*. Suele referirse al grupo de estas características como **CIDAN**, nombre sacado de la inicial de cada característica.

Los diferentes servicios de seguridad dependen unos de otros jerárquicamente, así si no existe el primero no puede aplicarse el siguiente.

**Disponibilidad:** Se trata de la capacidad de un servicio, de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.

**Confidencialidad:** Se trata de la cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

Un ejemplo de control de la confidencialidad sería el uso cifrado de clave

simétrica en el intercambio de mensajes.

**Integridad:** Es la cualidad que posee un documento o archivo que no ha sido alterado y que ademas permite comprobar que no se ha producido manipulación alguna en el documento original.

**Alta disponibilidad** (Hight Availability): son sistemas que están disponibles las 24 horas al día, 7 días a la semana, 365 días al año.
La disponibilidad se presenta en niveles:

- *Base*: Se produce paradas previstas y imprevistas.
- *Alta*: Incluyen tecnologías para disminuir el número y la duración de interrupciones imprevistas, aunque siempre existe alguna interrupción imprevista.
- *Operaciones continuas*: Utilizan tecnologías para segura que no hay interrupciones planificadas
- *Sistemas de disponibilidad continua*: Se incluyen tecnologías para asegurarse que no habrá paradas imprevistas ni previstas.
- *Sistemas de tolerancia al desastre*: requieren de sistemas alejados entre sí para asumir el control en una interrupción provocada por un desastre.

**Autenticación:** Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice. Las autenticaciones de los sistemas informático se realizan habitualmente mediante nombre y contraseña.

**No repudio:** El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.
Existen 2 posibilidades:

- *No repudio en origen*: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo el receptor recibe una prueba infalsificable del envío.
- *No repudio de destino*: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Si la autenticidad prueba quien es el autor y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (en origen) y que el destinatario la recibió (en destino).

### 1.3. Elementos vulnerables en un S.I.: Hw,Sw, Datos.

Seguridad es un concepto asociado a la certeza,falta de riesgo o contingencia conviene aclarar que no siendo posible la certeza absoluta el elemento de riesgo está siempre presente independientemente de las medidas que tomemos por lo que debemos hablar de niveles de seguridad, la seguridad

absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener niveles altos de seguridad, la seguridad es un problema integral, los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo, por otra parte, existe algo que los hackers llaman ingeniería asociada que consiste simplemente en conseguir mediante un engaño que los usuarios autorizados revelen sus password, por lo tanto la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

Los 3 elementos principales a proteger en cualquier sistema informático son el **software, el hardware y los datos**. Por hardware entendemos el conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red,etc... Por software entendemos el conjunto de programas lógicos que hacen funcionar el hardware tanto sistemas operativos como aplicaciones y por datos el conjunto de información lógica que 3 Amenazas Física maneja el software y el hardware como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Habitualmente los datos constituyen los 3 principales elementos a escoger ya que es el más amenazado y seguramente el más difícil de recuperar. También tenemos que ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware el sistema operativo, las comunicaciones, medidas de seguridad física, controles organizativos y legales.

**1.4 Las amenazas.**

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema desde un troyano, pasando por un programa descargando de forma gratuita que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad; se pueden clasificar por tanto en amenazas provocadas por **personas, lógicas y físicas**. A continuación, se presenta a una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. La primera son las personas, la mayoría de los ataques a nuestro sistema van a provenir de forma intencionada o inintencionada de personas y pueden causarnos enormes pérdidas. Aquí se describen brevemente los diferentes tipos de personas que pueden constituir un riesgo para nuestros sistemas:

1 Personas:

- **Personal** (se pasa por alto el hecho de la persona de la organización incluso a la persona ajeno a la estructura informática, puede comprometer la seguridad de los equipos)

- **Ex-empleados**(generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aun trabajaran el la organización)
- **Curiosos**(son los atacantes juntos con los crakers los que más se dan en un sistema )
- **Hackers**(una persona que intenta tener acceso no autorizado a los recursos de la red con intención maliciosa aunque no siempre tiende a ser esa su finalidad)
- **Crackers**(es un término mas preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa)
- **Intrusos remunerados**(se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la organización)

2 Amenazas lógicas:

- **Sofware incorrepto**(a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.)
- **Herramientas de seguridad**(cualquier herramienta de seguridad representa un arma de doble filo de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos, herramientas como NESUS,SAINT o SATAN pasa de ser útiles a peligrosas cuando la utilizan Crakers.)
- **Puertas traseras**(durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se esta diseñando.) Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial.)
- **Canales cubiertos**(son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.)
- **Virus**(un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a si mismo en otros programas.)
- **Gusanos**(es un programa capaz de ejecutarse y propagarse por si mismo a través de redes en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos a ser difíciles de programar su numero no es muy elevado pero el daño que causa es muy grave.)

- **Caballos de troya**(son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de el pero que realmente ejecuta funciones ocultas.), Programas conejo o bacterias(bajo este nombre se conoce a este programa que no hace nada útil si no que simplemente se delimitan a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación del servicio.

3 Amenazas Físicas: Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales.

1.5 **Formas de protección de nuestro sistema**: Para proteger nuestros sistemas hemos de realizar una análisis de las amenazas potenciales, las perdidas que podrían generar y la probabilidad de si ocurrencia a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan, a esto se le llama mecanismo de seguridad, son la herramienta básica para garantizar la protección de los sistemas o la red. Estos mecanismo se pueden clasificar en activas o pasivas.

- **Activas**> evitan daños en los sistemas informáticos mediante empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones, encriptación de los datos en las comunicaciones, filtrado de conexiones en redes y el uso de software especifico en seguridad informática.
- **Pasiva**> minimizan el impacto y los efectos causados por accidentes mediante uso de hardware adecuado, protección física, eléctrica y ambiental, realización de copias de seguridad.

# TEMA 2 - SEGURIDAD FÍSICA

## 2.1. Principios de la seguridad física

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos. Cada sistema es único, por lo tanto la política de seguridad a implementar no sera única es por ello siempre se recomendara pautas de aplicación general y no procedimientos específicos.

La seguridad física está enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico donde se encuentra ubicado

el centro.
Las principales amenazas que se ven en la seguridad física son amenazas ocasionadas por el hombre como robos destrucción de la información , disturbios, sabotajes internos y externos, incendios accidentales, tormentas e inundaciones.

## 3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

La mayoría de los daños que puede sufrir un sistema informático no será solo los medios físicos sino contra información almacenada y procesada. **El activo mas importante que se posee es la información** y por tanto deben existir técnicas mas allá de la seguridad física que la aseguren, estas técnicas las brinda la seguridad lógica.
Es decir que **la seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para ello**.
Los objetivos que se plantean serán:

- Restringir el acceso al arranque (desde la BIOS) al S.O, los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto analizando periódicamente los mismos.

### 3.2.4 MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y la información esta modalidad puede ser:

- **Lectura**: el usuario puede únicamente leer o visualizar la información, pero no puede alterarla, debe considerarse que la información puede ser copiada o impresa
- **Escritura**: este tipo de acceso permite agregar datos, modificar o borrar información
- **Ejecución**: otorga al usuario el privilegio de ejecutar programas.
- **Borrado**: permite al usuario eliminar recursos del sistema como programas, campos de datos o archivos.
- **Todas las anteriores**

Además, existen otras modalidades de acceso especiales:

- **Creación**: permite al usuario crear archivos nuevos, registros o campos.
- **Búsqueda**: permite listar los archivos de un directorio determinado

### 3.2.5 UBICACIÓN Y HORARIOS

El acceso a determinados recursos del sistema puede estar basado en la **ubicación física o lógica de los datos o personas.** En cuanto a los **horarios** este tipo de controles permite limitar el acceso de los usuarios a determinadas horas del día o a determinados días de la semana. Se debe mencionar que en estos dos tipos de controles siempre deben ir acompañados de algunos de los controles anteriormente mencionados.

## 3.3 ADMINISTRACIÓN

Una vez establecidos los controles de acceso sobre los sistemas y a las aplicaciones es necesario realizar una eficiente administración de estas medidas lo que involucra la **implementación, seguimientos, pruebas y modificaciones** sobre los accesos de los usuarios en los sistemas. La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos, especificando las concesiones necesarias para el establecimiento de perfiles de usuario. La definición de permisos de acceso requiere determinar cuál será el nivel de seguridad necesario sobre los datos por lo que es imprescindible **clasificar la información** determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad. Para empezar la implementación es conveniente empezar definiendo las medidas sobre la información **más sensible o las aplicaciones más críticas** y avanzar de acuerdo a un **orden de prioridad decreciente** establecido alrededor de las aplicaciones.
Tiene que existir una **conciencia de la seguridad organizacional** por parte de todos los empleados, esta consciencia puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y estableciendo **compromisos firmados** por el personal donde se especifique la responsabilidad de cada uno. Además debe existir una concienciación por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su perdida o apropiación por agentes extraños a la organización.

### 3.3.1 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS

Este proceso lleva generalmente 4 pasos:

- Definición de Puestos: Debe contemplarse la máxima separación de funciones y el otorgamiento mínimo de permisos de acceso por cada puesto para la ejecución de las tareas asignadas.
- Determinación de la sensibilidad del puesto: Es necesario determinar si la función requiere permisos arriesgados que le permitan alterar procesos, perpetuar fraudes o visualizar información confidencial.
- Elección de la persona para cada puesto: Requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto, así mismo para los puestos definidos como críticos puede requerirse una verificación de antecedentes personales.
- Entrenamiento inicial y continuo del empleado: Cuando la persona ingresa a la organización debe comunicársele las políticas de seguridad de la organización y su responsabilidad. El personal debe sentir que la seguridad es un elemento prioritario.

## GESTION DE ALMACENAMIENTO DE LA INFORMACION

### 5.1. INTRODUCCIÓN

Todo equipo informático dispone de un sistema de almacenamiento para guardar los datos. En un altísimo porcentaje, el sistema de almacenamiento está constituido por uno o varios discos duros. Estos serán de mayor o menor sofisticación, pero todos constituyen en sí mismos un elemento dedicado que necesitan unas condiciones mínimas de trabajo.

Hacer trabajar a los discos duros en condiciones extremas puede producir una avería física que como consecuencia podría hacer imposible acceder a la información que contiene. Por tanto, aunque los 3 elementos principales a proteger son el software ,el hardware y los datos, este último, es el **principal elemento** de los 3 ya que es el más amenazado y seguramente, el más difícil de recuperar.

Contra cualquiera de los 3 elementos se pueden realizar multitud de ataques o dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en 4 grandes grupos: *Interrupción, Interceptación, Modificación y Fabricación*.

- Una ataque se identifica como interrupción, si se hace con un objeto de sistema, se pierda, quede inutilizable, o no disponible.
- Se tratara de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema.
- Una modificación si además de conseguir el acceso, consigue modificar el objeto, algunos autores consideran un caso especial de la modificación la destrucción, entendiéndola como una modificación que inutilizable el objeto.
- Por último se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el original y el fabricado.

El almacenamiento de la información requiere una serie de principios y características que mejorar:

- Rendimiento.
- Disponibilidad.
- Accesibilidad.

### 5.1.1. Rendimiento

Se refiere a la capacidad de disponer un volumen de datos en un tiempo determinado. Se mide en tasas de transferencia (MBits/s).

Existen muchas tecnologías para fabricar dispositivos de almacenamiento, caracterizadas por: **coste por bit, tiempo de acceso y capacidad de almacenamiento**. El procesador es el elemento principal del ordenador, interesa que los datos con los que va a operar en un momento dado estén los mas próximas a ellas. Cuando la CPU encuentra un dato que necesita sus registros internos se intenta recuperar del nivel inmediatamente inferior (la caché), si no lo encuentra accede a la RAM y si tampoco está allí al disco duro, discos ópticos, etc. Se debe satisfacer por lo tanto la propiedad de *inclusión* según la cual la información en un determinado nivel se encuentra replicada en los niveles inferiores. Este principio determina la jerarquía de memorias, ubicación temporal de los datos, que está fuertemente ligada a la necesidad que tiene el micro de emplearlos en un momento determinado. Los datos recientemente accedidos se ubican en las memorias mas rápidas y estas deben estar próximas al microprocesador o a la CPU. Las memorias sucesivamente mayores y mas lentas de mayor tiempo de acceso por bit dispondrán todos los datos potencialmente accesibles por la CPU. La memoria interna de carácter volátil o no permanente en ausencia de alimentación eléctrica de mayor velocidad y coste compone los 3 escalones superiores de la pirámide (Registros internos, memoria caché y memoria RAM). Los niveles inferiores (discos magnéticos, ópticos y cintas magnéticas) se suelen agrupar con nombre de memoria externa de carácter no volátil, almacena la información de forma permanente en ausencia de electricidad, menor velocidad de acceso y menor coste por bit.

### 5.1.2. Disponibilidad

La disponibilidad se refiere a la seguridad que la información puede ser recuperada en el momento en que se necesite. Esto es evitar su perdida o bloqueo bien sea por ataque, mala operación accidental o situaciones fortuitas o de fuerza mayor. Las distintas técnicas que hoy favorecen la alta disponibilidad de los sistemas de almacenamiento son:

La **redundancia** o duplicados de información:

- Sistemas RAID de almacenamiento.
- Centro de procesamiento de centros de respaldo.

La **distribución** de la información:

- Disponer de copias de seguridad en distintas ubicaciones geográficas.
- Medios de almacenamiento extraíbles y portátiles.
- Servidores de almacenamiento redundantes y distribuidos geográficamente con sincronización en la información que contienen.
- Copias de seguridad en la nube
- Servicios de copias de seguridad online.

5.1.3. Accesibilidad
Se refiere a tener disponible la información por parte de los usuarios autorizados. Habitualmente se controla mediante técnicas de control de acceso.

## 5.2. Medios de almacenamiento

En primer lugar realizaremos una clasificación de los dispositivos de almacenamiento en función de varias características:

- La naturaleza del soporte de almacenamiento: magnético,óptico,magnetoóptico, memorias flash.
- Si es posible leer o escribir.
- Acceso a la información secuencial o directo.
- Dispositivos interno o externo al sistema informático.
- Conexión entre el soporte de la información y la unidad lectora-escritora.

5.2.1. Soporte de almacenamiento de la información
Se determina soporte a todo material o dispositivo en general destinado a registrar información sera un medio en el que se almacene información con una determinada escritura y de manera indefinida para que pueda ser utilizada por el sistema o por terceras personas. No se debe confundir soporte de información con periférico. Se considera periférico a cualquier periférico de entrada-salida conectado al ordenador que sirve para leer o escribir información sobre los soportes. Es pues, el soporte, el almacén de la información y el periférico el encargado de leer y escribir información sobre dicho soporte. Los mas extendidos son los siguiente:

- Magnéticos***:*** Los discos y cintas magnéticas contienen soportes de información constituidos por un sustrato de plástico o aluminio recubierto

con un material magnetizable tradicionalmente oxido férrico o oxido de cromo. La información se graba dentro de unidades elementales o celdas que forman lineas o pistas. Cada celda puede estar sin magnetizar o estar magnetizada en uno de dos estados o campos magnéticos(Norte o Sur) que podrán corresponder a un 0 o a un 1. Para escribir o leer una celda se emplea la electricidad para crear campos magnéticos orientados en una dirección u otra para representar 1 o 0. Ejemplos: Cintas magnéticas, discos magnéticos son los mas empleados para el almacenamiento masivo de gran volumen de información.

- Ópticos***:*** Usan la energía lumínica mediante un rayo láser u un elemento lumínico para almacenar o leer la información. Los 0 o 1 se representan por la presencia o ausencia de una señal luminosa, ejemplos: dvd's, cd's. Los mas extendidos de uso portátil multimedia, comercial, con usos de solo lectura.
- Magnetoópticos: Son soportes que permiten la lectura y la escritura. La información no se graba de manera mecánica, se graba magnéticamente. Los discos vírgenes tienen una magnetización previa mediante láser es posible cambiar la magnetización de las celdas. Los discos magnetoópticos como el cd-mo son regrabables aunque son mas duraderos que los cd-w ya que estos se van degradando en cada operación de escritura. Los mini disck y unidades zip han tenido un gran éxito comercial en los 80's y 90.
- Flash USB***:*** Emplean memoria semiconductora en uno o varios chips de tipo flash NAND su cualidad mas destacada es que a pesar de ser memoria semiconductora mantiene su contenido sin necesidad de suministrar energía eléctrica mediante tecnología de puerta flotante, los electrones quedan confinados en el transistor que forma la celda de memoria, ejemplo: memorias de cámaras, memorias usb.

### 5.2.2. Lectura-escritura

De todos los soportes se puede extraer la información almacenada, pero en algunos casos solo se puede realizar una escritura por lo que no se podrá volver a escribir en ellos. Podemos clasificarlos en:

- Reutilizables o regrabables: Podemos emplear el mismo soporte todas las veces que deseemos, ejemplos, cinta magnética, memoria usb, cd-rw.
- No reutilizable o de solo lectura: Una vez que se graba la información no se puede modificar, tan solo leerla, ejemplos cd, dvd.

### 5.2.3. Acceso a la información

- Secuencial: Para acceder a un dato tenemos que leer u escribir todos los anteriores, ejemplo, la grabación de un cd y en una cinta magnética la lectura y escritura.

- Directo: Podemos acceder a cualquier dato de forma casi inmediata, ejemplo, la lectura de un cd, disco duro, memoria USB es directa. Podemos leer cualquier archivo sin necesidad de acceder a los demás.

5.2.4. Ubicación de la unidad

- Interna: La unidad lectora-grabadora ser localiza dentro de la carcasa del ordenador, ejemplos, discos duros,unidades de cd.
- Externa: la unidad lectora-grabadora se sitúa fuera del ordenador, ejemplos, memoria USB,disco duro externo,unidad lectora de dvd y cd externa.

5.2.5._Conexión entre soporte y unidad

- Removibles: El soporte que almacena la información se puede cambiar permaneciendo la unidad lectora-grabadora, ejemplos, cd,dvd.
- No removibles: El soporte que almacena la información y la unidad lectora-grabadora se encuentran unidos,ejemplo, los discos duros y la memoria USB.