TEMA 1

1. Informática básica: conceptos fundamentales sobre el hardware y el software.
2. Sistemas de almacenamiento de datos.
3. Sistemas operativos.
4. Nociones básicas de seguridad informática.

Supera.
by thePower

PÁG.

Significado de los iconos que aparecen dentro de los TEMAS:

Examen


Importante


Recordatorio


Atención

1. Informática básica: conceptos fundamentales sobre el hardware y el software

1.1. HARDWARE

El término es propio del idioma inglés, y su traducción al español no tiene un significado acorde, por tal motivo se lo ha adoptado tal cual es y suena. La Real Academia Española lo define como ***«Conjunto de los componentes que integran la parte material de una computadora».***

El hardware principal de un computador se compone de una unidad central de procesamiento (CPU), encargada de procesar los datos; una memoria rápida de trabajo para almacenamiento temporal; una unidad de almacenamiento fija para mantener software y datos así como extraerlos de ella; uno o varios periféricos de entrada, los que permiten el ingreso de la información y uno o varios periféricos de salida, que posibilitan dar salida (normalmente en forma visual, impresa o auditiva) a los datos procesados.

La clasificación evolucionista del hardware del computador electrónico está dividida en generaciones, donde cada una supone un cambio tecnológico notable. El origen de las primeras es sencillo de establecer, ya que en ellas el hardware fue sufriendo cambios radicales. Los componentes esenciales que constituyen la electrónica del computador fueron totalmente reemplazados en las primeras tres generaciones, originando cambios que resultaron trascendentales. En las últimas décadas es más difícil distinguir las nuevas generaciones, ya que los cambios han sido graduales y existe cierta continuidad en las tecnologías usadas. En principio, se pueden distinguir:

1.ª generación (1945-1956): electrónica implementada con tubos de vacío. Fueron las primeras máquinas que desplazaron los componentes electromecánicos (relés).

2.ª generación (1957-1963): electrónica desarrollada con transistores. La lógica discreta era muy parecida a la anterior, pero la implementación resultó mucho más pequeña, reduciendo, entre otros factores, el tamaño de un computador en notable escala.

3.ª generación (1964-hoy): electrónica basada en circuitos integrados. Esta tecnología permitió integrar cientos de transistores y otros componentes electrónicos en un único circuito integrado impreso en una pastilla de silicio. Los ordenadores redujeron así considerablemente su costo, consumo y tamaño, incrementándose su capacidad, velocidad y fiabilidad, hasta producir máquinas como las que existen en la actualidad.

4.ª generación (futuro): probablemente se originará cuando los circuitos de silicio, integrados a alta escala, sean reemplazados por un nuevo tipo de material o tecnología.

La aparición del **microprocesador** marca un hito de relevancia, y para muchos autores constituye el inicio de la cuarta generación. A diferencia de los cambios tecnológicos anteriores, su invención no supuso la desaparición radical de los computadores que no lo utilizaban. Así, aunque el microprocesador 4004 fue lanzado al mercado en 1971, todavía a comienzo de la década de 1980 había computadores, como el PDP-11/44,10 con lógica carente de microprocesador que continuaban exitosamente en el mercado; es decir, en este caso el desplazamiento ha sido muy gradual.

Otro hito tecnológico usado con frecuencia para definir el inicio de la cuarta generación es la aparición de los **circuitos integrados VLSI (very large scale integration),** a principios de los ochenta. Al igual que el microprocesador, no supuso el cambio inmediato y la rápida desaparición de los computadores basados en circuitos integrados en más bajas escalas de integración. Muchos equipos implementados con tecnologías VLSI y MSI (medium scale integration) aún coexistían exitosamente hasta bien entrados la década de 1990.

Una de las formas de clasificar el hardware es en **dos categorías**: por un lado, el hardware principal, que abarca el conjunto de componentes indispensables necesarios para otorgar la funcionalidad mínima a una computadora; y por otro lado, el hardware complementario, que, como su nombre indica, es el utilizado para realizar funciones específicas (más allá de las básicas), no estrictamente necesarias para el funcionamiento de la computadora.

El hardware principal está básicamente constituido por: un medio de entrada de datos, la unidad central de procesamiento, la memoria RAM, un medio de salida de datos y un medio de almacenamiento de datos.

Los medios de entrada y salida de datos estrictamente indispensables dependen de la aplicación: desde el punto de vista de un usuario común, se debería disponer, al menos, de un teclado y un monitor para entrada y salida de información, respectivamente; pero ello no implica que no pueda haber una computadora (por ejemplo controlando un proceso) en la que no sea necesario teclado y/o monitor; bien puede ingresar información y sacar sus datos procesados, por ejemplo, a través de una placa de adquisición/salida de datos.

Los ordenadores son aparatos electrónicos capaces de interpretar y ejecutar instrucciones programadas y almacenadas en su memoria; consisten básicamente en operaciones aritmético-lógicas y de entrada/salida. Se reciben las entradas (datos), se las procesa y almacena (procesamiento), y finalmente se producen las salidas (resultados del procesamiento). Por ello todo sistema informático tiene, al menos, **componentes y dispositivos hardware dedicados a alguna de las funciones antedichas; a saber:**

- **Procesamiento**: unidad central de procesamiento.
    - *La Unidad Central de Procesamiento*, conocida por las siglas en inglés CPU, es el componente fundamental de la computadora, encargada de interpretar y ejecutar instrucciones y de procesar datos. En computadores modernos, la función de la CPU la realiza uno o más microprocesadores. Se conoce como microprocesador a una CPU que es manufacturada como un único circuito integrado. Un servidor de red o una máquina de cálculo de alto rendimiento (supercomputación), puede tener varios, incluso miles de microprocesadores trabajando simultáneamente o en paralelo multiprocesamiento); en este caso, todo ese conjunto conforma la CPU de la máquina. Las unidades centrales de proceso (CPU) en la forma

de un único microprocesador no solo están presentes en las computadoras personales (PC), sino también en otros tipos de dispositivos que incorporan una cierta capacidad de proceso o «inteligencia electrónica», como pueden ser: controladores de procesos industriales, televisores, automóviles, calculadoras, aviones, teléfonos móviles, electrodomésticos, juguetes y muchos más. Actualmente los diseñadores y fabricantes más populares de microprocesadores de PC son Intel y AMD; y para el mercado de dispositivos móviles y de muy bajo consumo, los principales son Samsung, Qualcomm, Texas Instruments, MediaTek, NVIDIA e Intel.

- *La placa base*, también conocida como placa madre o principal es un gran circuito impreso sobre el que se suelda el chipset, las ranuras de expansión (slots), los zócalos, conectores, diversos circuitos integrados, etc. Es el soporte fundamental que aloja y comunica a todos los demás componentes: microprocesador, módulos de memoria RAM, tarjetas gráficas, tarjetas de expansión, periféricos de entrada y salida. Para comunicar esos componentes, la placa base posee una serie de buses mediante los cuales se transmiten los datos hacia dentro y fuera del sistema.

- La tendencia de integración ha hecho que la placa base se convierta en un elemento que incluye a la mayoría de las funciones básicas (vídeo, audio, red, puertos de varios tipos), funciones que antes se realizaban con tarjetas de expansión. Aunque ello no excluye la capacidad de instalar otras tarjetas adicionales específicas, tales como capturadoras de vídeo, tarjetas de adquisición de datos, etc.

- **Almacenamiento: Memorias**

- **Memoria RAM:** La sigla RAM, del inglés *Random Access Memory*, literalmente significa memoria de acceso aleatorio. El término tiene relación con la característica de presentar iguales tiempos de acceso a cualquiera de sus posiciones (ya sea para lectura o para escritura). Esta particularidad también se conoce como «acceso directo», en contraposición al acceso secuencial.

  La RAM es la memoria utilizada en una computadora para el almacenamiento transitorio y de trabajo (no masivo). En la RAM se almacena temporalmente la información, datos y programas que la Unidad de Procesamiento (CPU) lee, procesa y ejecuta. La memoria RAM es conocida como memoria principal de la computadora, también como memoria central o de «trabajo»; a diferencia de las llamadas memorias auxiliares, secundarias o de almacenamiento masivo (como discos duros, unidades de estado sólido, cintas magnéticas u otras memorias).

  Entre los tipos de memoria RAM existentes, en la actualidad podemos encontrar de dos tipos:

  - DRAM: significa Dynamic RAM, y es la más utilizada en PCs y, de hecho, en casi cualquier dispositivo incluyendo smartphones. Este tipo de memoria está formada por condensadores que requieren que la controladora almacene varias veces por segundo los datos almacenados en ella para que no se pierdan. Se utiliza para memorias RAM convencionales y a diferencia de la SRAM necesita ser refrescada cada cierto tiempo para mantener los datos.

  - SRAM: significa Static RAM, y como su nombre indica es estática. En este caso los datos se almacenan hasta que se corte el suministro eléctrico sin que el controlador tenga que estar refrescando los datos constantemente; es más rápida y consume menos energía que la DRAM, pero se utiliza menos porque es más cara de fabricar y permite unas densidades (capacidades) muy inferiores. La SRAM se utiliza para las cachés y los registros tanto de CPUs como de GPUs.

- Por otro lado, hay que aclarar que la memoria NVRAM, Non Volatile RAM, hace referencia a la memoria NAND Flash, concretamente a módulos de memoria DIMM que integran chips de memoria NAND Flash en vez de RAM convencional. Sea cual sea el tipo de memoria flash esta no se usa como memoria RAM, excepto en componentes que funcionan muy baja velocidad de reloj.

- **La memoria ROM** se llama así por las siglas en inglés Read Only Memory, o memoria de solo lectura. La mayor diferencia entre la memoria RAM y la ROM es que la ROM no es volátil, es decir, la información almacenada se retiene, aunque apaguemos el PC. Este tipo de memoria tiene una capacidad muy inferior a la RAM y además es mucho más lenta.

  - En los primeros ordenadores debido a que la memoria de almacenamiento que se solía utilizar era muy lenta, ya que se solían utilizar discos magnéticos o cintas, se solía incluir una ROM donde se cargaba el sistema operativo y la BIOS del mismo.

  - La memoria ROM dejo de utilizarse tan pronto como la velocidad la supero y la latencia por utilizarla paso a demasiado alta. Cuando ese fenómeno ocurrió fue cuando los discos duros empezaron a estandarizarse en los PCs.

  - Inicialmente, la memoria ROM era únicamente de solo lectura, pero desde hace ya tiempo es simplemente memoria no volátil en la que también se puede escribir... de algunas maneras concretas. En la memoria ROM se almacena, por ejemplo, la BIOS (que como sabéis se puede actualizar), así como el firmware de los dispositivos. Estos son los tipos principales de memoria ROM que se utilizan hoy en día:

    - *Mask ROM*: este tipo de memoria es la que se utiliza durante el proceso de fabricación de los dispositivos, y una vez escritos los datos no pueden ser modificados.
    - *PROM*: significa «Programmable ROM», y como su nombre indica los datos que almacena pueden ser programados (a diferencia de la Mask ROM, después del proceso de fabricación). Tiene la particularidad de que una vez que se escribe en ella, estos datos ya no pueden ser modificados nunca más.
    - *EPROM*: significa «Erasable Programmable ROM», y es parecida a la PROM pero permite que los datos se eliminen en condiciones específicas (esencialmente exponiéndola a luz ultravioleta de alta intensidad).
    - *EEPROM*: significa «Electrically Erasable Programmable ROM», y es el tipo de memoria ROM más utilizado porque permite que los datos se eliminen y reescriban un número ilimitado de veces.

- **Entrada: Periféricos de entrada (E)**

  - Los dispositivos periféricos de entrada son todos aquellos dispositivos que permiten introducir datos o información en una computadora para que ésta los procese u ordene. A pesar de que el término "periférico" implica a menudo el concepto de "adicional pero no esencial", muchos periféricos son elementos fundamentales para un sistema informático. Sin embargo, al ser las fuentes primordiales de entrada, se pueden considerar como extensiones en un sistema.

  - Un dispositivo de entrada es cualquier periférico del equipamiento de la computadora, utilizado para proporcionar datos y señales de control a un sistema de procesamiento de la información. Los periféricos de entrada y salida componen la interfaz del hardware, por ejemplo, entre un escáner o controlador seis grados de libertad (6DOF).

- Ejemplos: teclado, ratón óptico, escáner, micrófono, palanca de mando, gamepad o controlador de videojuego, que están conectados a la computadora y son controlados por el microprocesador.

- **Salida: Periféricos de salida (S)**

Los periféricos de salida reciben la información procesada por la CPU y la reproducen, de modo que sea perceptible por el usuario.

- Visuales
  - Monitor de computadora
  - Impresora
  - Led
  - Visualizador
  - Proyector de vídeo
- Auditivos
  - Altavoz
  - Auriculares
  - Tarjeta de sonido
- Táctiles
  - Impresora braille
  - Impresora 3D
- Monitor
- Impresora
- Altavoz o parlante. Auriculares

- **Entrada/Salida: Periféricos mixtos (E/S).**
  - Los periféricos de entrada/salida son los que utiliza la computadora para mandar y para recibir información. Su función es la de almacenar o guardar, de forma permanente o virtual, todo aquello que hagamos con la computadora para que pueda ser utilizado por los usuarios u otros sistemas.
  - Pantalla táctil o multitáctil
  - Impresora multifunción
  - Casco virtual

- **Periféricos de almacenamiento**
  - Tarjeta perforada
  - Cinta perforada
  - Cinta magnética
  - Disco magnético
    - Disquete
    - Disco duro
      - Disco duro fijo o interno
      - Disco duro portátil o externo
  - Disco óptico (DO)
    - Disco compacto (CD o Compact Disc)
    - Disco Versátil Digital (DVD)
    - Disco Blu-ray (BD o Blu-ray Disc)
  - Disco magneto-óptico
    - Disco Zip (Iomega): 100 MB, tecnología magnética
    - Disquete SuperDisk de 3,5": 128 MB a 640 MB, tecnología magneto-óptica
      - LS-120
      - LS-240
    - Disco Jaz (Iomega): capacidad de 1 GB a 2 GB
  - Memoria Flash
    - Memoria USB
    - Tarjetas de memoria
    - Unidad de estado sólido

Desde un punto de vista básico y general, un dispositivo de entrada es el que provee el medio para permitir el ingreso de información, datos y programas (lectura); un dispositivo de salida brinda el medio para registrar la información y datos de salida (escritura); la memoria otorga la capacidad de almacenamiento, temporal o permanente (almacenamiento); y la CPU provee la capacidad de cálculo y procesamiento de la información ingresada (transformación).

Un periférico mixto es aquel que puede cumplir funciones tanto de entrada como de salida; el ejemplo más típico es el disco rígido o bien de estado sólido SSD (ya que en él se lee y se graba información y datos)

1.2. SOFTWARE

Se conoce como *software*, *logicial* o soporte lógico al sistema formal de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware. La interacción entre el *software* y el *hardware* hace operativo un ordenador (u otro dispositivo), es decir, el *software* envía instrucciones que el hardware ejecuta, haciendo posible su funcionamiento.

Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas, tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el llamado software de sistema, tal como el sistema operativo, que básicamente permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz con el usuario.

El *software*, en su gran mayoría, está escrito en lenguajes de programación de alto nivel, ya que son más fáciles y eficientes para que los programadores los usen, porque son más cercanos al Lenguaje natural respecto del lenguaje de máquina. Los lenguajes de alto nivel se traducen a lenguaje de máquina utilizando un compilador o un intérprete, o bien una combinación de ambos. El software también puede estar escrito en lenguaje ensamblador, que es de bajo nivel y tiene una alta correspondencia con las instrucciones de lenguaje máquina; se traduce al lenguaje de la máquina utilizando un ensamblador.

El **sistema operativo** de un equipo informático es un claro ejemplo de *software* de sistema. El usuario no opera directamente la OS, sino que interactúa con la interfaz gráfica de usuario o GUI proporcionada por este y mediante las aplicaciones instaladas sobre el sistema operativo.

Aparte de los sistemas operativos, dentro del *software* de sistema también se encuentran las siguientes clases de programas:

- Antivirus
- Utilidades de control de disco (herramientas de formateo y similares)
- Controladores de *hardware* o *drivers*
- Traductores de lenguajes informáticos
- Cargadores de programas
- Algunas BIOS y UEFI
- Gestores de arranque o *bootloaders*
- Hipervisores

Por otra parte, el ***software* de aplicación, *software* utilitario para usuario final o *apps*** (denominación generalista que comienza a coger tracción últimamente debido a la tecnología móvil), son todos **aquellos programas que ejecutan tareas concretas para las que han sido desarrollados específicamente**.

Finalmente, **el *software* de programación permite al usuario desarrollar sus propias herramientas a través de un lenguaje más cercano al humano**. Dentro de este apartado se encontrarían

herramientas como lenguajes de programación, compiladores, herramientas de *debugging* o depurado y similares.

Dado que hay mil y una aplicaciones posibles para el *software*, es difícil establecer una clasificación robusta y libre de interpretaciones según su utilidad. La taxonomía de los programas informáticos es un problema suficientemente complejo como para que en 2007 Microsoft se pusiese manos a la obra para crear un listado organizado de los mismos.

Otra posible clasificación del *software* se refiere a la forma en la que este se entrega al público. Atendiendo a esta característica podemos diferenciar los siguientes segmentos:

- ***Shareware***. Se refiere a los programas distribuidos en calidad de demostración; es decir, su uso el gratuito durante un periodo de prueba, al término de este es necesario adquirir una licencia para continuar usando el *software*. Hay una clara intencionalidad de venta, pues.

- ***Liteware***. En este caso hablamos de una variedad de *shareware* en la que el programa completo está deshabilitado hasta que se realiza la adquisición por parte del usuario, pero las funcionalidades básicas del *software* están disponibles sin necesidad de pagar.

- ***Freeware***. Se trata de *software* que se puede usar de forma totalmente gratuita, sin embargo, su distribución está sujeta a derechos de autor, licencias de distribución o protecciones comerciales.

- ***Public Domain Software* o programas de dominio público**. Es la evolución lógica del *freeware*, además de resultar gratuitos para el usuario, no hay ninguna restricción sobre su distribución.

- ***Open Source Software* o programas de código abierto**. Además de gratuitos y de libre distribución, los bloques de código que conforman este tipo de programas son públicos y su modificación queda a juicio de la comunidad de usuarios.

La terminación – ware, claramente asociada a la palabra *software*, se reconoce a menudo en varios grupos de programas cuyo fin tiene un efecto adverso sobre la experiencia de usuario. **Resumimos a continuación los tipos más comunes de *software* malicioso** que emplean esta terminación:

- ***Malware***. Se habla de *malware* al definir cualquier programa que tiene una intención maliciosa. Es un término generalista.

- ***Spyware***. Este tipo de *malware* está especializado en recopilar información sobre el equipo informático en el que se haya instalado desadvertidamente y sobre su usuario. Algunos de los objetivos de este tipo de programas son las costumbres de navegación, la información confidencial o las credenciales de acceso.

- ***Adware***. Hablamos de *adware* en el caso de que el *malware* esté diseñado para forzar anuncios de forma constante y habitual al usuario. Los desarrolladores de *adware* pueden salir beneficiados a través de la publicidad o mediante las propias ventas generadas.

- ***Ransomware***. Son programas que bloquean el funcionamiento del ordenador mientras no se pague un rescate. Se puede describir como un chantaje informático. En tiempos recientes el caso más mediático de *ransomware* ha sido WannaCry. La existencia de este tipo de *software* es suficiente justificación para mantener copias de seguridad redundantes de nuestros preciados archivos.

- ***Bloatware***. Se trata de programas innecesarios que se instalan durante la descarga de otro *software*. Dado que el usuario no requiere su uso, el código yace en las unidades de disco ocupando memoria. El desperdicio de espacio en memoria, junto con su instalación indeseada e inutilidad, son las características que lo validan como *software*

Al listado de *software* malicioso hay que añadir todo un abanico de virus informáticos: troyanos, gusanos, bombas lógicas, *recyclers*, *hoaxes* y otros.

El último *software* especial que vamos a introducir al lector es el *middleware*. También se conoce como **lógica de intercambio de información entre aplicaciones**, denominación que se justa mejor a la labor que desempeña: servir como **puente entre cualquier par de aplicaciones, paquetes de programas, OS, componente de *hardware* o redes**.

Un *software* de calidad es aquel que cumple con su funcionalidad, dispone de procedimientos de instalación sencillos, resulta previsible, su diseño prioriza la usabilidad y es extensible. La iteración de versiones que criben los errores de funcionamiento (*bugs* y *glitches*) y la certificación también aportan seguridad. Sin embargo, estas características no siempre son tan habituales en el mundo del *software*, ya que se trata de herramientas tremendamente complejas al nivel más básico.

Una fusión entre el *hardware* y el *software*: el *firmware*

El *firmware* es un punto de encuentro entre el *hardware* y el *software* en el sentido de que incluso **tratándose de líneas de código, datos e instrucciones intangibles, estas están estrictamente ligadas a un componente de *hardware***. Así, la mutabilidad inherente al *software* se pierde aquí, por eso en algunas ocasiones el *firmware* es referido como soporte lógico inalterable.

Algunos ejemplos de *firmware* son ciertas variedades de BIOS y UEFI, los RTAS (servicios de abstracción de tiempo de ejecución), los CFE (entornos comunes de *firmware*) y algunas otras tecnologías usadas en ordenadores específicos, *routers*, *firewalls* y NAS.

Clasificación

Si bien esta distinción es, en cierto modo, arbitraria, y a veces confusa, a los fines prácticos se puede clasificar al software en tres tipos:

- ***Software de sistema***: Su objetivo es desvincular adecuadamente al usuario y al programador de los detalles del sistema informático en particular que se use, aislándolo especialmente del procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc. El software de sistema le procura al usuario y programador adecuadas interfaces de alto nivel, controladores, herramientas y utilidades de apoyo que permiten el mantenimiento del sistema global. Incluye entre otros:

  - Sistemas operativos
  - Controladores de dispositivos

- Herramientas de diagnóstico
- Herramientas de corrección y optimización
- Servidores
- Utilidades

- ***Software de programación***: Es el conjunto de herramientas que permiten al programador desarrollar programas de informática, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluyen en forma básica:
  - Editores de texto
  - Compiladores
  - Intérpretes
  - Enlazadores
  - Depuradores
  - Entornos de desarrollo integrados (IDE): Agrupan las anteriores herramientas, usualmente en un entorno visual, de forma tal que el programador no necesite introducir múltiples comandos para compilar, interpretar, depurar, etc. Habitualmente cuentan con una avanzada interfaz gráfica de usuario (GUI).

- ***Software de aplicación***: Es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre muchos otros:
  - Aplicaciones para Control de sistemas y automatización industrial
  - Aplicaciones ofimáticas
  - Software educativo
  - Software empresarial
  - Bases de datos
  - Telecomunicaciones (por ejemplo Internet y toda su estructura lógica)
  - Videojuegos
  - Software médico
  - Software de cálculo numérico y simbólico.
  - Software de diseño asistido (CAD)
  - Software de control numérico (CAM)

2. Sistemas de almacenamiento de datos

El almacenamiento de datos es el proceso tecnológico por el cual se archiva, organiza y comparten los bytes de información que componen los archivos que se utilizan en el día a día como documentos de texto, imágenes, configuraciones, vídeos, sonidos y cualquier otra información en formato digital.

El almacenamiento de datos se realiza en dispositivos de hardware que disponen de unas características que los definen y que los hacen más adecuados para guardar copias de seguridad, dar acceso a los datos, transportar la información y otras funciones. Las principales características que definen a un sistema de almacenamiento de datos son:

- *Capacidad*. Mide la cantidad de datos que puede almacenar el sistema de almacenamiento, y es medida en bytes (Gigabytes o Terabytes, habitualmente, aunque con el Big Data se manejan incluso Petabytes).
- *Rendimiento*. Cómo de rápido y eficiente es el sistema de almacenamiento de datos.
- *Fiabilidad*. Es la disponibilidad de los datos cuando son solicitados, así como el hecho de disponer de una baja tasa de errores o fallos (por ejemplo, utilizando una configuración RAID).
- *Recuperabilidad*. Mide la capacidad del sistema para recuperar datos tras una pérdida, borrado, corrupción o cualquier otro incidente que impida el acceso a los mismos.

Se pueden clasificar en relación a su capacidad de almacenamiento o la manera en que acceden a los datos:

- ***Dispositivos de Almacenamiento Primario***: Se refiere a los dispositivos de almacenamiento masivos, caracterizados por siempre recibir energía eléctrica y guardar información en la memoria del ordenador.
- ***Dispositivos de Almacenamiento Secundario***: También denominados de almacenamiento secuencial, guardan la información en dispositivos externos hasta que el usuario lo requiera, por lo tanto son de menor velocidad que la memoria primaria.
- La ***unidad de disco junto con los discos que graba***, conforma un dispositivo de almacenamiento o unidad de almacenamiento (device drive).
- ***Acceso Secuencial***: En este caso para acceder a la información se debe leer registro por registro desde el inicio hasta llegar a la información en particular que deseamos encontrar. Se clasifican en: de desplazamiento, dispositivos de acoplamiento por carga, y de burbuja.
- ***Acceso Aleatorio***: El elemento de lectura accede directamente a la dirección donde encontramos la información físicamente a la que se pretende acceder, sin tener que pasar previamente por la almacenada entre el principio de la grabación y el lugar donde queda la información buscada.

Por ejemplo, una computadora tiene almacenamiento primario o principal (RAM y ROM) y secundario o auxiliar (disco rígido, disquete, pendrive, entre otros), sin embargo el almacenamiento secundario no es necesario para que inicie el equipo.

Los dispositivos que se abordan en este artículo están ordenados en base a su funcionamiento: magnéticos, ópticos, magneto-ópticos y de estado sólido. El almacenamiento en línea comprende características que orientan su descripción hacia artículos independientes.

- Dispositivos magnéticos
  - Unidad de cinta magnética
  - Unidad de disco flexible o «disquetera»
  - Unidad de disco rígido o duro
- Dispositivos ópticos
  - Unidad de CD-ROM o «lectora de CD»
  - Unidad de CD-R/RW o «grabadora/regrabadora» de CD-R/RW
  - Unidad de DVD-ROM o «lectora de DVD»
  - Unidad de DVD±R/RW o «grabadora de DVD±R/RW»
  - Unidad de BD, lectora o grabadora de discos Blu-ray
- Unidad de disco magneto-óptico
  - Unidad Zip
  - Unidad Jaz
  - Unidad SuperDisk
  - Orb Drive
- Unidad de estado sólido
  - Unidad de memoria flash
  - Unidad de tarjetas de memoria
- Otros dispositivos
  - ***Unidad de cinta perforada:*** se trata de un medio muy obsoleto, consistente en tarjetas o cintas de papel perforadas.
  - ***Almacenamiento en línea:*** hoy en día también debe hablarse de esta forma de almacenar información. Esta modalidad permite liberar espacio de los equipos de escritorio y trasladar los archivos a discos rígidos remotos provistos que garantizan normalmente la disponibilidad de la información. En este caso podemos hablar de dos tipos de almacenamiento en línea: un almacenamiento de corto plazo normalmente destinado a la transferencia de

grandes archivos vía web; otro almacenamiento de largo plazo, destinado a conservar información que normalmente se daría en el disco rígido del ordenador personal.

- Genéricamente, para agrupar un conjunto de unidades o dispositivos, se pueden denominar:
  - Unidad de cinta:
    - Cinta perforada.
    - Cinta magnética.
  - Unidad de disco:
    - Disco duro (unidad de disco duro, Hard-Disc Drive o HDD)
    - Disquete (disquetera)
    - Disco compacto (compactera o unidad de CD)
    - Disco Versátil Digital (unidad de DVD)
    - Disco Blu-ray (unidad de BD)

Habiendo abordado previamente los sistemas de almacenamiento de datos, resulta fundamental profundizar en el entendimiento de las unidades de almacenamiento,

Unidades de información básicas:

- **Bit (Shannon)**: El bit, en su definición más esencial y mínima, representa la unidad de información más básica en la informática y la teoría de la información. Representa un dígito en el sistema binario, pudiendo adoptar valores de 0 o 1. Es un acrónimo de "*binary digit*". Esta unidad se utiliza para medir la capacidad de almacenamiento y procesamiento en sistemas digitales.
- **Nat (Base e)**: el *nat* es una unidad de información basada en logaritmos naturales (base e). Menos común que el bit, se utiliza en contextos matemáticos y teóricos de la teoría de la información.
- **Trit (Base 3)**: un *trit* es la unidad de información en un sistema ternario, que utiliza tres símbolos (0, 1, 2). Aunque menos común en la práctica, su estudio es importante en la teoría de los sistemas de numeración y computación.
- **Hartley, Ban o Dit (Base 10)**: esta unidad se utiliza en sistemas de numeración decimal. Un *hartley* equivale a la cantidad de información que produce un evento de diez resultados igualmente probables.

Qubit (Cuántico):

- El *qubit* es la unidad fundamental de información en la computación cuántica. A diferencia del bit clásico, un *qubit* puede existir simultáneamente en una superposición de estados 0 y 1. Esta propiedad permite a los sistemas cuánticos realizar cálculos de manera más eficiente para ciertos problemas complejos.

Sistemas de Numeración y su Relación con las Unidades de Información:

- **Sistema binario**: en este sistema, solo se utilizan dos dígitos (0 y 1). Un bit representa un dígito binario. La capacidad de las memorias digitales se mide en múltiplos de bits.

- **Sistema octal**: utiliza ocho símbolos (del 0 al 7). En informática, se emplea ocasionalmente por su simplicidad al representar grupos de bits, aunque el sistema hexadecimal es más común para este propósito.
- **Nibble**: Un conjunto de cuatro bits. Importante en arquitecturas de computadoras y en la codificación hexadecimal.

Múltiplos de *bytes*:

- El vocablo byte fue acuñado por Werner Buchholz en 1957 durante las primeras fases de diseño del IBM 7030 Stretch. El cual adopto un tamaño fijo de 8 bits. El byte también es llamado *octeto*.
- En el contexto de la capacidad de almacenamiento, los bytes se utilizan como la unidad estándar. Un byte se compone de ocho bits. Los múltiplos de bytes, como kilobyte (kB), megabyte (MB), gigabyte (GB), etc., se utilizan comúnmente para medir capacidades de almacenamiento y transferencia de datos. Existen dos convenciones: una basada en múltiplos de 1000 (Sistema Internacional) y otra en múltiplos de 1024 (ISO/IEC), siendo esta última más prevalente en contextos informáticos.

MÚLTIPLOS DE BYTES			
Sistema Internacional (decimal)		ISO/IEC 80000-13 (binario)	
Múltiplo (símbolo)	**SI**	**Múltiplo (símbolo)**	**ISO/IEC**
kilobyte (kB)	10^3	kibibyte (KiB)	2^{10}
megabyte (MB)	10^6	mebibyte (MiB)	2^{20}
gigabyte (GB)	10^9	gibibyte (GiB)	2^{30}
terabyte (TB)	10^{12}	tebibyte (TiB)	2^{40}
petabyte (PB)	10^{15}	pebibyte (PiB)	2^{50}
exabyte (EB)	10^{18}	exbibyte (EiB)	2^{60}
zettabyte (ZB)	10^{21}	zebibyte (ZiB)	2^{70}
yottabyte (YB)	10^{24}	yobibyte (YiB)	2^{80}

3. Sistemas operativos

Un sistema operativo (SO o, frecuentemente, OS —del inglés *operating system*—) es el conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software. Estos programas se ejecutan en modo privilegiado respecto de los restantes.

Uno de los propósitos del sistema operativo que gestiona el núcleo intermediario consiste en gestionar los recursos de localización y protección de acceso del hardware, hecho que alivia a los programadores de aplicaciones de tener que tratar con estos detalles. La mayoría de aparatos electrónicos que utilizan microprocesadores para funcionar, llevan incorporado un sistema operativo (teléfonos móviles, reproductores de DVD, computadoras, enrutadores, etc.). En cuyo caso, son manejados mediante una interfaz gráfica de usuario, un gestor de ventanas o un entorno de escritorio, si es un celular, mediante una consola o control remoto si es un DVD y, mediante una línea de comandos o navegador web si es un enrutador.

El sistema operativo de escritorio dominante es Microsoft Windows con una cuota de mercado de alrededor del 82,74%. macOS de Apple Inc. ocupa el segundo lugar (13,23%), y las variedades de GNU/Linux están colectivamente en tercer lugar (1,57%). En el sector móvil (incluidos teléfonos inteligentes y tabletas), la participación de Android es de hasta un 70% en el año 2017. Las distribuciones Linux son dominantes en los sectores de servidores y supercomputación. Existen otras clases especializadas de sistemas operativos, como los sistemas integrados y en tiempo real, para muchas aplicaciones.

Clasificación

Administración de tareas

- *Monotarea*: Solamente permite ejecutar un proceso (aparte de los procesos del propio SO) en un momento dado. Una vez que empieza a ejecutar un proceso, continuará haciéndolo hasta su finalización y/o interrupción.
- *Multitarea*: Es capaz de ejecutar varios procesos al mismo tiempo. Este tipo de SO normalmente asigna los recursos disponibles (CPU, memoria, periféricos) de forma alternada a los procesos que los solicitan, de manera que el usuario percibe que todos funcionan a la vez, de forma concurrente.

Administración de usuarios

- *Monousuario*: Solo permite ejecutar los programas de un usuario al mismo tiempo.
- Multiusuario: Permite que varios usuarios ejecuten simultáneamente sus programas, *accediendo* a la vez a los recursos de la computadora. Normalmente estos sistemas operativos utilizan métodos de protección de datos, de manera que un programa no pueda usar o cambiar los datos de otro usuario.

Manejo de recursos

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

Ejemplos:

- Windows
- Mac OS
- Unix
- Solaris
- FreeBSD
- OpenBSD
- Android-x86 (GNU/Linux)
- Chrome OS (GNU/Linux)
- Debian GNU/Linux (GNU/Linux)
- Gentoo Linux (GNU/Linux)
- SUSE Linux (GNU/Linux)
- Red Hat Enterprise Linux (GNU/Linux)
- Ubuntu Linux (GNU/Linux)
- Elementary OS (GNU/Linux)
- Sabayon (GNU/Linux)
- Wave OS
- webOS
- Haiku (BeOS)
- Plan 9
- Freespire
- HP-UX
- ReactOS
- BeOS
- Kali Linux (GNU/Linux)
- LindowsOS/Linspire

Funciones principales

Algunas de las funciones principales de un sistema operativo son las siguientes:

- Gestionar la memoria de acceso aleatorio y ejecutar las aplicaciones, designando los recursos necesarios: El sistema operativo es responsable de administrar eficientemente la memoria RAM y asignar los recursos necesarios a las aplicaciones en ejecución. Además de asignar memoria, también gestiona la liberación de memoria cuando una aplicación ya no la necesita.

- Administrar la CPU gracias a un algoritmo de programación: El sistema operativo coordina el uso de la CPU entre las diferentes tareas y procesos que se ejecutan en el sistema. Utiliza algoritmos de programación para determinar el orden y la prioridad de ejecución de los procesos, asegurando un uso equitativo de los recursos de la CPU.

- Gestionar las entradas y salidas de datos a través de los periféricos: Además de direccionar las entradas y salidas de datos, el sistema operativo proporciona controladores (drivers) para interactuar con los periféricos de entrada y salida, como teclados, mouse, impresoras, discos duros externos, entre otros. Estos controladores permiten que los dispositivos se comuniquen correctamente con el sistema operativo y las aplicaciones.

- Administrar la información para el buen funcionamiento del sistema: El sistema operativo gestiona información esencial para el funcionamiento del sistema, como la tabla de procesos, la tabla de archivos abiertos y otros datos relevantes. Además, realiza tareas de monitoreo y gestión del rendimiento para asegurar un funcionamiento óptimo del sistema.

- Dirigir las autorizaciones de uso para los usuarios: El sistema operativo proporciona un mecanismo de autenticación y autorización para garantizar que los usuarios accedan solo a los recursos y funciones para los cuales tienen permisos. Esto incluye la gestión de cuentas de usuario, contraseñas y asignación de privilegios.

- Administrar los archivos: El sistema operativo maneja las operaciones relacionadas con la gestión de archivos, como la creación, modificación, eliminación y acceso a los archivos en el sistema de almacenamiento. Esto implica la organización de los archivos en directorios o carpetas, el control de acceso a los archivos y la implementación de mecanismos de seguridad para proteger la integridad y confidencialidad de la información.

4. Nociones básicas de seguridad informática

4.1. NOCIONES BÁSICAS

La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndose así en información privilegiada.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solamente se encarga de la seguridad en el medio informático, pero, por cierto, la información puede encontrarse en diferentes medios o formas, y no exclusivamente en medios informáticos.

La seguridad informática también se refiere a la práctica de prevenir los ataques maliciosos, a las computadoras y los servidores, a los dispositivos móviles, a los sistemas electrónicos, a las redes y los datos, etc.

En resumen, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- *La infraestructura computacional*: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- *Los usuarios*: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.
- *La información*: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

4.2. ESQUEMA NACIONAL DE SEGURIDAD

El **Real Decreto 311/2022**, de 3 de mayo, regula el Esquema Nacional de Seguridad (en adelante, ENS).

El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

4.2.1. Principios básicos del Esquema Nacional de Seguridad

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.

b) Gestión de la seguridad basada en los riesgos.

c) Prevención, detección, respuesta y conservación.

d) Existencia de líneas de defensa.

e) Vigilancia continua.

f) Reevaluación periódica.

g) Diferenciación de responsabilidades.

4.2.2. La seguridad como un proceso integral

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

4.2.3. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

a) Confidencialidad [C].

b) Integridad [I].

c) Trazabilidad [T].

d) Autenticidad [A].

e) Disponibilidad [D].

4.2.4. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: **BAJO, MEDIO O ALTO**. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) NIVEL BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio limitado:

1. La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2. Causar un daño menor en los activos de la organización.
3. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4. Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
5. Otros de naturaleza análoga.

b) NIVEL MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones

de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio grave:

1. La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2. Causar un daño significativo en los activos de la organización.
3. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4. Causar un perjuicio significativo a algún individuo, de difícil reparación.
5. Otros de naturaleza análoga.

c) **NIVEL ALTO.** Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1. ° La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
2. ° Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
3. ° El incumplimiento grave de alguna ley o regulación.
4. ° Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5. ° Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4.2.5. Determinación de la categoría de seguridad de un sistema de información

Se definen tres categorías de seguridad: **BÁSICA, MEDIA y ALTA.**

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

4.2.6. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías **CCN-STIC, del CCN**, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

4.2.7. Medidas de Seguridad

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.

b) La categoría de seguridad del sistema de información a proteger.

Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

4.3. AMENAZAS PARA LA SEGURIDAD

En esta era de avances tecnológicos rápidos y omnipresentes, la seguridad informática se ha convertido en un pilar esencial para la protección de datos y sistemas. Las amenazas a la seguridad informática vienen en diversas formas, cada una con su mecanismo de acción único y potencial para causar daño. Abordaremos algunas de las amenazas más comunes y perjudiciales: virus, gusanos, troyanos, *ransomware y spyware*.

El término malware (*software* malicioso): es un término general que engloba varios tipos de software diseñados con intenciones malévolas. Su objetivo es infiltrarse en sistemas sin autorización, causando daño, robando datos, o provocando disfunciones en el sistema. Entre las variantes más comunes de malware se encuentran los virus, gusanos, troyanos, ransomware, y spyware. Cada uno de estos tiene un modo de operación distinto y propósitos específicos, desde la simple molestia hasta el robo de información confidencial o la inutilización de sistemas.

Un **virus informático** es un tipo de malware que se replica a sí mismo al insertar sus propios códigos en otros programas informáticos. Al ejecutar el programa infectado, se activa el virus, permitiendo su propagación a otros programas y sistemas. Los virus pueden causar daños variados, desde la simple molestia hasta la corrupción de datos o el fallo completo del sistema afectado.

El **phishing** se utiliza para engañar a los usuarios y obtener información confidencial de forma fraudulenta. Por lo general, implica el envío de correos electrónicos o mensajes que parecen provenir de fuentes legítimas, como bancos o empresas conocidas, solicitando al destinatario que proporcione información personal, como contraseñas o números de tarjetas de crédito. Estos mensajes suelen contener enlaces a sitios web falsificados que imitan a los legítimos.

El ***sniffing*** se refiere a la práctica de interceptar y analizar paquetes de datos que se transmiten a través de una red. Los "*sniffers*" pueden ser utilizados tanto para fines legítimos, como la monitorización y el mantenimiento de redes, como para propósitos maliciosos, como el robo de información transmitida, incluyendo contraseñas, mensajes de correo electrónico y otros datos sensibles.

El ***spoofing*** implica la falsificación de la identidad de una entidad en una red. Puede darse en varias formas, incluyendo la suplantación de direcciones IP (IP *spoofing*), la falsificación de direcciones de correo electrónico (email *spoofing*), o la falsificación de sitios web (web *spoofing*). Su propósito es engañar a los receptores para que crean que están interactuando con una fuente legítima y confiable, lo que puede facilitar el robo de información o la distribución de malware.

Los **gusanos** son un tipo de malware autónomo que se replica y se propaga a través de redes informáticas sin la necesidad de adjuntarse a un programa específico. A diferencia de los virus, que requieren la intervención humana para propagarse (como ejecutar un programa infectado), los gusanos pueden diseminarse por sí mismos, explotando vulnerabilidades de seguridad en los sistemas a los que acceden.

Un **troyano** es un tipo de malware que se disfraza como un software legítimo o se incrusta en uno. A diferencia de los virus y gusanos, no se replica por sí mismo, pero una vez activado, puede permitir a los atacantes acceder al sistema infectado. Los troyanos pueden ser utilizados para robar información, espiar al usuario, o crear una puerta trasera en el sistema infectado.

El ***ransomware*** es un tipo de malware que cifra los datos del usuario, bloqueando el acceso a ellos hasta que se paga un rescate. Esta amenaza se ha vuelto particularmente prominente y dañina, con ataques dirigidos tanto a individuos como a grandes organizaciones. El ransomware representa un grave riesgo de pérdida de datos críticos y de interrupciones significativas en las operaciones comerciales y personales.

El **INCIBE (Instituto Nacional de Ciberseguridad),** incluye otros conceptos en su web como:

- **Adware**: aquel software que ofrece publicidad no deseada o engañosa. Estos anuncios pueden aparecer en el navegador con pop-ups o ventanas con gran contenido visual, e incluso audios. Se reproducen de manera automática con el fin de generar ganancias económicas a los creadores. En ocasiones este software provoca que el buscador predilecto del usuario sea cambiado por otro, generando errores en las búsquedas deseadas y entorpeciendo la experiencia de navegación del usuario.

- **Spyware**: tipo de virus se encarga de recopilar de manera fraudulenta la información sobre la navegación del usuario, además de datos personales y bancarios. Un ejemplo de este tipo de virus son los *Keyloggers*, los cuales monitorizan toda nuestra actividad con el teclado (teclas que se pulsan), para luego enviarla al ciberdelincuente.

ESQUEMA DE LA UNIDAD