

INSTITUTO POLITECNICO NACIONAL



Unidad Profesional Interdisciplinaria de
Ingeniería Ciencias Sociales y Administrativas

Lic. Administración Industrial
TECNOLOGÍAS DE INFORMACIÓN

UNIDAD TEMÁTICA IV

Tecnologías en ambiente web

Equipo 3

Del Río García Ricardo Isaac

Dorantes Prado Dulce Xcaret

Estela Castrejón Ayleen Guadalupe

Estrella Cárdenas Fernanda

Fernández Moreno Karina

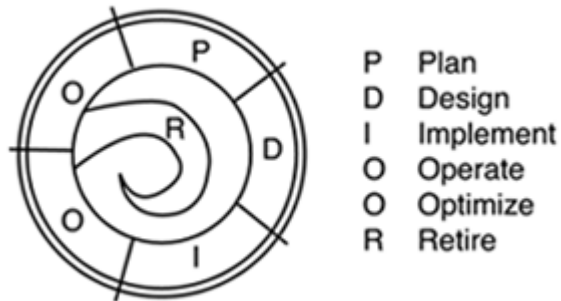
Índice

TECNOLOGÍAS DE INFORMACIÓN	1
Equipo 3	1
Unidad Temática IV “Tecnologías en ambiente web”	3
4.1. Metodología en Redes	3
4.1.1. Tipos de redes	7
4.1.2. Topologías de redes.....	10
4.1.3. Protocolos de redes	14
4.1.4. Estándares de redes	17
4.1.5. Redes Empresariales.....	18
4.1.6. Redes en la Nube y móviles.....	19
4.2. Internet.....	20
4.2.1. Origen del Internet	22
4.2.2. Servicios de Internet	23
4.2.3. Direcciones IP.....	24
4.2.4. Tipos de dominio	27
4.2.5. Nombre de dominio	29
4.3. Hardware y software para redes.....	30
4.3.1. Tipos de servidores	32
4.3.2. Dispositivos de comunicación	36
4.3.3. Medios alámbricos e inalámbrico	38
4.3.4. Diseño de sitios web con aplicaciones	40
4.3.5. Aplicaciones empresariales en la red	41
Videos de apoyo:.....	42
Bibliografía:	43

Unidad Temática IV “Tecnologías en ambiente web”

4.1. Metodología en Redes

La metodología en redes se refiere al conjunto de procesos, técnicas y herramientas utilizadas para planificar, implementar y gestionar una red de computadoras de forma eficiente y segura. Es un enfoque sistemático y estructurado para diseñar, implementar, gestionar y optimizar redes de computadoras. Esta metodología incluye una serie de pasos y procesos que ayudan a los ingenieros de redes a crear redes eficientes y seguras para satisfacer las necesidades de una organización.



La metodología de redes en informática es fundamental para garantizar que las redes funcionen de manera efectiva y cumplan con los requisitos de una organización en términos de comunicación, colaboración y acceso a recursos de información.

METODOLOGÍA CISCO

En esta metodología lo primero que se realizará es identificar las metas y necesidades del Negocio para lo cual se basa en:

Análisis estructurado de sistemas

Comienza en las capas superiores del modelo OSI hasta llegar a las capas inferiores

Los objetivos es obtener necesidades del cliente y trabajar por módulos.

Los modelos para considerar en esta metodología son:

1. Modelos Lógico: Representa la construcción básica bloques divididos por función y la estructura del sistema.
2. Modelo Físico: Representa los dispositivos y especifica las tecnologías e implementaciones.

Fases del Diseño Top/Down

- Análisis de Requerimientos
- Desarrollo del Diseño Lógico

- Desarrollo del Diseño Físico
- Pruebas
- Optimización
- Documentación del Diseño.

Ciclo de Vida

- Planear
- Diseñar
- Implementar
- Operar
- Optimizar
- Retirar

METODOLOGÍA MCCABE JAMES

En esta metodología es fundamental elaborar las siguientes Fases:

Fase de Análisis

- Recabar requerimientos
- Definir las aplicaciones que se ejecutarán en forma distribuida
- Caracterizar como usan los usuarios las aplicaciones, definir métricas para medir el desempeño
- Distinguir entre requerimientos de servicio: Entradas y Salidas
- Definir flujos, establecer las fronteras de flujo.

Fase de Diseño

- Establecer metas de diseño. - Desarrollar criterios para evaluación de tecnologías: costo, rapidez, confiabilidad, etc.
- Realizar la selección de tecnologías.
- Integrar mecanismos de interconexión.
- Integrar aspectos de administración y seguridad al diseño.
- Incorporar análisis de riesgos y planificación de contingencias.
- Evaluar opciones de diseño del cableado.
- -Seleccionar la ubicación de los equipos.
- Realizar el diagrama físico de la red.
- Incorporar las estrategias de enrutamiento con base en los flujos.
- Optimizar flujos de enrutamiento.
- Desarrollar una estrategia detallada de enrutamiento.

METODOLOGÍA LONG CORMAC

Esta metodología tiene mucho parecer con las metodologías mencionadas anteriormente en la cual consideramos las fases de análisis y diseño, será especificado de manera que usted lo entienda.

- Dentro de la cual se elegirá parámetros de desempeño con base a las aplicaciones (ancho de banda, % pérdida de paquetes, latencia, disponibilidad).
- Identificar Restricciones de diseño (presupuesto, tiempo de implantación, restricciones físicas restricciones de seguridad).
- Establecer objetivos viables para los parámetros de desempeño.
- Elaborar el diseño de alto nivel (nivel jerárquicos, elección de conectividad WAN, routing vs switching, etc.).
- Elaborar un diseño detallado teórico.
- Realizar verificaciones en laboratorio de aspecto mayores, si no se cumple con los requerimientos.
- Realizar la instalación y configuración final.

METODOLOGÍA UNTIVEROS SERGIO

En esta metodología nos dice que la administración de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad.

La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación y actualización.

Se basa en el modelo OSI, enfatiza en todos los aspectos relacionados en la buena operación de una red, como son el control sobre los sucesos en la red, la visualización de los tipos de tráfico, la determinación y atención oportuna de problemas, aspectos de seguridad, etc.

METODOLOGÍA INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

En esta metodología nos dice que el marco metodológico para un proyecto informático constará con 4 etapas y 5 dimensiones, Siendo estas las siguientes:

a) Etapas

- Organización
- Desarrollo
- Implantación
- Evaluación

b) Dimensiones

- Modelamiento del Proyecto
- Modelamiento de la Institución
- Modelamiento de Requerimiento
- Modelamiento de Tecnología
- Construcción

	O r g a n i z a c i ó n	D e s a r r o l l o	I m p l a n t a c i ó n	E v a l u a c i ó n
Mod. Proyecto				
Mod. Institución				
Mod. Requerimiento				
Mod. Tecnología				
Construcción				

Como pueden observar en la imagen las dimensiones son tareas que se realizará de acuerdo con cada Etapa.

ETAPA DE ORGANIZACIÓN

- Modelamiento del Proyecto
- Modelamiento de la Institución
- Modelamiento del Requerimiento

ETAPA DE DESARROLLO

- Modelamiento de la Organización
- Modelamiento de Requerimientos
- Modelamiento de la Tecnología
- Construcción

ETAPA DE IMPLANTACION

- Modelamiento de la Organización
- Modelamiento de la Instalación
- Modelamiento del Requerimiento
- Modelamiento de Tecnología
- Construcción

ETAPA DE EVALUACIÓN

a) Modelamiento de Requerimiento

La organización del proyecto debe verificar la eficacia del mismo, a partir de la opinión de los usuarios y de indicadores de productividad, que muestren a la alta dirección los beneficios del proyecto de red.

b) Modelamiento de la Tecnología

Se debe evaluar también la performance de la tecnología empleada, así como el impacto de ésta en las formas de trabajo de los usuarios.

las nuevas formas de trabajo deben permitir identificar a los usuarios que requieren de un refuerzo adicional.

c) Construcción

La correcta evaluación del proyecto, debe permitir implantar correctivos que coadyuven al éxito del proyecto, teniendo a los usuarios como principio y fin para el desarrollo exitoso de un proyecto de red (Perfil, s/f).

4.1.1. Tipos de redes

Existen diferentes tipos de redes informáticas que se pueden utilizar y que permiten conectar a los usuarios a distintas escalas.

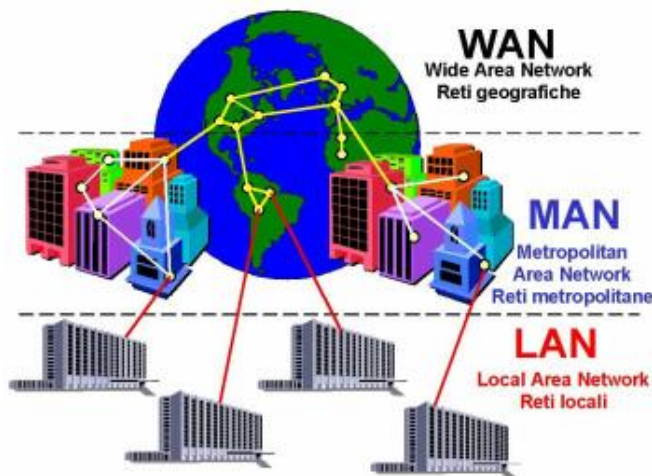
Por esta razón, las redes informáticas se clasifican según su complejidad y su tamaño. Además, estas mismas se diferencian entre sí por las tareas que pueden ser realizadas por los usuarios.

A continuación, te presentamos los tipos de redes informáticas más importantes:

LAN (Local Area Network)

Las redes de área local son uno de los tipos de redes informáticas más comunes en hogares y lugares de trabajo. Estas permiten la comunicación y compartir documentos entre diferentes equipos digitales dentro de un espacio relativamente pequeño, como una casa u oficina. Además, estas redes destacan por ser poco costosas y tener una alta velocidad (Abril, 2022).

MAN (Metropolitan Area Network)



Las redes de área metropolitana consisten, principalmente, en interconexiones de varias redes LAN. De este modo, son un tipo de redes informáticas de tamaño mediano que conectan a dispositivos y usuarios en espacios como una comunidad o una ciudad.

Tienen niveles de transferencia bastante altos y están administradas por un grupo de usuarios comunes o un proveedor de red regional. Además, son el punto de conexión entre las redes LAN y las redes WAN (abril, 2022).

WAN (Wide Area Network)

Se definen como redes de área amplia, ya que son redes computacionales más grandes que engloban e interconectan a las LAN, MAN y otros tipos de redes informáticas.

En concreto, conectan regiones o países por medio de satélites o líneas telefónicas. Sin embargo, la distancia y los tipos de conexiones hacen que, por lo general, las WAN cuenten con velocidades más lentas, que usualmente no superan los 2 Megas por segundo (abril, 2022).

WLAN (Wireless Local Area Network)

Las redes de área local inalámbricas son redes similares a las LAN que vinculan varios dispositivos para formar una red local de manera inalámbrica; haciendo uso del WIFI para conectarse (abril, 2022).

Entre todos los tipos de redes informáticas, estas son de las más prácticas para los usuarios, ya que no tienen que utilizar cables de Ethernet. No obstante, son más propensas a ciberataques (abril, 2022)

CAN (Campus Area Network)

Si se trata de dar servicios de conectividad a una red ubicada en un espacio mediano, se suele recurrir a este tipo de redes informáticas. Su infraestructura puede conectar campus universitarios o espacios corporativos de gran envergadura. En este último caso, cambian su nombre por Corporate Area Network (abril, 2022).

SAN (Storage Area Network)

Se utilizan para enlazar unidades de almacenamiento de información y datos por medio de redes de alta velocidad. Estas redes son instaladas de forma paralela a una red local para que el tráfico de datos almacenados no frene el tráfico de la red local, utilizada para la comunicación entre miembros de la empresa (abril, 2022).

VLAN (Virtual Local Area Network)

Las redes de área local virtual son un tipo de redes informáticas segmentadas dentro de una red local que permiten la transferencia segura y privada de datos.

Son muy similares a los VPNs, ya que protegen la comunicación y transferencia por medio de una conexión única entre dos equipos en una misma red (abril, 2022).

PAN (Personal Area Network)

Las PAN conectan y permiten la transferencia de datos entre los dispositivos de un mismo usuario como, por ejemplo, la computadora, el teléfono inteligente y la tableta, etc. Actualmente, muchas de estas redes son inalámbricas y utilizan tecnologías como el Bluetooth para facilitar el intercambio de información entre los dispositivos del consumidor (abril, 2022).

GAN (Global Area Network)

Con 5.160 millones de personas, lo que representa el 64,4% de la población mundial, según datos del informe Digital Report 2023 de We Are Social, Internet es el ejemplo más significativo de una Red Global, aunque no es la única.

Las empresas con presencia en todo el mundo suelen emplear este tipo de red informática para trabajar bajo criterios unificados y compartir la infraestructura dentro de su empresa, con el objetivo de tener un mayor control. Cabe mencionar que, a su vez, las redes globales se componen de otros tipos de redes informáticas (abril, 2022).

Wi-Fi (Redes inalámbricas)

Las redes inalámbricas son una de las tecnologías más utilizadas en la actualidad, permitiendo la conexión de dispositivos electrónicos sin necesidad de cables o alambres. Esta tecnología se ha vuelto fundamental para varias áreas de la vida moderna, desde la comunicación personal hasta la conectividad en entornos corporativos e industriales.

Las redes inalámbricas están formadas por una serie de dispositivos que se comunican entre sí mediante ondas de radio o infrarrojos (De Oliveira Gomes, 2023).

Red de Satélite

Es una red de comunicación de datos facilitada por uno o más satélites de comunicación en órbita terrestre. Se puede dividir en dos segmentos: el espacial y el terrestre.

El segmento espacial consiste en el hardware del satélite y la carga útil de comunicación. Los equipos de comunicación a bordo son para transmitir y recibir señales desde y hacia la Tierra. Si la red satelital tiene más de un satélite, el segmento espacial también puede incluir enlaces de comunicación entre satélites (ISL).

El segmento terrestre consta de estaciones terrestres, telepuertos y centros de operación de red (NOC). Una estación terrestre tiene una antena satelital

(generalmente en forma de plato) con hardware y software de comunicación para transmitir y recibir información de los satélites. Las estaciones terrestres también son la interfaz externa de las redes satelitales cuando forman parte de enrutadores de red y de puertas de enlace conectadas a otras redes. De esta manera, el NOC controla la operación del satélite y administra los recursos de la red (Abril, 2022).

PSN (Red conmutada por paquetes)

Una red de conmutación de paquetes (PSN) es un tipo de red de transmisión de datos que divide la información en pequeños segmentos llamados paquetes. Estos paquetes viajan por separado y pueden seguir caminos diferentes para llegar a su destino. Además, los paquetes de muchas computadoras pueden viajar por las mismas rutas simultáneamente sin disminuir la velocidad. Cuando una computadora recibe los paquetes, se vuelven a ensamblar (s/f).

VPN (Virtual Private Network)

Una red privada virtual o VPN es una conexión cifrada a Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar la transmisión segura de datos confidenciales. Evita que las personas no autorizadas espíen el tráfico y permite que el usuario trabaje de manera remota. La tecnología de VPN se usa ampliamente en los entornos corporativos (Duo for AnyConnect VPN Overview Video, 2019).

Redes 5G

Son redes de última generación que ofrecen velocidades de conexión más rápidas y mayor capacidad de datos, ideales para el Internet de las cosas (IoT) y aplicaciones de realidad virtual y aumentada.

4.1.2. Topologías de redes

La topología de red es cómo se organizan los elementos de una red de comunicaciones. La estructura topológica se puede representar física o lógicamente.

En el caso de la topología lógica, los dispositivos de comunicación se modelan como nodos y las conexiones entre dispositivos se modelan como enlaces o líneas entre nodos.

La topología física describe la verdadera apariencia o diseño de la red. Las distancias entre nodos, interconexiones físicas, velocidades de transmisión o tipos de señales pueden diferir entre dos redes, pero sus topologías lógicas pueden ser idénticas.

Al mapear gráficamente estos enlaces, obtenemos algunas formas geométricas que se pueden usar para describir diferentes topologías. Hay ventajas y desventajas

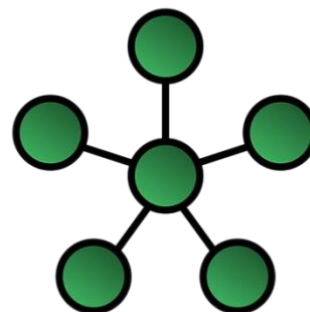
para cada uno de ellos, ya que difieren en cómo los dispositivos pueden (o no pueden) interconectarse.

Tipos de topologías de red

Un administrador de red tiene varias opciones a la hora de elegir qué tipo de topología utilizar. La elección dependerá del tamaño y la escala de su organización, sus objetivos comerciales y su presupuesto (International IT, 2021).

Topología en Estrella

Es el tipo de configuración más común. La red está organizada de modo que los nodos estén conectados a un dispositivo central (un hub), que actúa como servidor. El hub gestiona la transmisión de datos a través de la red. Es decir, cualquier dato enviado a través de la red viaja a través del dispositivo central antes de terminar en su destino (International IT, 2021).



Ventajas:

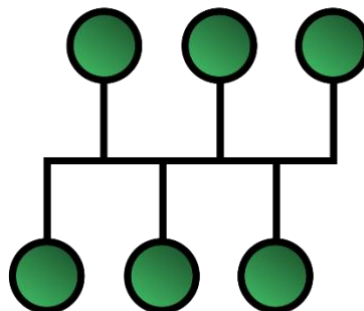
- Gestión conveniente desde una ubicación central
- Si un nodo falla, la red aún funciona
- Los dispositivos se pueden agregar o apartar sin interrumpir la red
- Más fácil de identificar y aislar los problemas de rendimiento

Desventajas:

- Si el dispositivo central falla, toda su red dejará de funcionar.
- El rendimiento y el ancho de banda están limitados por el nodo central
- Puede ser costoso de operar

Topología en Bus

También llamada topología de red troncal, bus o línea, guía los dispositivos a lo largo de un solo cable que se extiende desde un extremo de la red hasta el otro. Los datos fluirán a lo largo del cable a medida que viaja a su destino (International IT, 2021).



Ventajas:

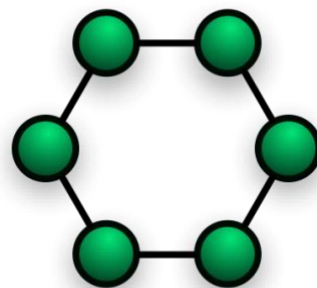
- Económico para redes más pequeñas
- Diseño simple; todos los dispositivos conectados a través de un cable
- Se pueden agregar más nodos alargando la línea

Desventajas:

- La red es vulnerable a fallas de cables.
- Cada nodo agregado disminuye la velocidad de transmisión
- Los datos solo se pueden enviar en una dirección a la vez.

Topología en Anillo

Los nodos se configuran en un patrón circular. Los datos viajan a través de cada dispositivo a medida que viajan a través del anillo. En una red grande, es posible que se necesiten repetidores para evitar la pérdida de paquetes durante la transmisión. Las topologías de anillo se pueden configurar como anillo único (half-dúplex) o anillo doble (full-dúplex) para permitir que el tráfico fluya en ambas direcciones simultáneamente (International IT, 2021).



Ventajas:

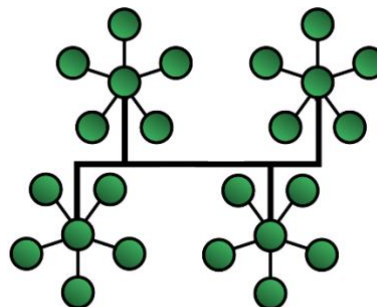
- Costo beneficio
- Barato de instalar
- Problemas de rendimiento fáciles de identificar

Desventajas:

- Si un nudo cae, puede caer varios nudos con él.
- Todos los dispositivos comparten ancho de banda, lo que puede limitar el rendimiento de transferencias.
- Agregar o eliminar nodos significa tiempo de inactividad para toda la red

Topología en Árbol

Un nodo central conecta los hubs secundarios. Estos hubs tienen una relación de padres-hijos con los dispositivos. El eje central es como el tronco del árbol. Donde las ramas se conectan son los concentradores secundarios o los nodos de control y luego los dispositivos conectados se conectan a los branches (International IT, 2021).



Ventajas:

- Extremadamente flexible y escalable
- Facilidad para identificar errores, ya que cada branch de la red puede diagnosticarse individualmente.

Desventajas:

- Si falla un hub central, los nodos se desconectarán (aunque las ramas pueden seguir funcionando de forma independiente)
- La estructura puede ser difícil de gestionar de forma eficaz
- Utiliza mucho más cableado que otros métodos

Topología de Malla (Mesh)

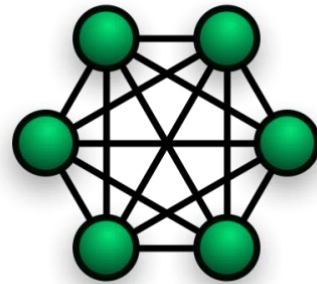
Los nodos están interconectados. Los modos full-mesh conectan todos los dispositivos en la red directamente. En una topología de malla parcial, la mayoría de los dispositivos se conectan directamente. Esto proporciona múltiples rutas para la entrega de datos. Los datos se envían a la distancia más corta disponible para la transmisión (International IT, 2021).

Ventajas:

- Confiable y estable
- Ningún fallo de un solo nodo desconecta la red

Desventajas:

- Grado complejo de interconectividad entre nodos.
- Mano de obra intensiva para instalar
- Utiliza mucho cableado para conectar todos los dispositivos.



Topología Híbrida

Utiliza varias estructuras de topología. Esto es más común en organizaciones grandes donde cada departamento puede tener un tipo de topología, como estrella o línea, con el hub del departamento conectando a un hub central (International IT, 2021).

Ventajas:

- Flexibilidad
- Puede personalizarse según las necesidades del cliente.

Desventajas:

- La complejidad aumenta
- Se requiere experiencia en múltiples topologías
- Puede ser más difícil determinar los problemas de rendimiento.

4.1.3. Protocolos de redes

Un protocolo de red es un estándar de comunicaciones. Contiene las reglas necesarias y la información sobre cómo las computadoras intercambian datos entre sí. Se requiere una interacción de diferentes tipos para diversas tareas, como, por ejemplo, el simple intercambio de mensajes.

Así, cada uno de los protocolos de comunicación de redes asume entonces una tarea específica en el medio que se requiera, el cual puede abarcar sectores como el industrial o empresarial. Y son desarrollados por entidades, organizaciones y personas que trabajan en la industria, institutos de investigación, etc.



Luego se publican y aceptan en conferencias internacionales para marcar estándares de comunicaciones como lo es la ISO (International Standards Organization), por medio de la arquitectura OSI (Open Systems Interconnect) por mencionar un ejemplo. Más adelante veremos las características de este modelo y de otro más, el TCP/IP.

De manera general, los protocolos de red llevan a cabo las siguientes tareas:

- Establecer una conexión confiable entre los equipos implicados en la comunicación.
- Dirigir los paquetes de datos enviados al destinatario correcto.
- Si los paquetes no llegan, el protocolo se asegura de que se reenvíen.
- Transmisión sin errores de los paquetes de información.
- Organización y fusión de los paquetes de datos entrantes.
- Cifrado de los datos transmitidos para que no puedan ser leídos por terceros (encriptación).

Por ello, los protocolos de red se definen como lineamientos, normas o reglas bien definidas mediante las cuales un usuario se comunica a través de Internet (red o conjunto de redes locales distribuidas en todo el mundo) o Intranet (al igual que el Internet, es un conjunto de computadoras, con la excepción de estar determinado a un público específico).

Ambos extremos del canal de comunicación siguen estas reglas para un intercambio de información adecuado. También tiene la tarea de evitar la manipulación por parte de terceros, cuya función se incluye, además, en la seguridad de los entornos digitales, también conocida como.

Existen diversos tipos; el IP o Protocolo de Internet, por ejemplo, es la base de Internet tal y como la conocemos, sin este protocolo, no podríamos mantener la comunicación digital como la conocemos hoy en día. Los protocolos de red como IMAP (Protocolo de acceso a mensajes de Internet), SMTP (Protocolo simple de transferencia de correo) y POP3 (Protocolo de oficina de correos) también se utilizan en la vida diaria en la industria para que, dentro de la misma instalación, y sólo dentro de la misma, sea posible recibir y enviar correos electrónicos.

Además, en tiempos recientes, la comunicación digital, es esencial para que las personas mantengan su estilo de vida habitual. De tal manera, podría ser un serio problema si todos los procesos de redes inalámbricas del mundo fallaran en algún momento.

Por lo tanto, se crearon varios sistemas para permitir una comunicación exitosa, así como protocolos de red porque juegan un papel importante en la optimización del desarrollo de las comunicaciones informáticas. Estos protocolos se clasifican en varias bases como algunos mapas para la capa de transporte, otros para la capa de red, y de esa forma, se van moviendo entre cada una de ellas. Sin embargo, eso lo dejaremos para más adelante y ahora, seguiremos con un poco de contexto histórico y como surgieron (¿Qué es un protocolo de red?, 2022).

En las redes, un protocolo es un conjunto de reglas para formatear y procesar datos. Los protocolos de red son como una lengua franca para los ordenadores. Los ordenadores de una red pueden utilizar software y hardware muy diferentes; sin embargo, el uso de protocolos les permite comunicarse entre sí (s/f-b).

Protocolos se ejecutan en la capa de red

Como se ha descrito anteriormente, el IP es un protocolo de capa de red responsable del enrutamiento. Pero no es el único protocolo de la capa de red.

IPsec: La Seguridad del protocolo de Internet (IPsec) establece conexiones IP cifradas y autenticadas a través de una red privada virtual (VPN). Técnicamente, IPsec no es un protocolo, sino un conjunto de protocolos que incluye el Protocolo de seguridad de encapsulación (ESP), el Encabezado de autenticación (AH) y las Asociaciones de seguridad (SA).

ICMP: El Protocolo de control de mensajes de Internet (ICMP) informa de errores y proporciona actualizaciones de estado. Por ejemplo, si un router no puede entregar un paquete, enviará un mensaje ICMP a la fuente del paquete.

IGMP: El Protocolo de gestión de grupos de Internet (IGMP) establece conexiones de red de uno a varios. El IGMP ayuda a establecer la multidifusión, lo cual implica que varios ordenadores pueden recibir paquetes de datos dirigidos a una dirección IP.

Protocolos se utilizan en Internet

Algunos de los protocolos más importantes que hay que conocer son:

TCP: Como se ha descrito antes, TCP es un protocolo de capa de transporte que garantiza la entrega fiable de datos. El TCP se diseñó para ser utilizado con el IP, y ambos protocolos suelen denominarse conjuntamente TCP/IP.

HTTP: El Protocolo de transferencia de hipertexto (HTTP) es la base de la World Wide Web, la Internet con la que interactúan la mayoría de los usuarios. Se utiliza para transferir datos entre dispositivos. HTTP pertenece a la capa de aplicación (capa 7), porque pone los datos en un formato que las aplicaciones (por ejemplo, un navegador) pueden utilizar directamente, sin necesidad de interpretación. Las capas inferiores del modelo OSI las maneja el sistema operativo de un ordenador, no las aplicaciones.

HTTPS: El problema de HTTP es que no está encriptado: cualquier atacante que intercepte un mensaje HTTP puede leerlo. HTTPS (HTTP Secure) corrige esto encriptando los mensajes HTTP.

TLS/SSL: Transport Layer Security (TLS) es el protocolo que utiliza HTTPS para la encriptación. TLS solía llamarse Capa de puertos seguros (SSL).

UDP: el Protocolo de datagrama de usuarios (UDP) es una alternativa más rápida pero menos fiable al TCP en la capa de transporte. A menudo se utiliza en servicios como la transmisión de vídeo y los videojuegos, donde la rapidez en la provisión de datos es primordial.

Protocolos utilizan los routers

Los routers de red utilizan determinados protocolos para descubrir las rutas de red más eficientes hacia otros routers. Estos protocolos no se utilizan para transferir datos del usuario. Los protocolos de enrutamiento de red más importantes son:

BGP: El Protocolo de puerta de enlace de frontera (BGP) es un protocolo de capa de aplicación que las redes utilizan para difundir las direcciones IP que controlan. Esta información permite que los routers decidan por qué redes deben pasar los paquetes de datos de camino a sus destinos.

EIGRP: El Protocolo de enrutamiento de puerta de enlace anterior mejorado (EIGRP) identifica las distancias entre los routers. EIGRP actualiza automáticamente el registro de las mejores rutas de cada router (que se conoce como tabla de enrutamiento) y difunde esas actualizaciones a otros routers de la red.

OSPF: El protocolo Open Shortest Path First (OSPF) calcula las rutas de red más eficientes en función de diversos factores, como la distancia y el ancho de banda.

RIP: El Protocolo de información de enrutamiento (RIP) es un antiguo protocolo de enrutamiento que identifica las distancias entre routers. El RIP es un protocolo de capa de aplicación.

Protocolos en los ciberataques

Como sucede en cualquier aspecto de la informática, los atacantes pueden aprovechar el funcionamiento de los protocolos de red para comprometer o sobrecargar los sistemas. Muchos de estos protocolos se utilizan en ataques de denegación de servicio distribuido (DDoS). Por ejemplo, en un ataque de inundación SYN, un atacante se aprovecha de cómo funciona el protocolo TCP. Envían paquetes SYN para iniciar repetidamente un protocolo de enlace TCP con un servidor, hasta que el servidor no puede dar servicio a los usuarios legítimos porque sus recursos están ocupados por todas las conexiones TCP falsas.

Cloudflare ofrece una serie de soluciones para detener estos y otros ciberataques. Magic Transit de Cloudflare es capaz de mitigar los ataques en las capas 3, 4 y 7 del modelo OSI. En el caso de un ataque de inundación SYN, Cloudflare se encarga del proceso de intercambio de información TCP en nombre del servidor, de modo que los recursos del servidor nunca se vean sobrecargados por las conexiones TCP abiertas (s/f-b).

4.1.4. Estándares de redes

Los estándares de redes son conjunto de reglas y normas que establecen los protocolos que gobiernan la comunicación y transmisión de datos en una red. Estos estándares son desarrollados por organizaciones como IEEE, IETF, y ISO, entre otros, con el objetivo de asegurar la interoperabilidad entre diferentes dispositivos y redes.

Algunos de los estándares más comunes en redes incluyen:

1. Ethernet (IEEE 802.3): Estándar para la transmisión de datos en redes de área local (LAN).
2. Wi-Fi (IEEE 802.11): Estándar para redes inalámbricas que permite la conectividad entre dispositivos sin la necesidad de cables.
3. TCP/IP: Protocolo de comunicación utilizado en Internet que define cómo los



dispositivos en una red se comunican entre sí.

4. DNS (Domain Name System): Protocolo utilizado para traducir nombres de dominio en direcciones IP.
5. HTTP (Hypertext Transfer Protocol): Protocolo utilizado para la transferencia de información en la web.
6. SNMP (Simple Network Management Protocol): Protocolo utilizado para monitorear y gestionar dispositivos de red.

Estos estándares son fundamentales para el funcionamiento de las redes de comunicación, ya que permiten que diferentes dispositivos y sistemas puedan comunicarse entre sí de manera eficiente y segura.

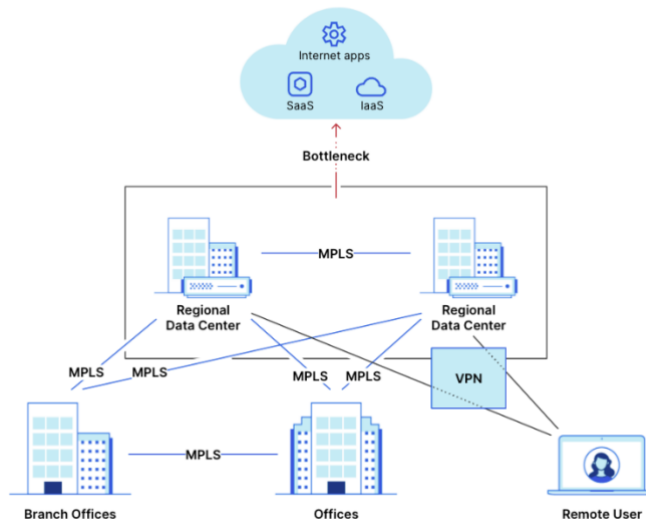
4.1.5. Redes Empresariales

Una red es un grupo de ordenadores conectados, y una red empresarial es un grupo de este tipo creado para atender las necesidades de una gran empresa. Las redes empresariales se componen de redes de área local (LAN) que, a su vez, se conectan a redes de área amplia (WAN) y a la nube (s/f-c).

En un entorno empresarial, los centros de datos, las sucursales, las nubes públicas y privadas, los dispositivos del Internet de las Cosas (IoT) y los empleados individuales de una organización necesitan conexiones de red fiables. Estas conexiones permiten que las empresas intercambien datos, ejecuten procesos empresariales y analicen lo que ocurre en la red; básicamente, la red hace posible el funcionamiento de la empresa (s/f-c).

A diferencia de Internet, las redes empresariales no están abiertas a cualquiera que quiera conectarse. Las redes empresariales limitan la conectividad a usuarios, dispositivos e instalaciones específicas. Suelen encriptar los datos que pasan por ellas mediante el uso de redes privadas virtuales (VPN) o encriptación de Transport Layer Security (TLS) (s/f-c).

Las redes empresariales también se diferencian de otros tipos de redes por su escala. Una persona normal puede tener acceso a una LAN doméstica que conecta unos pocos dispositivos a Internet mediante un único enrutador. Pero las empresas tienen redes internas que conectan miles de dispositivos entre sí y con Internet. (Algunas redes empresariales son lo suficientemente grandes y están lo suficientemente conectadas como para que se les asigne un número de sistema autónomo, o ASN: Más información sobre los ASN.) (s/f-c).



Las redes empresariales son sistemas de comunicación que permiten la interconexión de diferentes dispositivos dentro de una organización para facilitar el intercambio de información, recursos y servicios. Estas redes pueden ser cableadas o inalámbricas y se utilizan para mejorar la eficiencia y productividad de la empresa, así como para facilitar la colaboración entre los empleados (s/f-c)

Las redes empresariales pueden incluir diferentes tipos de dispositivos como computadoras, servidores, impresoras, teléfonos, tabletas, entre otros. Además, estas redes pueden estar conectadas a Internet para permitir el acceso a recursos externos y la comunicación con otras organizaciones (s/f-c).

Algunos de los beneficios de tener una red empresarial bien estructurada incluyen la optimización de los procesos internos, la mejora de la comunicación entre los empleados, la seguridad de la información y la posibilidad de acceder a datos en tiempo real. Sin embargo, es importante asegurarse de implementar medidas de seguridad adecuadas para proteger la información sensible de la empresa y prevenir posibles ciberataques (s/f-c).

4.1.6. Redes en la Nube y móviles

Las redes en la nube son el uso de servicios basados en la nube para implementar una red corporativa que conecte a los empleados, los recursos y las aplicaciones de una organización. Tradicionalmente, las



organizaciones utilizaban sus propios componentes de hardware de red privada para crear una red de área extendida (WAN) aislada para una comunicación y una implementación de aplicaciones seguras. Configurar y administrar la red era caro y complicado. Las redes en la nube resuelven estos desafíos al permitir que su organización utilice componentes de redes virtuales en su lugar. Un proveedor externo de servicios en la nube administra y mantiene el hardware y la infraestructura de la red. De esta forma, los administradores de red de su organización pueden centrarse en la eficiencia y en optimizar la configuración (s/f-d).

Las redes en la nube y móviles se refieren a la conexión de dispositivos móviles a la nube, donde la información y los servicios están almacenados y accesibles a través de Internet. Esta tecnología permite a los usuarios acceder a sus datos desde cualquier lugar y en cualquier momento, siempre que tengan una conexión a Internet.

Algunos ejemplos de redes en la nube y móviles incluyen el almacenamiento en la nube, como Dropbox o Google Drive, donde los usuarios pueden guardar sus archivos y acceder a ellos desde sus dispositivos móviles. También existen aplicaciones móviles que utilizan la nube para sincronizar datos entre diferentes dispositivos, como calendarios, contactos o notas.

En resumen, las redes en la nube y móviles facilitan el acceso a la información y los servicios desde cualquier lugar, lo que ha revolucionado la forma en que trabajamos y nos comunicamos en la actualidad.

4.2. Internet

El término Internet se utiliza para hacer referencia a una red de computadoras interconectadas entre sí a nivel mundial con el objetivo de hacer común información de acceso público. Esta red utiliza un lenguaje en común para la comunicación entre los dispositivos (Internet: qué es, qué tipos de conexión existen, s/f).

Internet se vale de protocolos, recursos y servicios para operar a través de diferentes medios de conexión a la red, ya sea por medio de una línea telefónica, un cable o medios más modernos como conexión: 4G (LTE) y 5G, fibra óptica o ADSL (Internet: qué es, qué tipos de conexión existen, s/f).

Para acceder a los sitios web disponibles en Internet se hace uso de navegadores web como Google Chrome, Mozilla Firefox, Internet Explorer, entre otros (Internet: qué es, qué tipos de conexión existen, s/f).



Su nombre proviene del anglicismo International Network of Computers, cuya traducción al español es Red internacional de Computadoras, también denominada como Red Informática Descentralizada de Alcance Global o Red de Redes (Internet: qué es, qué tipos de conexión existen, s/f).

Características del internet

- **Ofrece información las 24 horas del día**, y se puede acceder a ella siempre y cuando la conexión sea posible.
- **Es de carácter público.**
- No pertenece a ningún ente, **es de orden universal y descentralizado**, por lo que no hay puntos de control a nivel jerárquico.
- **Es colaborativo**, es decir, toda persona puede compartir información en Internet.
- **Es de crecimiento ilimitado y colaborativo**, permitiendo nuevas conexiones a la red de forma compartida.
- **Genera rastro a partir de cada interacción** que realizan los usuarios, de manera que se puede ofrecer una experiencia personalizada adaptada a sus intereses y preferencias. No obstante, **es una red anónima** que no exige que los usuarios se identifiquen para su uso.
- **Puede consultarse desde cualquier dispositivo de forma inmediata**, y los mensajes se transmiten de forma instantánea.
- Sus usos pueden ir desde la búsqueda de información, pasando por la investigación, contacto social, comunicación inmediata, educación hasta llegar a operaciones financieras.

(Internet: qué es, qué tipos de conexión existen, s/f).

Tipos de conexión a internet que existen:

1. **Fibra óptica (cable):** se implementan señales luminosas y no eléctricas para codificar la información, permitiendo la transmisión de datos entre nodos.
2. **Líneas telefónicas:** pueden ser convencionales (es decir, que transmiten analógicamente la señal) o digitales (funcionan a través de un adaptador de red).
3. **Redes inalámbricas:** sustituyen a los cables por señales infrarrojas u ondas de radio para la transmisión de la información. Un método común es el LMDS (*Local Multipoint Distribution System*), que se vale de ondas de radio de alta frecuencia.

4. **Satelital:** sistema que se combina con la conexión telefónica para reducir la congestión de las redes terrestres.
5. **Móvil:** se trata de la conexión a través de *smartphones*, ofreciendo un acceso a Internet rápido.
6. **Hotspots de Wi-Fi:** se trata de sitios que ofrecen acceso a Internet por medio de una red local inalámbrica (WLAN) a través de un *router* que se conecta a un proveedor de servicio de Internet. Se utiliza tecnología Wi-Fi para facilitar la conexión de equipos y lograr el intercambio de datos de forma inalámbrica a través de ondas de radio.
7. **ADSL (Línea Digital Asimétrica Suscriptora o Asymmetric Digital Subscriber Line):** este tipo de conexión permite la transmisión digital de datos a alta velocidad a través de una línea telefónica común.
8. **PLC (Conexión por red eléctrica o Power Line Communications):** conexión que se vale de líneas eléctricas para transmitir datos a alta velocidad, a través de instalaciones eléctricas como puntos de acceso. De esta forma, se establecen redes internas para compartir datos entre diferentes dispositivos.

(Internet: qué es, qué tipos de conexión existen, s/f).

4.2.1. Origen del Internet

Internet surge en el año 1969 en Estados Unidos, cuando la Agencia de Proyectos de Investigación Avanzada ARPA, hoy llamada DARPA (Defense Advanced Research Projects Agency), buscó mejorar los sistemas de comunicación en remoto entre su red de computadoras (Internet: qué es, qué tipos de conexión existen, s/f).

No obstante, no es hasta que nace la Red de la Agencia para los Proyectos de Investigación Avanzada (Advanced Research Projects Agency Network) que es posible establecer una red de comunicaciones de alta velocidad con el objetivo de crear una red de computadoras que les permitiera a centros de investigación y defensa mantener contacto de forma remota sin que se viese interrumpido su funcionamiento en caso de que algunos nodos fueran atacados o destruidos (Internet: qué es, qué tipos de conexión existen, s/f).



Para el año 1983 la ARPANET empieza a utilizar protocolos TCP/IP para establecer comunicación entre computadoras. Posteriormente, a finales de los años ochenta se crea el servicio World Wide Web (WWW) que se vale de Internet como medio de

transmisión para la consulta remota de archivos de hipertexto. Esta fue la primera propuesta de uso de computadoras y enlaces para crear una red (Internet: qué es, qué tipos de conexión existen, s/f).

4.2.2. Servicios de Internet

A través de internet hoy en día es posible realizar diversas operaciones ya que son muy variados los servicios que ofrece la red.

El internet nos ofrece muchas opciones con las cuales es posible que nos mantengamos en contacto e intercambiando información con personas de diferentes lugares alrededor del mundo ya sea a través de un correo electrónico, tener conversaciones cara a cara por medio de videollamadas, o tener conversaciones en línea. Los servicios en internet se dividen en dos grupos, los que se ofrecen en tiempo real o síncrono y los que se ofrecen en tiempo diferido o asíncrono.

Los que se ofrecen en tiempo síncrono, los participantes interactúan en el mismo momento en el que tiene lugar la comunicación, como es el caso de la mensajería instantánea, mientras que los que son asíncronos esta interacción no es inmediata y puede tener lugar en diferentes momentos.

A continuación, se enumerarán algunos de los servicios de internet:

- **Los buscadores:** En la actualidad existen millones de paginas web, por lo tanto, es muy complicado encontrar información sobre cualquier tema. Para que sea más sencillo encontrar información existen los llamados buscadores que permiten encontrar determinadas paginas utilizando una combinación de palabras clave y signos. Se introducen los términos que se desean buscar y buscador realiza una búsqueda en su base de datos para encontrar las paginas donde aparecen los términos buscados, ofreciendo la posibilidad de enlazarte directamente con las páginas que tienen los términos. Los buscadores más utilizados son Google, AltaVista y Yahoo!.
- **El correo electrónico:** Este junto con el WWW, es de los servicios mas utilizados en el internet y consiste en intercambiar mensajes entre dos o mas usuarios que utilizan esta red. Las direcciones de correo de os usuarios de internet son únicas. Para poder crear una se requiere de un dominio y un identificador.
- **Los chats:** Estos permiten intercambiar mensajes de texto en tiempo real entre dos o mas personas. Se basan en el sistema IRC (Internet Relay Chat) el cual hace posible que un grupo de usuarios intercambien mensajes escritos. Existen canales temáticos en los que los usuarios se reúnen para hablar sobre un plan determinado, así como es posible establecer canales

privados en los que únicamente pueden participar usuarios determinados. Actualmente se pueden enviar mensajes de audio y video.

- **Foros:** Estos a diferencia de los chats permiten intercambiar mensajes en tiempo diferido es decir que cada mensaje es publicado y posteriormente visualizado, haciendo posible que cualquier persona puede aportar sus ideas y comentarios y observar los comentarios de los demás usuarios. Sus comentarios se van publicando por orden de fecha. Esta aplicación es muy útil para poder mantener discusiones profundas, así como para intercambiar información relevante.
- **Videoconferencia:** Es un tipo de chat en el cual se nos permite integrar la modalidad de audio e imagen haciendo posible comunicarse con personas de distintos lugares. Para que esto sea posible se requiere de una webcam, un micrófono y altavoces para que se pueda mantener la conversación, además mientras se realiza la videollamada se pueden compartir archivos y mensajes escrito.

4.2.3. Direcciones IP

Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

En esencia, las direcciones IP son el identificador que permite el envío de información entre dispositivos en una red. Contienen información de la ubicación y brindan a los dispositivos acceso de comunicación. Internet necesita una forma de diferenciar entre distintas computadoras, enrutadores y sitios web. Las direcciones IP proporcionan una forma de hacerlo y forman una parte esencial de cómo funciona Internet.

Una dirección IP es una cadena de números separados por puntos. Las direcciones IP se expresan como un conjunto de cuatro números, por ejemplo, 192.158.1.38. Cada número del conjunto puede variar de 0 a 255. Por lo tanto, el rango completo de direcciones IP va desde 0.0.0.0 hasta 255.255.255.255.

Las direcciones IP no son aleatorias. La Autoridad de números asignados de Internet (Internet Assigned Numbers Authority, IANA), una división de Internet Corporation para números y nombres asignados (Internet Corporation for Assigned Names and Numbers, ICANN), genera y asigna matemáticamente las direcciones IP.

El uso de direcciones IP normalmente ocurre sin que lo notemos. El proceso funciona de la siguiente manera:

En un principio, el dispositivo se conecta indirectamente a Internet mediante una red conectada a Internet, que luego le otorga acceso al dispositivo.

Cuando estés en casa, esa red probablemente será tu proveedor de servicios de Internet (ISP). En el trabajo, será la red de tu empresa.

Tu ISP asigna la dirección IP al dispositivo.

Tu actividad en Internet pasa por el ISP, el que la redirige a ti mediante tu dirección IP. Dado que te brinda acceso a Internet, es responsabilidad del ISP asignarle una dirección IP a tu dispositivo.

Sin embargo, tu dirección IP puede cambiar. Por ejemplo, la dirección puede cambiar si enciendes o apagas el módem o enrutador. O bien, puedes comunicarte con tu proveedor de servicios de Internet (ISP) para que la cambie en tu nombre.

Cuando estás fuera de casa, por ejemplo, viajando, y llevas tu dispositivo contigo, la dirección IP de tu casa no te sigue. Esto se debe a que utilizarás otra red (Wi-Fi en un hotel, aeropuerto o cafetería, etc.) para acceder a Internet y utilizarás una dirección IP diferente (y temporal) que te asignará el ISP del hotel, el aeropuerto o la cafetería.

Tipos de direcciones IP

Hay diferentes categorías de direcciones IP, y en cada categoría, diferentes tipos.

1. Direcciones IP

Cada individuo o empresa con un plan de servicio de Internet tendrá dos tipos de direcciones IP: sus direcciones IP privadas y su dirección IP pública. Los términos “pública” y “privada” se relacionan con la ubicación de la red, es decir, una dirección IP privada se utiliza dentro de una red, mientras que una pública se utiliza fuera de ella.

2. Direcciones IP privadas

Cada dispositivo que se conecta a tu red de Internet tiene una dirección IP privada. Esto incluye computadoras, teléfonos y tablets, pero también cualquier dispositivo que pueda conectarse mediante Bluetooth, como los altavoces, impresoras o televisores inteligentes.

Con el creciente Internet de las cosas, la cantidad de direcciones IP privadas que tienes en casa probablemente está aumentando. El enrutador necesita una forma de identificar estos artículos por separado y muchos necesitan una forma de reconocerse entre sí.

Por lo tanto, tu enrutador genera direcciones IP privadas que son identificadores únicos para cada dispositivo que los diferencian dentro la red.

3. Direcciones IP públicas

Una dirección IP pública es la dirección principal asociada a toda la red. Si bien cada dispositivo conectado tiene su propia dirección IP, también se incluyen en la dirección IP principal de la red.

Como se describió anteriormente, tu ISP proporciona la dirección IP pública de tu enrutador. Normalmente, los ISP tienen un gran conjunto de direcciones IP que distribuyen a sus clientes.

Tu dirección IP pública es la dirección que todos los dispositivos fuera de tu red de Internet utilizarán para reconocer tu red.

4. Direcciones IP públicas

Las direcciones IP públicas se presentan de dos formas: dinámica y estática.

5. Direcciones IP dinámicas

Las direcciones IP dinámicas cambian de forma automática y con regularidad. Los ISP compran un gran grupo de direcciones IP y las asignan automáticamente a sus clientes.

De forma periódica, reasignan y devuelven las direcciones IP más antiguas al grupo para que las utilicen otros clientes. La explicación detrás de esta estrategia es generar ahorros para el ISP. Automatizar el movimiento regular de las direcciones IP significa que no es necesario realizar acciones específicas para restablecer la dirección IP de un cliente, por ejemplo, si se muda de casa.

También existen beneficios de seguridad, ya que una dirección IP cambiante facilita a los delincuentes el pirateo de la interfaz de red.

6. Direcciones IP estáticas

Por el contrario, las direcciones IP estáticas son siempre las mismas. Una vez que la red asigna una dirección IP, esta permanece igual. La mayoría de las personas y empresas no necesitan una dirección IP estática, pero para las empresas que planean alojar su propio servidor, es fundamental tener una.

Esto se debe a que una dirección IP estática garantiza que los sitios web y las direcciones de correo electrónico vinculados tengan una dirección IP constante, lo que es vital si desea que otros dispositivos puedan encontrarlos de manera predecible en la Web.

Lo que nos lleva al siguiente punto, que es los dos tipos de direcciones IP para sitios web.

Existen dos tipos de direcciones IP para sitios web

En el caso de los propietarios de sitios web que no alojan su propio servidor, y en su lugar dependen de un paquete de alojamiento web (que es el caso de la mayoría

de los sitios web), existen dos tipos de direcciones IP. Estas son direcciones compartidas y direcciones dedicadas.

1. Direcciones IP compartidas

Por lo general, los sitios web que dependen de planes de alojamiento compartidos pertenecientes a los proveedores de alojamiento web serán uno de los numerosos sitios web alojados en el mismo servidor.

Este suele ser el caso cuando se trata de sitios web individuales o sitios web de expertos en la materia (Subject Matter Expert, SME), en los que los volúmenes de tráfico son manejables y los sitios mismos están limitados en términos de la cantidad de páginas, etc.

Los sitios web alojados de esta manera tendrán direcciones IP compartidas.

2. Direcciones IP dedicadas

Algunos planes de alojamiento web tienen la opción de comprar una dirección IP dedicada (o varias). Esto puede facilitar la obtención de un certificado SSL y te permite ejecutar tu propio servidor de protocolo de transferencia de archivos (FTP).

De esta forma, se facilita el uso compartido y la transferencia de archivos con varias personas dentro de una organización y se permiten opciones de uso compartido de FTP anónimo.

Una dirección IP dedicada también te permite acceder a tu sitio web solo con la dirección IP, en lugar del nombre de dominio, lo que resulta útil si deseas desarrollarlo y probarlo antes de registrar tu dominio.

4.2.4. Tipos de dominio

El dominio de internet de una aplicación web es el equivalente a una dirección física del servidor donde está alojado a nuestro servicio. Se conforma de dos elementos principales, el nombre de dominio y la extensión.

Facilita su comprensión el siguiente ejemplo:

La URL principal es ipn.mx, que está compuesta por el nombre del sitio web (ipn) y por la extensión (.mx).

Cuando alguien registra un dominio puede elegir tanto el nombre como la extensión, siempre que esté disponible. Tras el registro, tendremos los derechos de uso teniendo que renovarlo cada cierto tiempo, normalmente de forma anual.

Tipos de dominios

En los dominios de internet no existe un solo tipo, dependiendo de la intención de la plataforma, lugar de origen, función y otras características puede ser de un tipo u otro. De forma general, pueden encontrarse varios de ellos incluidos en la dirección URL.

Los niveles del dominio se separan por puntos, empezando a contar de derecha a izquierda, también se deben diferenciar el nombre de dominio de las extensiones.

Los diferentes tipos de dominio de internet que existen son:

Dominios de Nivel Superior (TLD)

El TLD es el primer nivel en esta clasificación, la extensión es el primer nivel y el nombre de dominio es el segundo nivel. Por tanto, contempla lo que está a la derecha del punto y generalmente se han diferenciado las extensiones de primer nivel entre genéricas y territoriales (gTLD y ccTLD).

Los TLD tienen dos subdivisiones:

Nombres de Dominio Internacionalizados (IDNs) o de Nivel Superior de Código de País

Los gTLDs son los dominios de nivel superior genéricos, en este grupo se pueden encontrar las extensiones más conocidas y comunes: .com, .net, .org, etc.

Las extensiones de los gTLDs en sus inicios iban dirigidas a la creación de un tipo de web temática en concreto, por ejemplo, los .org para organizaciones, .net para empresas tecnológicas, o los .edu para organizaciones educativas. Esta orientación hoy día no sigue vigente, ya que se ha generalizado el uso de extensiones como .com para todo tipo de proyectos.

Dominios Geográficos/Territoriales

Estos tipos de dominios suelen corresponderse con las iniciales del nombre de naciones, Suelen ser utilizados cuando una marca u organización quiere especializarse en una determinada región y proporciona contenido específico para el mismo.

Algunos ejemplos de estos dominios son los terminados en .es de España, .us de Estados Unidos o .pt de Portugal. A veces son utilizados también como subdivisión para la traducción en diferentes idiomas.

Dominios de Segundo Nivel (SLD)

El dominio de segundo nivel o Second Level Domain se encuentra directamente a la izquierda del dominio de primer nivel, siendo usualmente el nombre de la marca, organización o persona en la que se enfoca el sitio. Por ejemplo, en la dirección URL www.openwebinars.net, openwebinars sería el SLD, actuando como identificador en lo que a usuario se refiere.

Dominios de Tercer Nivel (TLD)

El dominio de tercer nivel es aquel tipo de dominio en el que se produce una mezcla entre un dominio de tipo genérico y un dominio específico de país.

Por ejemplo, la combinación .gob.es, indicaría que se trata de una organización gubernamental para España.

Subdominios

Además de los dominios jerárquicos también existen los subdominios, los cuales se pueden describir como anexos o subpartes usualmente del dominio del segundo nivel.

Por ejemplo, si para el sitio www.empresa.com se encuentra una sección importante como un blog, es posible incluir un subdominio en la URL general que lleve a la página de dicho blog directamente. El resultado sería algo parecido a: www.blog.empresa.com.

4.2.5. Nombre de dominio

Un nombre de dominio es una cadena de texto que se asigna a una dirección IP numérica, que se utiliza para acceder a un sitio web desde el software cliente. Dicho de forma más sencilla, un nombre de dominio es el texto que un usuario escribe en una ventana del navegador para llegar a un sitio web concreto. Por ejemplo, el nombre de dominio de Google es "google.com".

La dirección real de un sitio web es una compleja dirección IP numérica (por ejemplo, 192.0.2.2), pero gracias a DNS, los usuarios pueden introducir nombres de dominio fácil de escribir y ser dirigidos a los sitios web que buscan. Este proceso se conoce como búsqueda de DNS.

Todos los nombres de dominio son gestionados por los registros de dominios, que delegan la reserva de estos en los registradores. El que quiera crear un sitio web puede registrar un nombre de dominio en un registrador y, en la actualidad, hay más de 300 millones de nombres de dominio registrados.

4.3. Hardware y software para redes

Las redes informáticas tienen un papel fundamental en nuestro día a día y, actualmente, podemos usarlas en entornos laborales, centros comerciales e incluso lugares públicos. Tal y como hemos explicado, además de información las redes informáticas permiten compartir elementos de hardware (es decir, si uno de los ordenadores tiene un dispositivo como una impresora todos pueden usarlo) y de software (algunos programas pueden instalarse en un único ordenador y ser usados por el resto de los ordenadores de la red).

A nivel empresarial, las redes informáticas son sinónimo de eficacia y productividad, ya que son la forma más rápida y sencilla para compartir contenidos o datos entre compañeros o en diferentes departamentos. Las redes informáticas también son muy útiles en instituciones públicas y en centros de formación como universidades, colegios o bibliotecas.

Las redes de computadoras están conectadas tanto por hardware y por software. Los elementos que forman parte del hardware son equipos informáticos (tarjetas de red, routers, repetidores) y medios de interconexión (servidores y estaciones de trabajo). El software incluye los controladores y programas empleados para gestionar los dispositivos y el sistema operativo de la red en sí mismo.

Los principales elementos necesarios para instalar una red informática son:

- **Tarjetas de conexión a la red**
Las tarjetas de red son dispositivos electrónicos que permiten la interconexión de varios ordenadores y/o máquinas. Su aspecto puede variar. Por ejemplo, la tarjeta de red de un ordenador es una placa electrónica que se pincha a la placa madre. Una placa madre (Motherboard), a su vez, es una placa situada dentro de los ordenadores y a la que se conectan el resto de los componentes del sistema (memoria, microprocesador, disco duro, tarjeta gráfica, etc.).
Hoy en día existen diferentes tipos de tarjetas de red según la velocidad que soportan, los protocolos con los que trabajan, o el tipo de red que la forman parte. Las más habituales son las tarjetas de red Ethernet, las tarjetas Wifi y las tarjetas Token Ring.
- **Estaciones de trabajo**
Las estaciones de trabajo (Workstation) son otro de los elementos necesarios para instalar una red informática. Éstas son las computadoras que están conectadas directamente a la tarjeta de red, convirtiéndose en nodos o módulos de ésta.

Estos equipos pueden ser computadores personales, aunque tienen una capacidad de procesamiento, cálculo y gráfico superior a los equipos de escritorio de uso personal.

- **Servidores**

Los servidores son ordenadores encargados de suministrar información (archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc.) al resto de equipos conectados a la red. Existen diferentes tipos de servidores (de archivos, de correo, de almacenamiento, de fax, etc.) Dicho de manera coloquial, un servidor funciona como cerebro de la red informática. Actualmente muchas empresas contratan cloud servers (servidores en la nube), que permiten trasladar las herramientas de los servidores al mundo virtual mejorando su funcionalidad.

- **Repetidores**

Entre los elementos necesarios para instalar una red informática también se encuentran los repetidores. Un repetidor es un dispositivo que permite mejorar la señal de una red inalámbrica Wifi. Los repetidores se conectan de manera inalámbrica y su funcionamiento es relativamente sencillo: reciben la señal de otros equipos y la emiten, amplificándola tanto que pueden cubrir distancias muy amplias.

- **Bridges (puentes de conexión)**

Los puentes de red son dispositivos que permiten interconectar dos o más redes. Estos dispositivos se construyen en el estándar de IEEE 802.11 y pueden ser locales (para enlazar redes cercanas) o remotos (permiten enlazar varias redes locales para formar un área más extensa).

- **Routers**

Los enrutadores (routers) son los elementos del sistema de las redes informáticas encargados de transmitir la información. Gracias a las direcciones IP, el router sabe a qué máquina debe mandar cada paquete de datos. Los routers son más rápidos que otros sistemas de distribución de información como los switches. Además, se consideran dispositivos inteligentes porque tienen varias interfaces y pueden reconocer las redes directamente conectadas a él.

- **Concentradores**

Un Hub o concentrador es un elemento necesario para instalar una red informática. Se trata de hardware que forma parte de las redes informáticas y que sirve para conectar equipos entre sí. Su objetivo es concentrar el tráfico de red que proviene de múltiples host y regenerar la señal siguiendo este proceso: primero recupera los datos binarios que ingresan en un puerto y después los envía al resto de puertos; de ahí que a veces también se le denomine <repetidor multipuertos>.

4.3.1. Tipos de servidores

Los servidores son equipos informáticos que almacenan y distribuyen información a otros dispositivos o aplicaciones que se conectan a ellos. Existen diferentes tipos de servidores según diferentes clasificaciones, como el tipo de cliente, el software, el hardware o el tipo de servicio. Los servidores son esenciales para el funcionamiento de Internet y de muchas organizaciones que dependen de ellos para gestionar sus datos y comunicaciones.

- Servidores de archivos

Los servidores de archivos almacenan y distribuyen ficheros que varios clientes o usuarios pueden compartir. Además, el almacenamiento centralizado de archivos ofrece soluciones de copia de seguridad o tolerancia a fallos de forma más sencilla que tratar de proporcionar seguridad e integridad a los archivos en todos y cada uno de los dispositivos de la organización. Se puede diseñar el hardware del servidor de archivos de modo que potencie las velocidades de lectura y escritura para mejorar el rendimiento.

- Servidores de impresión

Los servidores de impresión permiten la gestión y distribución de la funcionalidad de imprimir documentos. Para no tener que conectar una impresora a cada estación de trabajo, podemos tener un único servidor de impresión para responder a las solicitudes de impresión de numerosos clientes. Hoy en día, algunas impresoras de alta gama y gran tamaño vienen con su propio servidor de impresión incorporado, ahorrando la necesidad de instalar uno en un equipo separado. Este servidor de impresión interno hace que la impresora responda también a las solicitudes de impresión de los clientes conectados.

- Servidores de aplicaciones

Este tipo de servidores sirve para ejecutar aplicaciones de forma remota, en lugar de que los equipos cliente lo hagan localmente. Los servidores de aplicaciones a menudo ejecutan software que hace un uso intensivo de los recursos, y lo comparten para una gran cantidad de usuarios. Al hacerlo, por un lado, solo tenemos que instalar y mantener el software en una única máquina, y evitamos la necesidad de que cada cliente disponga de suficientes recursos de forma local.

- Servidores DNS

Los servidores del sistema de nombres de dominio (DNS) son servidores de aplicaciones que proporcionan funcionalidades de resolución de nombres a los equipos cliente. La resolución de nombres consiste en convertir nombres fácilmente comprensibles por los humanos en direcciones IP legibles por las máquinas. El sistema DNS es una base de datos ampliamente distribuida de nombres y otros servidores DNS a los que se puede consultar para obtener un nombre de equipo

desconocido. Cuando un cliente necesita la dirección de un sistema, envía una solicitud con el nombre del recurso deseado a un servidor de DNS, que le responde con la dirección IP correspondiente de su tabla de nombres.

- Servidores de correo

Los servidores de correo son un tipo muy común de servidor de aplicaciones. Los servidores de correo reciben los mensajes de correo electrónico que se remiten a un usuario y los almacenan hasta que un cliente los solicite en nombre de dicho usuario. Disponer de un servidor de correo electrónico nos permite tener una sola máquina configurada y conectada correctamente a la red en todo momento, lista para enviar y recibir mensajes en lugar de esperar que cada cliente tenga su propio subsistema de correo electrónico ejecutándose de forma continua.

- Servidores web

Uno de los tipos de servidores más abundantes en el mercado actual son los servidores web. Un servidor web es un tipo especial de servidor de aplicaciones que aloja programas y datos solicitados por los usuarios a través de internet o en una intranet. Los servidores web responden a las solicitudes de páginas web u otros servicios basados en la web que llegan de los navegadores que se ejecutan en los ordenadores cliente. Entre los servidores web que podemos encontrar más frecuentemente tenemos servidores Apache, Microsoft Internet Information Services (IIS) y Nginx.

- Servidor de base de datos

La cantidad de datos utilizados por empresas, usuarios y otros servicios es sobrecogedora. Gran parte de ellos se almacena en bases de datos. Estas bases de datos deben poder ser accesibles por parte de múltiples clientes en cualquier momento y, generalmente, exigen cantidades extraordinarias de espacio de almacenamiento. Ambas necesidades son la excusa perfecta para ubicar dichas bases de datos en un servidor. Los servidores de bases de datos ejecutan aplicaciones de bases de datos y responden a numerosas solicitudes de clientes. Los servidores de bases de datos más frecuentes son Oracle, Microsoft SQL Server, DB2 e Informix.

- Servidores virtuales

Los servidores virtuales están arrasando en el mundo de los servidores. A diferencia de los servidores tradicionales, que se instalan como una dupla de sistema operativo y máquina de hardware, los servidores virtuales solo existen según los parámetros establecidos en un software especializado denominado hipervisor. Cada hipervisor puede ejecutar cientos o incluso miles de servidores virtuales a la vez. El hipervisor presenta el hardware virtual al servidor como si de una máquina física se tratase. El

servidor virtual usa el hardware virtual como de costumbre, y el hipervisor traslada las necesidades reales de computación y almacenamiento al hardware real subyacente que se comparte entre todos los demás servidores virtuales.

- Servidores proxy

Un servidor proxy actúa como intermediario entre un cliente y un servidor. A menudo se emplean para aislar a clientes o servidores por motivos de seguridad. Un servidor proxy toma la solicitud del cliente, pero, en lugar de responderle directamente, traslada la solicitud a otro servidor o proceso. El servidor proxy recibe la respuesta del segundo servidor y, luego, responde al cliente original como si lo hiciera por sí mismo. De este modo, ni el cliente ni el servidor que se comunican realmente se conectan entre sí.

- Servidores de supervisión y administración

Algunos servidores tienen la finalidad de supervisar o gestionar otros sistemas y clientes. Hay muchos tipos de servidores de supervisión. Algunos de ellos escuchan la red, recibiendo cada solicitud del cliente y cada respuesta del servidor, pero otros ni solicitan ni responden a los datos por sí mismos. De este modo, el servidor de supervisión puede realizar un seguimiento de todo el tráfico en la red, así como de las solicitudes y respuestas de otros servidores y clientes sin interferir con tales operaciones. Un servidor de supervisión responderá a las solicitudes de monitorización de los clientes, como aquellas que ejecutan los administradores de red cuando vigilan el estado de la red.

- Estructuras de servidor

El concepto del servidor es casi tan antiguo como el de la red. Después de todo, el objetivo de una red es permitir que un equipo se comuniquen con otro de forma que se distribuya el trabajo o los recursos. La informática ha evolucionado mucho desde entonces, dando como resultado diferentes tipos de estructuras de servidor y hardware.

- Mainframe o minicomputadora (AS/400)

Se podría decir que los servidores originales, los equipos de mainframe y, más tarde, las minicomputadoras, se encargaban de gestionar casi todas las tareas operativas exceptuando la interacción con el usuario a través de una pantalla y un teclado, que se dejaba a los sistemas cliente.

- Servidor de hardware

La siguiente gran ola de servidores comprendía servidores basados en ordenadores. En muchos aspectos, estos no eran más que ordenadores de

escritorio, pero más grandes y potentes. Generalmente, también eran más caros y tenían mucha más memoria y espacio en disco que la mayoría de los equipos cliente. Cada servidor seguía siendo una unidad autónoma con su propia placa base, procesador, memoria, unidades de disco y fuente de alimentación. A menudo, este tipo de servidores se almacenaba en estancias con aire acondicionado denominadas salas de servidores y, luego, se atornillaban en bastidores o racks para un mejor almacenamiento y accesibilidad.

- Servidores Blade

Los servidores de hardware originales ocupaban mucho espacio y se almacenaban en bastidores que podían pesar toneladas. Sin embargo, con el tiempo, la aparición de medios de transferencia más rápidos en el hardware provocó la extracción de partes de esos servidores autónomos. Gracias a la posibilidad de eliminar los discos duros, quitar el sistema de refrigeración interna y miniaturizar de forma continua los componentes computacionales, los servidores se acabaron reduciendo a un único “servidor delgado” conocido como servidor Blade. Aunque se siguen almacenando en bastidores dentro de las salas de servidores, los Blade son más pequeños y se pueden reemplazar más fácilmente.

- Combinar servidores

Ya se buscaba separar los servidores del modelo estándar de máquina de hardware individual con sistema operativo propio antes de que la virtualización entrara en escena. Los avances tecnológicos, como la funcionalidad de almacenamiento conectado a la red, eliminaron la necesidad de que un servidor tuviera su propio sistema de almacenamiento. Otras tecnologías, como el mirroring y los clústeres, permitieron combinar partes de hardware en servidores más grandes y potentes que podían estar compuestos de diferentes blades, varios dispositivos de almacenamiento conectados y una fuente de alimentación externa, y cada uno de estos módulos podía intercambiarse por otro mientras el servidor seguía en funcionamiento.

- Servidores virtuales

Los servidores virtuales siguen necesitando de una capa de hardware, pero dicha capa ejecuta ahora un proceso diferente conocido como hipervisor. En algunos casos, como Hyper-V de Microsoft, tenemos un sistema operativo completo que se ejecuta sobre el propio hardware. En otros casos, los llamados “hipervisores bare-metal” se pueden instalar directamente en el hardware del servidor. En ambos casos, el hardware como tal suele extenderse a través de múltiples servidores blade, sistemas de almacenamiento en red y fuentes de alimentación, lo que produce un entorno en el cual es imposible saber dónde termina un servidor individual y dónde comienza otro.

- Microsoft Windows Server

Podría decirse que Windows para trabajo en grupo (Windows for Workgroups) fue el primer sistema operativo de servidores de Microsoft. En esa versión, ciertos ordenadores podían configurarse para compartir recursos y responder a las solicitudes de los clientes, lo que los convertía en servidores, por definición. El primer sistema operativo de servidores de verdad de Microsoft fue Windows NT. Sus versiones 3.5 y 3.51 podían encontrarse en muchas redes comerciales hasta que Microsoft lanzó su línea Windows Server, que continúa existiendo hoy en día. La versión más actual es Windows Server 2016, que admite numerosas aplicaciones y bases de datos, así como un hipervisor que permite servidores virtuales.

- Servidores Linux/Unix

El otro actor principal de los sistemas operativos de servidores es Linux/Unix. Podemos encontrarlo en múltiples versiones y de todos los colores, como Red Hat Enterprise Linux, Debian y CentOS como algunos de los más famosos. Al ser un sistema operativo de código abierto, Linux es muy popular como servidor web, generalmente con una instalación del servidor web Apache.

- Servidores en la nube

Aquellos servidores virtuales alojados en una infraestructura de terceros en una red abierta, como internet, se denominan servidores en la nube. En la actualidad, existen numerosos proveedores de servidores en la nube como Google Cloud Platform, Microsoft Azure e IBM Cloud. Sin embargo, el principal pionero en el campo de la computación en la nube corporativa fue la plataforma AWS de Amazon. Comenzó usando la capacidad libre de los propios servidores y redes de Amazon, y actualmente AWS ahora permite a sus clientes crear un servidor virtual casi instantáneamente y, luego, ajustar la cantidad de recursos que dicho servidor puede utilizar sobre la marcha. Hoy en día, un servidor puede no ser más que un conjunto de datos del hardware físico, compuesto por multitud de procesadores, unidades de disco, memoria y conexiones de red. No obstante, en el fondo, un servidor sigue siendo simplemente un sistema que responde a una solicitud de un cliente.

4.3.2. Dispositivos de comunicación

Los dispositivos de comunicación son aparatos que generan y/o reciben señales analógicas o digitales, permitiendo el intercambio de información. Estos medios fueron creados por el ser humano a lo largo de su evolución histórica.

En sentido amplio, un dispositivo de comunicación es cualquier aparato que pueda ser empleado para transmitir un mensaje. En tiempos actuales se constituyen como los principales protagonistas de las tecnologías de la comunicación (TIC).

Las computadoras u ordenadores son los más representativos dispositivos de comunicación. Estas máquinas electrónicas han sido diseñadas para recibir, procesar datos y convertirlos en información.

1- El módem: Es un dispositivo que transforma las señales digitales en analógicas a través de un proceso denominado modulación, y las analógicas en digitales a través de la desmodulación.

Su función es enviar la señal moduladora a través de otra señal denominada portadora. El módem surgió a raíz de la necesidad de comunicar computadoras para compartir datos entre ellas.

2- El switch: Es un aparato digital que sirve para la interconexión de equipos computarizados, o de segmentos de una red conformada por estos. También se le denomina conmutador.

Opera de manera lógica fusionando tramos de una misma red, filtrando la información para así optimizarla en cuanto a rendimiento y seguridad.

3- El router: También es llamado enrutador o encaminador de paquetes. Este dispositivo permite el uso de varias direcciones IP dentro de una misma red, permitiendo la creación de subredes.

4- El teléfono celular: Es un dispositivo electrónico inalámbrico de acceso a la telefonía móvil. Se llama celular debido a que cada una de las antenas repetidoras que forman parte de la red está compuesta de células.

5- Dispositivos de larga distancia: Este tipo de dispositivos se conectan a través de una red elaborada que logra la comunicación a larga distancia por poseer una LAN incorporada.

Las llamadas telefónicas de larga distancia ocurren por la modulación digital de señales de portadoras analógicas.

6- Telefonía satelital: Los teléfonos satelitales permiten la comunicación eficiente en los lugares más remotos de la Tierra.

Estos dispositivos usan la misma tecnología móvil ubicando los satélites de órbita baja que giran en el espacio.

Al establecerse el enlace al satélite, la señal se redirige a una estación de comunicación en la tierra.

7- Basados en VOIP: La tecnología VoIP consiste en la transmisión de señales telefónicas de ida y vuelta a través de Internet.

Las conversaciones telefónicas basadas en dispositivos de esta tecnología son más nítidas comparadas con la telefonía convencional.

8- El GPS: Este aparato permite determinar la posición exacta y precisa de un objeto en la Tierra. Se utiliza para la localización de niños, ancianos y personas con discapacidad.

También se usa para la ubicación de vehículos como medida preventiva contra robos.

9- Dispositivos aumentativos: Aumentativos o de asistencia, son dispositivos de comunicación que dan voz a las personas que padecen discapacidades, permitiéndoles expresarse sin necesidad de ser asistidos por otras personas.

10- Bluetooth: Los dispositivos Bluetooth permiten conectar varios equipos entre sí a pequeña distancia, con la peculiaridad de que se puede prescindir de cualquier tipo de cableado. Gracias a sus ondas de radio de baja frecuencia, podemos intercambiar información a una gran velocidad de manera cómoda.

11- Infrarrojos: Antes de que Bluetooth se desarrollase, los infrarrojos eran los principales transmisores de datos libre de cables. Sin embargo, su tecnología era poco potente, ya que requería que los dispositivos debían estar prácticamente pegados y la velocidad de transmisión no era especialmente rápida.

12- FAX: A partir de la señal telefónica, el FAX podía transmitir documentos y otros tipos de textos de un dispositivo a otro a amplias distancias. Era la evolución del teletipo, funcionando como una fotocopidora. Sin embargo, las nuevas tecnologías han lo han dejado en desuso.

4.3.3. Medios alámbricos e inalámbrico

Medios de transmisión inalámbricos.

Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión. Estos dispositivos pueden ser de muy variadas formas y tecnologías entre ellos:

- Computadoras de escritorio.
- Teléfonos celulares.
- Asistentes digitales personales (PDA).
- Access Point (encargado de permitir a los dispositivos inalámbricos el acceso a la red).
- Computadoras portátiles: Laptop, Netbook y Notebook.

Tecnologías actuales para la red inalámbrica.

- Wi-Fi (Wireless Fidelity): en lenguajes español significa literalmente fidelidad sin cables. También se les denomina WLAN (Wireless Local Area Network) o redes de área local inalámbricas. Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m).
- Infrarrojo (Ir): se trata de una tecnología de transmisión inalámbrica por medio de ondas de calor a corta distancia (hasta 1 m), capaces de traspasar cristales.
- BlueTooth: en lenguajes español significa literalmente diente azul, ello por ser un nombre de un Rey de la antigüedad. Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio de corto alcance (1,20 y 100 m a la redonda dependiendo la versión). Las ondas pueden incluso ser capaces de cruzar cierto tipo de materiales, incluyendo muros.
- Láser: son tecnologías de muy alta velocidad, basadas en el envío de datos en grandes regiones por medio de un haz de luz láser emitida por un diodo especial (hasta 5 km de distancia) y un fotodiodo que reciba las señales.

Medios de transmisión alámbricos.

La función de los medios de transmisión alámbricos es la de transportar paquetes de bits de una máquina a otra. Hay distintos tipos de medios alámbricos.

- Líneas de par trenzado.
 - Cable Coaxial.
 - Fibra Óptica.
-
- Líneas de par trenzado: Consiste en 2 cables de cobre aislados y trenzados para reducir la interferencia eléctrica externa y de pares adyacentes. Dos cables forman una antena. Si se trenzan se reduce la diafonía.
 - Cable coaxial: Es un conductor central protegido por un aislante, sobre este está un segundo conductor trenzado (como una fina malla).
 - Fibra Óptica: Está formada por un núcleo central de vidrio rodeado por varias capas de protección. El modo de transmisión es óptico en vez de eléctrico.

Puede transmitir señales a distancias mucho más largas que con el par trenzado y el cable coaxial. Puede alcanzar velocidades muy grandes (miles de MHz).

4.3.4. Diseño de sitios web con aplicaciones

El diseño web implica trabajo relacionado con el layout y diseño de páginas online, así como la producción de contenido, aunque generalmente se aplica a la creación de sitios web.

En este caso, los diseñadores web crean las páginas utilizando lenguajes de marcado como HTML o XML.

Por otro lado, la parte visual de los sitios está a cargo del CSS, término utilizado para estilizar los elementos escritos en HTML.

Por lo tanto, es común que los diseñadores web utilicen ambos para construir un site porque juntos definirán cómo aparecerán las páginas en los navegadores.

El proceso de creación de sitios se puede realizar desde herramientas como Adobe Dreamweaver (que requerirá que el profesional sepa más sobre los códigos) y CMS que son plataformas de administración de contenido.

WordPress es uno de los más conocidos y prácticos porque tiene una serie de templates que pueden basar el sitio. El web designer tiene la tarea de instalarlos y personalizarlos según lo que cada cliente

Cuando hablamos de un buen diseño web, algunos puntos son fundamentales y no pueden faltar en tu sitio. Aquí están los aspectos más destacados:

Responsividad

Como cada vez más las personas acceden a internet solo por teléfono celular, es muy importante que tu sitio sea adecuado para dispositivos móviles, es decir, que sea responsivo.

Escaneabilidad

La escaneabilidad es la facilidad para encontrar de un vistazo elementos de un todo, en nuestro caso una pantalla. Es decir, que los elementos de la interfaz puedan ser diferenciados e identificados fácilmente.

Tipografía

La tipografía web no es más que el tipo de letra que usamos en una web.

Esto incluye además de la fuente, el tamaño, color y formato de la letra que aplicaremos en todo el conjunto de nuestra web.

Velocidad de carga

En un mundo donde todos parecen estar siempre apurados, tener un sitio web de carga rápida es esencial. Según Google, los sitios que tardan más de 2 segundos en cargarse dañan tanto la experiencia del usuario como la indexación del sitio.

4.3.5. Aplicaciones empresariales en la red

Una aplicación empresarial es una colección de componentes que proporciona una funcionalidad empresarial que se puede utilizar internamente, externamente o con otras aplicaciones empresariales. Puede crear aplicaciones empresariales de componentes individuales, que están relacionados entre sí.

Por ejemplo, Gestión de pedidos, Gestión de inventario y Facturación son aplicaciones empresariales que pueden utilizar componentes individuales como un servidor de aplicaciones Java EE, LDAP y una base de datos que se ejecuta en el servidor de Solaris.

Una aplicación empresarial es un tipo de colección personalizada. También puede crear los siguientes tipos de colecciones personalizadas:

Colección, que es un grupo de recursos que se pueden seleccionar de acuerdo con las necesidades.

Colección de accesos, que es una colección que se utiliza para controlar el acceso a elementos de configuración (CI) y permisos para modificar elementos de configuración. Puede crear recopilaciones de acceso sólo cuando la seguridad a nivel de datos está habilitada.

Se proporcionan los siguientes métodos para crear aplicaciones empresariales:

- Utilizando modelos de agrupación en Data Management Portal.
- Utilizando descriptores de aplicación.
- Utilizando modelos de agrupación creados con la API de Java y cargados por el programa de carga masiva.

Funciones de las aplicaciones para negocios

Organiza la información

Digitalizar los documentos de tu negocio facilitará su administración y será más sencillo tener acceso a ellos en cualquier momento y desde cualquier lugar.

Usa las aplicaciones de negocios de manera intuitiva

Este tipo de aplicaciones están desarrolladas para que su uso sea sencillo y cualquier persona pueda hacer distintas operaciones convenientes para el negocio.

Trabaja en equipo

Las aplicaciones empresariales te permiten mejorar la colaboración con tu equipo al tener la posibilidad de compartir información relevante, resolver dudas u optimizar los procesos de trabajo.

Reduce costos

Generalmente las aplicaciones para negocios ofrecen automatizaciones para agilizar tareas cotidianas y evitar la duplicidad o trabajo extra de las personas. De esta manera, pueden enfocar sus esfuerzos en otras actividades de mayor importancia.

Mejora la comunicación

A través de estas herramientas digitales tienes la posibilidad de incrementar positivamente la comunicación con tu equipo y clientes.

Dale seguimiento a los proyectos

Con estas aplicaciones para negocios puedes tener un registro de todas las actividades realizadas dentro del equipo o peticiones por parte del cliente para evitar malentendidos.

Videos de apoyo:

- <https://www.youtube.com/watch?v=01WulhAY6Ts>
- <https://www.youtube.com/watch?v=801xu7tGEfA>
- <https://www.youtube.com/watch?v=9A6IKGXKkzU>
- <https://www.youtube.com/watch?v=O-OHTvMldgw>

Bibliografía:

Abril, 19. (2022, abril 19). Las redes satelitales tienen una comunicación de datos muy compleja. axessnet. <https://axessnet.com/las-redes-satelitales/>

De Oliveira Gomes, T. (2023, marzo 17). Redes sem fio - Definição, uso, aplicações e tecnologias. Linkedin.com. <https://pt.linkedin.com/pulse/redes-sem-fio-defini%C3%A7%C3%A3o-uso-aplica%C3%A7%C3%B5es-e-thales-de-oliveira-gomes>

Duo for AnyConnect VPN Overview Video. (2019, abril 17).

International IT. (2021, septiembre 28). Topología de Red: conozca los principales tipos. International IT. <https://www.internationalit.com/post/topologia-de-red-conozca-los-principales-tipos?lang=es>

Internet: qué es, qué tipos de conexión existen. (s/f). Ferrovial. Recuperado el 5 de abril de 2024, de <https://www.ferrovial.com/es/stem/internet/>

Perfil, V. T. mi. (s/f). METODOLOGÍAS DE REDES. Blogspot.com. Recuperado el 5 de abril de 2024, de <https://metodologiasredes.blogspot.com/>

¿Qué es un protocolo de red? (2022, mayo 3). Autmix.com. <https://autmix.com/blog/que-es-protocolo-red>

(S/f-a). Com.br. Recuperado el 5 de abril de 2024, de <https://www.capterra.com.br/glossary/339/packet-switched-network>

(S/f-b). Cloudflare.com. Recuperado el 5 de abril de 2024, de <https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-protocol/>

(S/f-c). Cloudflare.com. Recuperado el 5 de abril de 2024, de <https://www.cloudflare.com/es-es/learning/network-layer/enterprise-networking/>

(S/f-d). Amazon.com. Recuperado el 5 de abril de 2024, de <https://aws.amazon.com/es/what-is/cloud-networking/>

Artigas, S. G. (25 de Febrero de 2022). *torresburriel estudio*. Obtenido de <https://torresburriel.com/weblog/producto-digital-escaneable/#:~:text=La%20escaneabilidad%20es%20la%20facilidad,ser%20diferenciados%20e%20identificados%20f%C3%A1cilmente>.

Barragán, A. (9 de Julio de 2021). *openwebinars*. Obtenido de <https://openwebinars.net/blog/que-es-un-dominio-de-internet-y-tipos-que-existen/>

BBVA. (s.f.). Obtenido de <https://www.bbva.mx/educacion-financiera/blog/aplicaciones-empresariales.html>

Civera Electrificaciones, S,L. (11 de Octubre de 2019). Obtenido de <https://civeraelectrificaciones.com/que-elementos-son-necesarios-para-instalar-una-red-informatica/>

Cloudflare. (s.f.). Obtenido de <https://www.cloudflare.com/es-es/learning/dns/glossary/what-is-a-domain-name/>

Hiru.eus. (s.f.). Obtenido de <https://www.hiru.eus/es/tecnologias-para-la-informacion-y-la-comunicacion/servicios-de-internet>

Kaspersky. (s.f.). Obtenido de <https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address>

KYOCERA Document Solutions. (s.f.). Obtenido de <https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/insights-hub/articles/tipos-de-servidores-para-empresas.html>

Murillo, N. (19 de septiembre de 2022). *Lifeder*. Obtenido de <https://www.lifeder.com/dispositivos-comunicacion/>

paessler. (s.f.). Obtenido de <https://www.paessler.com/es/it-explained/server>

Rockcontent. (s.f.). Obtenido de <https://rockcontent.com/es/blog/disenio-web/>

Slack . (s.f.). Obtenido de <https://slack.com/intl/es-es/blog/collaboration/mensajeria-instantanea-comunicacion-sincronica-y-asincronica-diferencias>

Terzakyan, T. (15 de Marzo de 2022). *Deel*. Obtenido de <https://www.deel.com/es/blog/comunicacion-sincronica-y-asincronica>

Yañez, C. (31 de Enero de 2020). *Deusto Formacion* . Obtenido de <https://www.deustoformacion.com/blog/disenio-produccion-audiovisual/importancia-tipografia-hacer-web#:~:text=%C2%BFQu%C3%A9%20es%20la%20tipograf%C3%ADa%20web,el%20conjunto%20de%20nuestra%20web>