Colegio Concertado Virgen Blanca (León) – Fundación Educere

Departamento de Tecnologías de la Información y la Comunicación

INTERNET

Realizado por el alumno Marcos Álvarez Gómez

Para el Profesor D. Oliver Fernández González

Febrero 2025

ÍNDICE

1. DEFINICIÓN DE INTERNET

Internet es una red global de comunicaciones que conecta millones de dispositivos alrededor del mundo, permitiendo el intercambio de información, la interacción digital, y el acceso a servicios como la World Wide Web, correo electrónico, redes sociales y más. Funciona mediante una infraestructura de cables, satélites y servidores, utilizando el protocolo TCP/IP para transmitir datos entre los dispositivos conectados. Internet es una herramienta fundamental que ha transformado todos los aspectos de la vida moderna, incluyendo el trabajo, la educación, la cultura, y la economía.

2. HISTORIA DE INTERNET

La historia de Internet es el resultado de décadas de investigación militar, científica y tecnológica que comenzaron en plena Guerra Fría. En los años cincuenta y sesenta, Estados Unidos temía que un ataque soviético pudiera destruir los centros de comunicaciones tradicionales. Este escenario llevó a los estrategas militares a plantearse una cuestión fundamental: cómo crear una red de comunicaciones que pudiera seguir funcionando incluso si una parte significativa de ella era destruida.

En este contexto se creó la ARPA, más tarde conocida como DARPA, una agencia del Departamento de Defensa de Estados Unidos dedicada a desarrollar tecnologías avanzadas. Uno de los investigadores más influyentes en esta etapa temprana fue Paul Baran, quien trabajó en la RAND Corporation. Baran propuso un sistema de comunicaciones distribuido, en el que la información no circulara en bloques completos, sino fragmentada en pequeñas unidades que pudieran viajar por múltiples rutas hasta llegar a su destino. Este principio, conocido como conmutación de paquetes, se convertiría en la base indispensable para el funcionamiento de Internet.

La conmutación de paquetes no fue resultado del trabajo de un único investigador. Durante la década de 1960, expertos de diferentes países desarrollaron ideas complementarias. Donald Davies, del National Physical Laboratory del Reino Unido, también ideó un sistema de comunicación basado en paquetes y fue quien introdujo el término “packet”.

Por su parte, Leonard Kleinrock, investigador en la Universidad de California en Los Ángeles (UCLA), aportó el soporte matemático que demostraba que esta forma de comunicación era eficiente y viable. La unión de estos avances permitió que DARPA comenzara a plantearse la creación de una red experimental basada en estos principios.

Ese proyecto se materializó en 1969 bajo el nombre de ARPANET, considerada el antecesor directo de Internet. El 29 de octubre de aquel año tuvo lugar un hecho histórico: el primer envío de datos entre ordenadores conectados a distancia. El mensaje se transmitió desde UCLA hasta el Stanford Research Institute. La intención era enviar la palabra “LOGIN”, pero la red se cayó tras enviar solo las dos primeras letras: “LO”. A pesar del fallo, ese momento marcó el nacimiento oficial de Internet. ARPANET se inició con solo cuatro nodos interconectados: UCLA, Stanford Research Institute, la Universidad de California en Santa Bárbara y la Universidad de Utah. En los años siguientes, múltiples universidades y centros de investigación se incorporaron a la red, ampliando su alcance.

A lo largo de la década de 1970 surgió un desafío decisivo para la expansión de Internet: la necesidad de que todos los equipos conectados utilizaran un conjunto común de reglas para comunicarse.

En respuesta a este problema, Vinton Cerf y Robert Kahn desarrollaron un conjunto de protocolos llamados TCP/IP. Estos protocolos permitían que dispositivos de diferentes redes y arquitecturas pudieran intercambiar información sin conflictos. Tras años de desarrollo, el 1 de enero de 1983 ARPANET adoptó oficialmente TCP/IP. Este día es considerado por muchos historiadores como el nacimiento del Internet moderno, ya que por primera vez existía un estándar universal que permitía la interconexión global de redes.

Mientras ARPANET se desarrollaba, surgían otras redes que contribuyeron al avance de Internet. En el Reino Unido, la NPL Network desarrollada por Donald Davies experimentaba con el uso de paquetes. En Francia, el proyecto CYCLADES, dirigido por Louis Pouzin, aportó ideas cruciales sobre la transmisión descentralizada de datos. Paralelamente aparecieron redes como UUCP y Usenet, que permitían el intercambio de mensajes entre ordenadores, y BITNET, que facilitó la comunicación entre universidades. Todas estas redes influyeron directa o indirectamente en la evolución de Internet.

Uno de los avances más importantes de esta época fue el nacimiento del correo electrónico. En 1971, Ray Tomlinson creó el sistema de e-mail moderno al permitir que los mensajes pudieran enviarse de un ordenador a otro a través de ARPANET. Tomlinson escogió el símbolo "@" para separar el nombre del usuario del nombre del servidor. Desde su aparición, el correo electrónico se convirtió rápidamente en la aplicación más utilizada en ARPANET y en el primer servicio popular de Internet.

Durante los años ochenta se produjo una expansión significativa más allá del ámbito militar. ARPANET se dividió en dos: la parte militar pasó a llamarse MILNET, mientras que ARPANET permaneció como red académica y de investigación. Instituciones como la National Science Foundation (NSF) promovieron la creación de nuevas redes y facilitaron la conexión de universidades e instituciones científicas de todo el mundo. Además, surgieron organizaciones como Internet Society y la IETF, responsables de desarrollar y mantener los estándares técnicos de la red. Al mismo tiempo, comenzaron a aparecer los primeros proveedores de servicios de Internet, que permitían el acceso comercial a la red.

A finales de los años ochenta y principios de los noventa se produjo un cambio decisivo: la creación de la World Wide Web. Aunque mucha gente confunde la Web con Internet, lo cierto es que Internet ya existía antes de que aparecieran las páginas web. En 1989, Tim Berners-Lee, un investigador del CERN, propuso un sistema que permitiera enlazar documentos mediante hipertexto. Para lograrlo creó tres elementos fundamentales: el protocolo HTTP para acceder a los documentos, el lenguaje HTML para estructurarlos y las URL para identificarlos. También desarrolló el primer servidor web y el primer navegador, llamado WorldWideWeb. En 1991 la Web se abrió al público, transformando Internet en una plataforma accesible para cualquier persona.

El verdadero despegue de Internet comenzó en 1993, cuando apareció Mosaic, el primer navegador gráfico ampliamente utilizado. Mosaic facilitó el uso de Internet incluso a quienes no tenían conocimientos técnicos. Sus creadores fundaron posteriormente Netscape, cuyo navegador Netscape Navigator dominó el mercado durante varios años. La competencia llegó pronto con Microsoft, que lanzó Internet Explorer en 1995. Esta "guerra de navegadores" impulsó la rápida expansión de la Web. En esta misma época surgieron empresas que hoy son gigantes tecnológicos: Yahoo (1994), Amazon (1995), eBay (1995), y servicios como Hotmail (1996). También aparecieron los primeros buscadores modernos, que facilitaron encontrar información en un océano de páginas web cada vez mayor.

El entusiasmo tecnológico llevó a un crecimiento masivo de empresas relacionadas con Internet, lo que acabó provocando la llamada "burbuja puntocom" a finales de los años noventa. Miles de compañías tecnológicas recibieron inversiones exageradas sin contar con modelos de negocio sostenibles. En el año 2000 la burbuja estalló, provocando quiebras masivas. Sin embargo, pese a la crisis económica, Internet no dejó de crecer. De hecho, en 1998 apareció Google, cuyo algoritmo revolucionó la búsqueda en la Web y acabó dominando el mercado.

Los años 2000 marcaron el inicio de la llamada Web 2.0, un término que define la transición desde páginas estáticas hacia plataformas dinámicas basadas en la participación del usuario. En este período surgieron servicios que redefinieron la comunicación y el acceso a la información. Wikipedia apareció en 2001, seguida de redes sociales como Facebook en 2004, YouTube en 2005 y Twitter en 2006. La Web se convirtió en un espacio colaborativo donde los usuarios no solo consumían información, sino que también la generaban mediante blogs, foros, plataformas de vídeo, comentarios y redes sociales.

A partir de la década de 2010 Internet sufrió otra transformación decisiva: la irrupción de los teléfonos inteligentes. La llegada del iPhone en 2007 y del sistema Android en 2008

permitió que millones de personas pudieran conectarse a Internet desde cualquier lugar. Por primera vez, el tráfico móvil superó al tráfico generado desde ordenadores. Las redes sociales se convirtieron en el principal medio de comunicación para gran parte de la población, mientras que el comercio electrónico, el vídeo en streaming y las aplicaciones móviles crecieron vertiginosamente. Plataformas como Netflix, Spotify, Instagram o WhatsApp se integraron en la vida diaria de millones de personas.

Finalmente, en los años recientes, Internet ha entrado en una nueva etapa marcada por el uso masivo de la inteligencia artificial, el internet de las cosas, las redes 5G y el consumo de datos a gran escala. Aplicaciones como TikTok transformaron el consumo de contenido mediante algoritmos que personalizan la experiencia de cada usuario. La inteligencia artificial generativa, como la que impulsa herramientas capaces de crear textos, imágenes o vídeos, ha modificado radicalmente la manera en que interactuamos con la red.

Al mismo tiempo, la computación en la nube, las criptomonedas, el blockchain y los dispositivos conectados han ampliado aún más las posibilidades de Internet. En la actualidad, las fronteras entre el mundo digital y el físico prácticamente han desaparecido, y la mayoría de actividades sociales, económicas y culturales dependen directa o indirectamente de Internet.

3. TARJETA DE RED Y MÓDEM

3.1 Tarjeta de Red (NIC):

Una Tarjeta de Red, también llamada NIC (Network Interface Card), es el componente del ordenador que permite que un dispositivo se conecte a una red, ya sea una red local (LAN) o internet. Su función principal es actuar como el intermediario entre el ordenador y el medio de transmisión por el cual viajan los datos, ya sea un cable Ethernet, ondas de radio en el caso del WiFi o fibra óptica en algunos sistemas avanzados. Sin una tarjeta de red, un ordenador no podría comunicarse con otros equipos ni acceder a recursos compartidos como impresoras, servidores o conexiones a internet.

La tarjeta de red es responsable de convertir la información que genera el ordenador en señales que puedan viajar por la red. Estas señales pueden ser eléctricas, ópticas o electromagnéticas, según el tipo de conexión. De igual forma, también recibe las señales provenientes de la red y las convierte de nuevo en información comprensible para el sistema operativo.

Cada tarjeta de red tiene una dirección física única llamada dirección MAC (Media Access Control). Esta dirección es un identificador compuesto por 48 bits y se utiliza para reconocer de forma inequívoca el dispositivo dentro de una red. Las direcciones MAC están grabadas de fábrica por el fabricante y no se repiten en ningún otro dispositivo del mundo, lo que permite una organización precisa en la comunicación local de los equipos. Además, la dirección MAC es esencial en el proceso de comunicación dentro de redes Ethernet y WiFi, porque determina cómo se envían y reciben los paquetes.

El funcionamiento de la tarjeta de red se basa en el modelo OSI, especialmente en las dos capas inferiores: la capa física y la capa de enlace de datos. En la capa física, la tarjeta se encarga de transmitir y recibir señales por el medio de comunicación. En la capa de enlace de datos, gestiona la estructura de los paquetes, los controles de errores, la sincronización

y la interacción con la red mediante protocolos como Ethernet, WiFi (IEEE 802.11) o Bluetooth. En otras palabras, la tarjeta de red ejecuta tareas esenciales para que los datos viajen correctamente y sin interferencias.

Existen dos grandes tipos de tarjetas de red: las inalámbricas (WiFi) y las cableadas (Ethernet). Las tarjetas Ethernet utilizan cables de red, generalmente de tipo RJ45, y permiten velocidades estables y altas, desde 10 Mbps hasta varios gigabits por segundo. Son muy utilizadas en ordenadores de sobremesa, portátiles con adaptadores o servidores que requieren estabilidad y baja latencia. Las tarjetas WiFi, en cambio, permiten conectar dispositivos a través de ondas de radio y ofrecen mayor comodidad al no requerir cables, aunque suelen ser más sensibles a interferencias, distancia y obstáculos. Los estándares WiFi han evolucionado desde el 802.11b hasta el moderno WiFi 6 y WiFi 6E, aumentando la velocidad, estabilidad y seguridad.

Las tarjetas de red pueden venir integradas en la placa base del ordenador, lo que es muy común actualmente en ordenadores de sobremesa y portátiles, o pueden instalarse como tarjetas independientes mediante puertos PCI, PCIe o USB. Las integradas son suficientes para la mayoría de usuarios, pero las tarjetas dedicadas ofrecen mejores prestaciones, como mayor velocidad, mejor calidad de señal y funciones avanzadas como soporte para VLAN, gestión remota o controladores optimizados.

Otra función importante de las tarjetas de red es el control del flujo de datos. Esto incluye técnicas como la detección de colisiones en redes Ethernet antiguas o la modulación de la señal en tarjetas WiFi. También participan en procesos como la fragmentación y el empaquetado de datos, la verificación mediante CRC (Cyclic Redundancy Check) y la retransmisión de información cuando existe un error en la comunicación.

Las tarjetas NIC modernas incluyen hardware adicional como procesadores internos, controladores avanzados o buffers de memoria para gestionar más eficientemente los datos. Esto se conoce como "offloading", porque permite descargar al procesador principal del trabajo de gestionar paquetes, reduciendo el uso de la CPU y aumentando el rendimiento del sistema. Esta característica es muy apreciada en servidores y equipos que manejan grandes cantidades de tráfico en red.

En cuanto a la instalación, las tarjetas de red requieren controladores (drivers) para funcionar correctamente. Estos controladores permiten al sistema operativo interactuar con la tarjeta de red y aprovechar sus funciones. Los drivers suelen venir instalados por defecto en sistemas como Windows, macOS o Linux, aunque algunos modelos avanzados requieren descargas adicionales del fabricante.

La seguridad también forma parte del funcionamiento de una tarjeta de red. Aunque la mayor parte de la seguridad se gestiona a niveles superiores (como los protocolos de cifrado y los firewalls), la NIC puede soportar funciones como filtros de direcciones MAC, limitación de tráfico, autenticación a redes inalámbricas y gestión de paquetes sospechosos.

En resumen, la tarjeta de red es un componente esencial en cualquier dispositivo moderno, ya que permite la conexión y comunicación a través de redes. Su evolución ha sido clave para el desarrollo de internet y las comunicaciones actuales, proporcionando mayores velocidades, estabilidad y seguridad. Sin una tarjeta NIC, ningún ordenador podría acceder a la red, interactuar con otros dispositivos ni realizar actividades básicas como navegar por internet, enviar correos o usar servicios en la nube.

3.2 Módem:

El módem es un dispositivo fundamental en la historia y el funcionamiento de internet porque permite la comunicación entre redes digitales y líneas analógicas. Su nombre proviene de la combinación de dos procesos: “modulación” y “demodulación”. Estas dos funciones explican su propósito principal: convertir las señales digitales generadas por un ordenador en señales analógicas capaces de viajar por medios como líneas telefónicas tradicionales, y luego volver a convertir esas señales analógicas en digitales para que el ordenador receptor las entienda. Sin este proceso, los primeros ordenadores no hubieran podido comunicarse a través de infraestructuras creadas originalmente para la voz humana.

Los primeros módems aparecieron en la década de 1950, utilizados por el ejército de los Estados Unidos para transmitir datos estratégicos a través de líneas telefónicas. Eran enormes, lentos y extremadamente rudimentarios, pero introdujeron el concepto que más tarde permitiría la expansión de internet a nivel doméstico. En los años 60 y 70 empezaron a usarse en universidades y centros de investigación, donde se conectaban terminales remotos a grandes mainframes. Sus velocidades eran muy reducidas, normalmente entre 300 y 1200 bits por segundo, pero fueron suficientes para transmitir información simple.

En la década de 1980 los módems comenzaron a popularizarse en hogares y pequeñas empresas, convirtiéndose en una herramienta clave para la aparición de servicios como los BBS (Bulletin Board Systems), que fueron los precursores de los foros y páginas web actuales. Estos módems de marcado telefónico, conocidos como "dial-up", utilizaban la línea telefónica analógica y requerían que el usuario “marcara” un número para establecer la conexión. Era común escuchar sonidos característicos durante este proceso, resultado de la negociación entre módems para acordar velocidad y protocolos. Las velocidades aumentaron gradualmente hasta alcanzar los 56 Kbps, que fue el límite técnico de las líneas analógicas.

El funcionamiento del módem dial-up consiste en que el dispositivo toma los datos digitales del ordenador y los convierte en tonos analógicos que pueden transmitirse por la red telefónica. Cuando llegan al módem receptor, este interpreta los tonos y reconstruye la información original. Este proceso presenta limitaciones importantes: las líneas telefónicas no están diseñadas para transmitir datos de alta frecuencia, las interferencias afectan fácilmente la comunicación y, además, la línea queda ocupada mientras se navega. Por eso, durante años, no se podía hablar por teléfono y navegar a la vez.

Con la llegada de nuevas tecnologías surgieron otros tipos de módems, como los módems ADSL. Estos dispositivos ya no transforman señales digitales en analógicas, sino que aprovechan frecuencias no utilizadas de la línea telefónica para enviar datos de manera digital. Esto permitió velocidades mucho más altas que el dial-up y la posibilidad de usar el teléfono simultáneamente. Los módems ADSL utilizan filtros, conocidos como splitters o microfiltros, para separar las frecuencias de voz y de datos. De esta forma, la conexión se vuelve más estable, rápida y continua, sin necesidad de "marcar" cada vez que se quería acceder a internet.

Más adelante aparecieron los módems de cable, que funcionan a través de redes de televisión por cable. A diferencia de los anteriores, estos módems utilizan infraestructura coaxial, capaz de transportar mayor ancho de banda. La señal llega al hogar a través del cable de televisión, y el módem se encarga de convertirla en datos digitales que el ordenador o el router pueden usar. Las velocidades de estos módems superaban ampliamente a las del ADSL y siguen siendo una opción común en muchas zonas urbanas.

En los últimos años también se han extendido los módems de fibra óptica. La fibra óptica transmite datos mediante pulsos de luz y no mediante señales eléctricas o analógicas, lo que permite velocidades muy altas, estabilidad, baja latencia y una capacidad de transmisión enorme. En las conexiones de fibra, el módem actúa como un ONT (Optical Network Terminal), un dispositivo que convierte la señal luminosa de la fibra en una señal eléctrica digital para el router o el ordenador. Aunque técnicamente cumple la función de

un módem, su tecnología es mucho más avanzada y no utiliza modulación analógica tradicional.

Los módems también pueden ser internos o externos. Los módems internos se instalan dentro del ordenador mediante puertos PCI, mientras que los externos se conectan por USB o por cable de red a un router. Los externos ofrecen ventajas como mayor facilidad de instalación, mejor refrigeración, luces que indican el estado de la conexión y una mayor compatibilidad. Los internos eran más populares en los años 90 y principios de los 2000, especialmente para conexión dial-up.

Es común confundir módem con router, pero no son lo mismo. El módem se encarga de comunicar la red del hogar con el proveedor de internet, transformando la señal para que sea utilizable por los dispositivos. El router, en cambio, distribuye la conexión entre varios dispositivos, gestiona direcciones IP locales y crea la red WiFi. Muchos dispositivos modernos combinan ambas funciones en un único aparato (módem-router), pero internamente siguen cumpliendo tareas distintas.

Los módems han ido incorporando cada vez más funciones de seguridad, como filtros, diagnóstico de línea, cifrado en conexiones inalámbricas (cuando están integrados con un router), protección contra interferencias y actualizaciones de firmware. Sin embargo, la seguridad depende principalmente del router y de los protocolos de la red, más que del módem en sí.

En resumen, el módem es un componente esencial que ha permitido la evolución de internet desde sus primeras versiones analógicas hasta las conexiones de altísima velocidad actuales. A lo largo de su historia, ha transformado datos digitales en señales compatibles con diferentes infraestructuras de comunicación, adaptándose a los avances tecnológicos de cada época. Su papel ha sido clave para hacer posible el acceso a internet

en hogares y empresas, y sigue siendo un elemento imprescindible en las conexiones modernas, especialmente en fibra óptica y cable.

4. TIPOS DE CONEXIONES A INTERNET

Las conexiones a internet han evolucionado de forma constante desde los primeros métodos de transmisión analógica hasta las modernas redes de fibra óptica de alta velocidad. Cada tipo de conexión utiliza tecnologías distintas para transportar datos entre el usuario y el proveedor de servicios, y cada una presenta características propias en cuanto a velocidad, estabilidad, latencia, capacidad de descarga y fiabilidad. Comprender estos tipos de conexión permite entender mejor cómo ha progresado internet y por qué algunos métodos han sido sustituidos por otros más eficientes.

Uno de los primeros tipos de conexión ampliamente utilizados fue la conexión por línea telefónica analógica, conocida como dial-up. Este sistema utilizaba un módem que transformaba los datos digitales del ordenador en tonos analógicos. Estos tonos viajaban por la línea telefónica tradicional y permitían establecer una comunicación con el proveedor de internet. La velocidad era extremadamente limitada, llegando como máximo a 56 Kbps en condiciones ideales. Además, esta conexión ocupaba completamente la línea telefónica, de modo que no se podía hablar por teléfono mientras se navegaba. A pesar de sus inconvenientes, fue la tecnología que posibilitó la primera expansión del acceso doméstico a internet.

Un avance importante llegó con las conexiones RDSI, también llamadas ISDN (Integrated Services Digital Network). Estas líneas digitales ofrecían velocidades superiores al dial-up y permitían la transmisión simultánea de voz y datos. A diferencia de las líneas telefónicas analógicas, la RDSI trabajaba con señales digitales puras, lo que reducía el ruido y los errores. Su velocidad típica alcanzaba los 64 Kbps por canal, pudiendo combinarse dos canales para llegar a 128 Kbps. Aunque representó una mejora, su coste era elevado y fue una tecnología de transición.

Más adelante surgió la conexión ADSL, basada en la red telefónica de cobre pero utilizando frecuencias que no interferían con la voz. Esto permitía navegar por internet

sin bloquear la línea telefónica. ADSL se convirtió durante muchos años en la conexión más común en hogares. Sus velocidades iniciales variaban desde 256 Kbps hasta varios megabits por segundo conforme se desarrollaron nuevas versiones del estándar. La estabilidad dependía de la distancia entre la vivienda y la central telefónica, ya que las señales se debilitaban cuanto más lejos estuviera el usuario. ADSL marcó un antes y un después porque proporcionó acceso permanente a internet sin necesidad de marcar, con costes razonables y una velocidad aceptable para la mayoría de los usos.

En paralelo al ADSL, apareció otra tecnología importante: la conexión por cable coaxial. Esta utiliza la red de televisión por cable para la transmisión de datos. Los módems de cable son capaces de alcanzar velocidades superiores a las del ADSL y presentan menor degradación por distancia, ya que el cable coaxial está diseñado para soportar un ancho de banda considerable. En zonas urbanas ha sido una de las conexiones más populares porque permite velocidades elevadas tanto de descarga como de subida, con una estabilidad mucho mayor que el ADSL.

El siguiente gran salto tecnológico llegó con la fibra óptica. Este tipo de conexión usa cables formados por filamentos de vidrio o plástico que transmiten datos mediante pulsos de luz. Las señales ópticas no sufren interferencias electromagnéticas ni pérdida significativa de calidad, lo que permite velocidades extremadamente altas, latencias muy bajas y una estabilidad sobresaliente. La fibra óptica es actualmente la tecnología más avanzada y eficiente para el acceso doméstico a internet. Sus velocidades pueden superar fácilmente 1 Gbps y seguir aumentando conforme evolucionan los equipos. También permite conexiones simétricas, donde la velocidad de subida es igual a la de bajada, algo esencial para servicios como videollamadas, streaming, almacenamiento en la nube y juegos en línea.

Además de las conexiones físicas, existen conexiones inalámbricas. La más común es la conexión WiFi, que no es un tipo de conexión a internet en sí misma, sino el método mediante el cual los dispositivos se conectan al router dentro de una casa o un edificio.

Las tecnologías WiFi han mejorado de manera continua con nuevos estándares, como WiFi 4, WiFi 5, WiFi 6 y WiFi 6E, cada uno ofreciendo mayor velocidad, cobertura y capacidad para conectar múltiples dispositivos en simultáneo.

Otro tipo de conexión inalámbrica importante es la conexión móvil a través de redes celulares. Las primeras redes de datos móviles, como GPRS y EDGE, ofrecían velocidades muy bajas, pero permitieron el uso inicial de internet en teléfonos. El verdadero despegue llegó con las redes 3G, que introdujeron velocidades más altas y posibilitaron el uso de aplicaciones, navegación fluida y transmisión de archivos. Posteriormente, las redes 4G LTE aumentaron tanto la velocidad como la estabilidad, convirtiéndose en uno de los métodos más utilizados para acceder a internet fuera de casa. Actualmente, las redes 5G permiten velocidades muy superiores, baja latencia y mayor capacidad de conexión simultánea, lo que las convierte en una tecnología ideal para dispositivos móviles, hogares sin cableado y aplicaciones como vehículos conectados o Internet de las Cosas.

Existen también conexiones inalámbricas de largo alcance como WiMAX, una tecnología diseñada para proporcionar acceso de banda ancha en áreas rurales o donde no existe infraestructura de cable o fibra. Aunque nunca tuvo una adopción masiva, fue importante como alternativa en regiones con poca cobertura.

Otro método de conexión es el satélite. Este tipo de conexión es útil en zonas geográficamente aisladas donde los cables no llegan. Utiliza antenas parabólicas que envían y reciben señales desde satélites en órbita. Aunque permite acceso global, presenta desventajas como la latencia muy alta debido a la distancia que recorren las señales y la limitación del ancho de banda. En los últimos años, empresas como Starlink han introducido un nuevo tipo de conexión satelital de órbita baja, que reduce enormemente la latencia y mejora la velocidad, haciéndola más competitiva frente a otras opciones.

Finalmente, existen conexiones PLC, que utilizan la red eléctrica del hogar para transmitir datos. Este sistema permite llevar la conexión a diferentes habitaciones sin necesidad de tirar cables adicionales. Aunque no es un tipo de conexión a internet externa, sí es una forma de distribuir la conexión dentro del hogar cuando la señal WiFi no es suficiente.

En conjunto, los diferentes tipos de conexión a internet muestran cómo la tecnología ha avanzado desde transmisiones analógicas lentas hasta sistemas ópticos capaces de transportar información a velocidades casi instantáneas. Cada una ha cumplido un papel fundamental en su época y ha permitido que internet evolucione y se convierta en la herramienta esencial que es hoy.

5. NAVEGADORES: CONCEPTO, HISTORIA, FUNCIONAMIENTO Y TIPOS

5.1 Concepto:

Un navegador web es un software que permite acceder, visualizar e interactuar con las páginas web disponibles en Internet. Los navegadores interpretan el código HTML, CSS, y JavaScript de las páginas y lo muestran de manera comprensible para el usuario.

5.2 Historia:

El primer navegador web fue **WorldWideWeb** (luego renombrado Nexus), desarrollado por Tim Berners-Lee en 1990. Sin embargo, el navegador más popular de los primeros años fue **Mosaic**, que permitió que la web se volviera accesible para un público más amplio. Con el tiempo, surgieron otros navegadores como **Netscape Navigator**, **Internet Explorer** y, más recientemente, **Google Chrome**, **Mozilla Firefox** y **Safari**.

5.3 Funcionamiento:

El navegador se comunica con los servidores web a través del **Protocolo HTTP**, enviando solicitudes y recibiendo las respuestas en forma de documentos HTML, que interpreta y presenta al usuario de manera visual. También puede ejecutar scripts, manejar multimedia y almacenar datos en caché para mejorar el rendimiento.

5.4 Tipos:

- **Google Chrome**: El más utilizado, rápido y con un amplio soporte para extensiones.
- **Mozilla Firefox**: Conocido por su enfoque en la privacidad y código abierto.
- **Safari**: El navegador de Apple, optimizado para dispositivos macOS y iOS.
- **Microsoft Edge**: El sucesor de Internet Explorer, basado en Chromium.

6. PROTOCOLO TCP/IP Y FTP

6.1 TCP/IP:

El **Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP)** es un conjunto de reglas que gobiernan cómo se envían y reciben los datos en Internet. TCP asegura que los datos se entreguen de manera confiable y sin errores, mientras que IP es responsable de la dirección y el enrutamiento de esos datos a través de la red.

6.2 FTP (File Transfer Protocol):

FTP es un protocolo de red utilizado para transferir archivos entre un servidor y un cliente. Permite subir y bajar archivos de un servidor web o sistema remoto. Aunque es menos seguro que otros métodos de transferencia (como **SFTP**), sigue siendo ampliamente utilizado en el mundo del desarrollo web.

7. PÁGINAS WEB: CONCEPTO, TIPOS, CONSTRUCCIÓN, FUNCIONAMIENTO Y PROTOCOLO HTTP

7.1 Concepto:

Una página web es un documento que se encuentra en Internet y es accesible a través de un navegador. Está formada por una combinación de texto, imágenes, videos y otros recursos multimedia.

7.2 Tipos:

- **Estáticas**: Son páginas web cuyos contenidos no cambian a menos que se editen manualmente. Se construyen utilizando solo HTML y CSS.

- **Dinámicas**: Las páginas dinámicas pueden cambiar su contenido en función de las interacciones del usuario o de datos almacenados en bases de datos. Se crean utilizando lenguajes como **PHP**, **JavaScript**, **ASP**, y **JSP**.

7.3 Construcción:

Las páginas web se construyen utilizando lenguajes de programación como:

- **HTML**: Define la estructura de la página web.

- **CSS**: Se utiliza para dar estilo a la página.

- **JavaScript**: Proporciona interactividad.

- **PHP, ASP, JSP**: Lenguajes de programación para crear páginas dinámicas y conectarlas con bases de datos.

- **SQL**: Lenguaje utilizado para gestionar bases de datos.

7.4 Funcionamiento:

Las páginas web se cargan cuando un navegador envía una solicitud a un servidor web a través de HTTP (HyperText Transfer Protocol). El servidor responde enviando el código HTML de la página, que es interpretado y mostrado por el navegador.

7.5 Protocolo HTTP:

HTTP es el protocolo de comunicación que se utiliza para transferir páginas web. En su versión segura, **HTTPS**, se utiliza cifrado para proteger la información que se transmite entre el navegador y el servidor.

8. FUNCIONALIDADES DE INTERNET

Las principales funcionalidades que Internet ofrece a los usuarios incluyen:

- **Correo electrónico**: Permite el envío y recepción de mensajes entre usuarios.

- **Videoconferencias**: Herramientas como **Zoom**, **Google Meet** o **Skype** facilitan reuniones en tiempo real.

- **Compras**: Plataformas de **e-commerce** como **Amazon** o **eBay** permiten comprar productos online.

- **Juegos online**: Juegos que se juegan a través de la web, tanto individuales como multijugador.

- **Chats**: Aplicaciones de mensajería como **WhatsApp** o **Telegram** permiten la comunicación instantánea.

- **Redes sociales**: Plataformas como **Facebook**, **Twitter**, e **Instagram** permiten la interacción social.

- **Streaming**: Servicios como **Netflix**, **Spotify** y **YouTube** ofrecen contenido multimedia en tiempo real.

- **Buscadores**: Motores como **Google** permiten encontrar información en la web.

- **Inteligencia Artificial**: Algoritmos que mejoran la personalización, como los asistentes virtuales y recomendaciones.

9. PRIVACIDAD Y SEGURIDAD EN REDES SOCIALES Y CHATS

La seguridad en internet es uno de los temas más importantes dentro del mundo digital porque afecta directamente a la protección de los datos personales, la privacidad, la integridad de la información y la confianza en los servicios online.

Desde el momento en que un dispositivo se conecta a una red, queda expuesto a una serie de riesgos que pueden comprometerlo si no existen medidas de protección adecuadas. A lo largo del tiempo, la seguridad en internet ha evolucionado a medida que crecían las amenazas, la sofisticación de los atacantes y la dependencia de las tecnologías digitales. Protegerse no solo implica herramientas técnicas, sino también hábitos de uso responsable.

La seguridad en internet se basa en tres principios fundamentales: la confidencialidad, la integridad y la disponibilidad. La confidencialidad consiste en garantizar que solo las personas autorizadas puedan acceder a determinados datos. La integridad se refiere a que la información no debe ser modificada de forma no autorizada durante su almacenamiento o transmisión. La disponibilidad asegura que los datos y servicios estén accesibles cuando el usuario los necesite. Si cualquiera de estos tres pilares falla, la seguridad queda comprometida. Estos principios se aplican tanto a usuarios comunes como a empresas, instituciones educativas, gobiernos y plataformas digitales.

Uno de los mayores riesgos en internet son los malware, que son programas maliciosos diseñados para causar daño, robar información o infiltrarse en sistemas ajenos. Entre los tipos de malware más comunes se encuentran los virus, los gusanos, los troyanos, el ransomware, los spyware y los adware. Cada uno actúa de forma distinta: los virus infectan archivos, los gusanos se replican automáticamente a través de la red, los troyanos se presentan como programas legítimos para engañar al usuario, el ransomware cifra los

datos de la víctima y exige un rescate para recuperarlos, los spyware recopilan información sin permiso y los adware muestran publicidad no deseada. El malware es una de las principales amenazas en internet porque puede comprometer la seguridad de dispositivos personales, redes empresariales e incluso infraestructuras críticas.

Otro aspecto esencial de la seguridad en internet es el uso de contraseñas. Muchos ataques ocurren porque los usuarios utilizan claves débiles, repetidas o fáciles de adivinar. Una contraseña segura debe ser larga, combinar letras, números y símbolos y no contener datos personales evidentes. Sin embargo, incluso las contraseñas fuertes pueden ser insuficientes si no se acompañan de medidas adicionales como la autenticación de dos factores, que requiere un segundo paso de verificación, normalmente a través de un mensaje, una app o una llave física. La autenticación en dos pasos reduce significativamente la probabilidad de que un atacante acceda a una cuenta incluso si logra obtener la contraseña.

La seguridad también incluye el uso de conexiones cifradas. Cuando un usuario navega por un sitio web, el protocolo HTTPS garantiza que los datos intercambiados entre el navegador y el servidor viajen cifrados, impidiendo que terceros puedan leerlos o interceptarlos. El candado que aparece en los navegadores indica que la página utiliza un certificado de seguridad válido. Sin este cifrado, cualquier información transmitida, como contraseñas o datos personales, puede ser capturada mediante técnicas de espionaje conocidas como ataques “man-in-the-middle”.

El phishing es otra amenaza muy extendida. Consiste en engañar al usuario para que revele voluntariamente información sensible, como claves bancarias o credenciales de acceso, mediante correos electrónicos, mensajes o páginas falsas que imitan a servicios legítimos. El phishing funciona porque explota la confianza y el desconocimiento de la víctima. Existen variantes más sofisticadas, como el spear-phishing, dirigido a individuos específicos con mensajes personalizados, y el smishing, que utiliza mensajes SMS. La forma de protegerse ante el phishing es verificar siempre el remitente, revisar

cuidadosamente los enlaces antes de hacer clic y desconfiar de mensajes que piden información urgente o amenazan con consecuencias.

Las redes WiFi públicas representan otro riesgo importante. Conectarse a una red abierta, como la de un bar o un aeropuerto, puede permitir a atacantes interceptar la información que envía el usuario. Además, existen redes falsas creadas por ciberdelincuentes para robar datos. Por eso es recomendable evitar realizar compras, acceder a la banca online o introducir contraseñas en redes públicas.

Utilizar una VPN (red privada virtual) puede ofrecer una capa adicional de seguridad porque cifra todo el tráfico que sale del dispositivo, haciendo que incluso en una red insegura los datos no puedan ser interpretados por terceros.

Las redes sociales también suponen un riesgo significativo para la seguridad y la privacidad. Compartir información personal en exceso facilita que los atacantes construyan perfiles detallados para realizar estafas, suplantación de identidad o ingeniería social. La ingeniería social es una técnica que consiste en manipular a las personas para obtener datos o acceso a sistemas.

No se basa en conocimientos técnicos, sino en el engaño emocional o psicológico. Por ejemplo, un atacante puede hacerse pasar por un servicio técnico para pedir una contraseña o fingir ser un conocido para obtener información privada. Para protegerse, es necesario limitar la información pública en redes sociales, revisar la configuración de privacidad y desconfiar de solicitudes inesperadas.

En el ámbito de la seguridad, los firewalls juegan un papel fundamental. Un firewall es un sistema que controla el tráfico entre un dispositivo o una red y el exterior, permitiendo

o bloqueando conexiones según unas reglas establecidas. Existen firewalls de software, incluidos en la mayoría de sistemas operativos, y firewalls físicos utilizados en empresas. Estos sistemas evitan intrusiones, bloquean conexiones sospechosas y reducen la posibilidad de ataques directos.

Las actualizaciones de software también son cruciales. Muchos ataques aprovechan vulnerabilidades presentes en versiones antiguas de programas. Los desarrolladores publican parches para corregir estos fallos, por lo que mantener actualizado el sistema operativo, el navegador, las aplicaciones y el antivirus es una de las medidas más efectivas para evitar problemas. Las vulnerabilidades no corregidas son una de las causas más comunes de ciberataques exitosos.

La educación digital también es una pieza fundamental de la seguridad en internet. Muchos ataques tienen éxito porque los usuarios no conocen los riesgos ni las formas adecuadas de reaccionar. Saber identificar un correo sospechoso, evitar descargar archivos desconocidos, reconocer páginas falsas o gestionar correctamente la privacidad puede prevenir la mayoría de incidentes. La seguridad no depende solo de la tecnología, sino también del comportamiento humano.

Finalmente, la seguridad en internet abarca la protección de datos personales. Las leyes de privacidad, como el Reglamento General de Protección de Datos (RGPD) en Europa, obligan a las empresas a tratar los datos de forma segura y transparente. Esto incluye la obligación de solicitar el consentimiento, proteger la información almacenada y notificar a los usuarios cuando ocurre una brecha de seguridad.

En conjunto, la seguridad en internet es un proceso continuo que combina tecnologías, buenas prácticas, conocimientos y actualizaciones constantes. No existe una protección

absoluta, pero una combinación adecuada de medidas reduce significativamente los riesgos y permite un uso seguro y confiable de los servicios digitales.