

Puntos mínimos a desarrollar en el trabajo.

1. Conceptos básicos de redes

- a. Concepto: Red. Red de comunicación. Ejemplos de redes de comunicación.

Red: Una red de computadoras, también llamada red de ordenadores o red informática es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.)

Red de comunicación: es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían impulsos electromagnéticos con el fin de compartir datos, recursos y ofrecer servicios.

Algunos ejemplos de redes de comunicación son internet, redes locales(lan), de area amplia(wan), de área metropolitana(man), intranets, etc.

- b. Concepto: Telemática, ejemplos de procesos telemáticos.

La telemática es un campo interdisciplinario que combina las tecnologías de la información y las telecomunicaciones para gestionar y controlar sistemas a distancia.

Algunos ejemplos de procesos telemáticos son:

1. **Telemedicina:** La consulta médica a distancia, el diagnóstico y el seguimiento de pacientes a través de videoconferencias y aplicaciones de telemedicina.
2. **Domótica:** El control de sistemas de seguridad, iluminación, calefacción y electrodomésticos en el hogar a través de dispositivos móviles o interfaces web.
3. **Teletrabajo:** La realización de tareas laborales desde casa o lugares remotos, utilizando herramientas de comunicación y colaboración en línea.
4. **Educación a Distancia:** La entrega de cursos en línea, la realización de videoconferencias y la colaboración en proyectos educativos a través de plataformas digitales.
5. **Logística y Cadena de Suministro:** La gestión de inventarios, seguimiento de envíos y planificación de rutas mediante sistemas telemáticos para una distribución más eficiente.

Entre muchos otros.

c. Componentes de una red de comunicación.

i. Conceptos: información, transmisión y comunicación.

- **Información:** Desde el punto de vista de la ciencia de la computación, la información, es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno.
- **Transmisión:** Se entiende por transmisión de datos al movimiento de información codificada, de un punto a uno más puntos, mediante señales eléctricas, ópticas, electromagnéticas o electroópticas.
- **Comunicación:** es la transferencia de información o datos mediante señales digitales a través de un canal punto a punto.

ii. Elementos de la comunicación

Los elementos básicos de la comunicación en informática son:

- **Emisor:** Quien envía el mensaje.
- **Receptor:** Quien recibe el mensaje.
- **Mensaje:** La información transmitida.
- **Canal:** El medio de comunicación (como internet).
- **Código:** El sistema de signos utilizado.
- **Contexto:** El entorno tecnológico.
- **Ruido:** Interferencias en la comunicación.
- **Retroalimentación:** Respuesta del receptor al emisor.

iii. Circuito de datos:

1. Tipos de señales de comunicación

- **Señales Analógicas:** Estas señales varían continuamente en amplitud y tiempo.
- **Señales Digitales:** Estas señales son discretas y representadas mediante una secuencia de dígitos binarios (0 y 1).
- **Señales Unipolares y Bipolares:** Las señales unipolares tienen valores en un solo lado de la línea base, generalmente positivos.
- **Señales Analógicas Moduladas:** Estas señales combinan una señal analógica con una portadora (señal de alta frecuencia) para transmitir información.
- **Señales Digitales Moduladas:** En este caso, señales digitales se modulan en una portadora para su transmisión.
- **Señales de Tiempo Continuo y de Tiempo Discreto:** Las señales de tiempo continuo varían en cualquier momento, mientras que las señales de tiempo discreto solo toman valores en momentos específicos.
- **Señales de Banda Base y Señales de Banda Ancha:** Las señales de banda base representan directamente la información (por ejemplo, una señal de audio), mientras que las señales de banda ancha se generan a partir de señales de banda base mediante modulación.

- **Señales de Datos y Señales de Control:** Las señales de datos contienen la información que se transmite, mientras que las señales de control se utilizan para gestionar la transmisión y asegurar la integridad de los datos.

2. Transmisión de señales analógicas por redes digitales

La transmisión de señales analógicas por redes digitales es un proceso en el que se convierten señales analógicas en señales digitales para ser transmitidas a través de una red de comunicación digital. Esto se hace mediante un proceso llamado "digitalización" o "muestreo".

3. Transmisión de señales digitales por redes analógicas

La transmisión de señales digitales por redes analógicas implica enviar datos digitales a través de un medio que normalmente maneja señales analógicas. Esto se logra mediante un proceso llamado modulación, que convierte las señales digitales en una forma adecuada para su transmisión sobre una red analógica.

4. Modos de transmisión

- Según el número de unidades de datos que se pueden enviar de manera simultánea.
 - Paralelo
 - Serie
- Según su sincronización
 - Síncrona
 - Asíncrona
- Según su direccionamiento
 - Simplex
 - Half Duplex
 - Full Duplex

[Referencia:](http://textoscientificos.com) textoscientificos.com

2. Redes Informáticas

a. Origen y evolución de las Redes Informáticas.

Se puede decir que las redes informáticas tal y como las conocemos hoy en día empezaron con el desarrollo de ARPANET a finales de la década de los 60's. Algo con lo que ya se había teorizado desde muchos años antes, pero que culminó en 1969 con la primera transferencia de datos entre dos ordenadores situados a más de 600km de distancia.

Antes de ese momento, existían redes de proveedores de ordenadores diseñadas principalmente para conectar terminales o estaciones de trabajo remotas a un ordenador central.

b. Ventajas e inconvenientes del uso de redes. ¿Qué podemos compartir?

Ventajas de las redes informáticas:

Comunicación eficiente: Permiten la comunicación rápida y eficiente entre usuarios, dispositivos y sistemas, independientemente de la ubicación física.

Compartir recursos: Las redes permiten compartir recursos, como impresoras, archivos y bases de datos, lo que ahorra costos y mejora la productividad.

Acceso a información y servicios en línea: Facilitan el acceso a información y servicios en línea, incluyendo la World Wide Web, correo electrónico y sistemas de gestión de bases de datos.

Flexibilidad y escalabilidad: Pueden adaptarse a las necesidades cambiantes de una organización y escalar fácilmente para acomodar un mayor número de usuarios y dispositivos.

Seguridad y control centralizado: Permiten implementar medidas de seguridad centralizadas para proteger la información y los recursos de la red.

Backup y recuperación de datos: Facilitan la realización de copias de seguridad y la recuperación de datos en caso de fallos o pérdida de información.

Colaboración: Fomentan la colaboración en tiempo real entre usuarios a través de herramientas como videoconferencias y compartición de documentos.

Acceso remoto: Permiten el acceso a la red y a los recursos desde ubicaciones remotas, lo que es esencial para el trabajo a distancia y la movilidad.

Reducción de costos: A menudo, resulta más económico implementar y mantener una red en lugar de sistemas de comunicación aislados.

Desventajas de las redes informáticas:

Seguridad y privacidad: Las redes pueden ser vulnerables a ataques cibernéticos y violaciones de la privacidad si no se implementan medidas de seguridad adecuadas.

Costos iniciales y mantenimiento: La configuración inicial y el mantenimiento de una red pueden requerir una inversión significativa en hardware, software y personal especializado.

Complejidad: La gestión de redes puede ser compleja, y la resolución de problemas a veces es difícil, especialmente en redes grandes.

Rendimiento variable: El rendimiento de la red puede verse afectado por la congestión, la velocidad de la conexión y la calidad de los dispositivos y cables utilizados.

Dependencia de la electricidad y la conectividad a Internet: La operación de la red depende de la electricidad y la disponibilidad de una conexión a Internet, lo que puede ser un problema en caso de cortes de energía o interrupciones de la red.

Aislamiento de fallas: Las fallas en una red pueden afectar a múltiples usuarios y sistemas, lo que hace que el aislamiento y la corrección de fallas sean fundamentales.

Problemas de interoperabilidad: En entornos con diversos dispositivos y sistemas, pueden surgir problemas de interoperabilidad si no se utilizan estándares y protocolos comunes.

Posible obsolescencia tecnológica: Las tecnologías de red evolucionan rápidamente, lo que puede llevar a que el hardware y el software de la red se vuelvan obsoletos en un corto período de tiempo.

A. Componentes de una red informática

• Dispositivos de Red:

- **Computadoras:** Estos son los dispositivos que envían, reciben y procesan datos en la red. Pueden ser computadoras de escritorio, portátiles, servidores, etc.
- **Enrutadores (Routers):** Los enrutadores son dispositivos que dirigen el tráfico de datos entre diferentes redes. Conectan redes locales a la Internet o entre sí.

- **Conmutadores (Switches):** Los conmutadores son utilizados para conectar dispositivos dentro de una red local. Dirigen el tráfico dentro de la red y mejoran la eficiencia de la comunicación.
- **Puntos de Acceso (Access Points):** Estos dispositivos se utilizan para conectar dispositivos inalámbricos a una red cableada, como Wi-Fi.
- **Hubs:** Aunque menos comunes en redes modernas, los hubs son dispositivos simples que retransmiten todos los datos que reciben a todos los dispositivos en la red.
- **Medios de Transmisión:**
 - **Cableado:** Los cables de red (como cables Ethernet) son utilizados para transmitir datos en redes cableadas.
 - **Conexiones Inalámbricas:** Las redes inalámbricas utilizan señales de radio o infrarrojas para transmitir datos entre dispositivos.
- **Protocolos de Comunicación:**
 - **TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet):** Este es el protocolo más comúnmente utilizado en Internet y define cómo los datos se envían, reciben y direccionan en una red.
 - **HTTP/HTTPS, FTP, SMTP, etc.:** Son protocolos específicos utilizados para tareas particulares, como navegación web, transferencia de archivos, correo electrónico, etc.
- **Direcciones IP:** Cada dispositivo en una red necesita una dirección IP única para identificarse en la red. Las direcciones IPv4 e IPv6 son comunes.
- **Topología de Red:** Esto se refiere a la estructura física o lógica de la red, como redes de estrella, bus, anillo o malla.
- **Seguridad de Red:**
 - **Firewalls:** Los firewalls protegen la red al filtrar el tráfico no deseado y controlar el acceso.
 - **Cifrado:** La información transmitida a través de la red se puede cifrar para protegerla de accesos no autorizados.
 - **Contraseñas y Autenticación:** Para garantizar que solo usuarios autorizados accedan a la red.
- **Servidores:**
 - **Servidores de Archivos:** Almacenan y gestionan archivos para su acceso compartido en la red.
 - **Servidores de Correo:** Gestionan el correo electrónico.
 - **Servidores Web:** Albergan sitios web y aplicaciones web.
 - **Servidores de Base de Datos:** Almacenan y gestionan datos para aplicaciones y servicios.
- **Periféricos de Red:**
- Impresoras de red, escáneres y otros dispositivos que se pueden compartir en la red.
- **Software de Red:**
- Sistemas operativos de red y software de gestión que ayudan a administrar y mantener la red.
- **Administración de Red:**
- Personal de administración y políticas que controlan el funcionamiento y el acceso a la red.

B. Ejemplo de conexión de elementos de una red

- **Computadoras:** En la oficina, hay cinco computadoras: A, B, C, D y E.
- **Router:** Para permitir que las computadoras se comuniquen entre sí y accedan a Internet, se utiliza un router como punto central de la red.
- **Switch:** Además del router, se utiliza un switch para conectar todas las computadoras entre sí. Un switch permite que las computadoras se comuniquen dentro de la red local de manera eficiente.
- **Conexiones físicas:** Se utilizan cables Ethernet para conectar todas las computadoras al switch. Cada computadora tiene un cable que se conecta a uno de los puertos del switch.
- **Conexión a Internet:** El router se conecta a un módem, que a su vez se conecta al proveedor de servicios de Internet (ISP). Esto permite que todas las computadoras de la red tengan acceso a Internet.
- **Asignación de direcciones IP:** Cada computadora en la red tiene una dirección IP única que le permite ser identificada en la red. El router asigna automáticamente direcciones IP a cada dispositivo conectado a la red local.
- **Firewall:** El router también puede actuar como un firewall, protegiendo la red de amenazas externas y controlando el tráfico de la red.
- **Impresora compartida:** Una impresora está conectada a una de las computadoras (por ejemplo, la computadora A) y se comparte en la red. Las otras computadoras pueden imprimir en esta impresora a través de la red.

3. Clasificación de redes

a. Extensión geográfica.

1. Redes de Área Personal (PAN - Personal Area Network):

Alcance: Muy pequeña, generalmente a nivel personal.

Propósito: Conectar dispositivos personales, como teléfonos móviles, computadoras portátiles y periféricos cercanos.

2. Redes de Área Local (LAN - Local Area Network):

Alcance: Pequeña área geográfica, como una oficina, un edificio o un campus.

Propósito: Conectar dispositivos en un espacio físico limitado, como computadoras, impresoras y servidores locales.

3. Redes de Área de Campus (CAN - Campus Area Network):

Alcance: Se utilizan en campus universitarios, parques tecnológicos o instalaciones similares.

Propósito: Interconectar múltiples edificios o áreas dentro de un campus o ubicación geográfica cercana.

4. Redes de Área Metropolitana (MAN - Metropolitan Area Network):

Alcance: Una ciudad o una zona metropolitana.

Propósito: Interconectar múltiples redes LAN dentro de un área geográfica más grande.

5. Redes de Área Amplia (WAN - Wide Area Network):

Alcance: Abarcan una gran área geográfica, incluso un país o incluso a nivel global.

Propósito: Conectar redes MAN, LAN o dispositivos a través de distancias más largas, a menudo utilizando redes públicas, como Internet.

b. Su titularidad

1. Redes Públicas:

Propiedad: Estas redes son propiedad del gobierno o de una entidad pública y están disponibles para uso público. Ejemplos incluyen la Internet y redes de telefonía móvil de uso generalizado.

2. Redes Privadas:

Propiedad: Son propiedad y operadas por organizaciones o empresas para uso exclusivo de sus propios empleados o fines internos. Ejemplos incluyen las redes corporativas de empresas y las redes de campus universitarios.

3. Redes Comunitarias:

Propiedad: Pueden ser propiedad de una comunidad o una cooperativa de usuarios que comparten los costos y beneficios de la red. Estas redes a menudo se utilizan para proporcionar acceso a Internet en áreas rurales o mal atendidas.

c. Según los servicios que brinda: Cliente-servidor o de igual a igual

Una red entre iguales, también conocida como red P2P (peer-to-peer), es un tipo de red informática en la que las computadoras conectadas actúan como iguales, compartiendo recursos y datos directamente entre sí, sin necesidad de un servidor central.

Una red cliente-servidor es una arquitectura de red en la que las computadoras (clientes) solicitan y acceden a recursos o servicios almacenados en una computadora centralizada (servidor). El servidor proporciona recursos, como archivos, aplicaciones o servicios, a través de la red, y los clientes solicitan y utilizan estos recursos.

d. Otras

Las redes se pueden clasificar según su función o propósito en una organización o sistema. A continuación, se presentan algunos de los principales tipos de redes en función de su propósito:

Redes de Datos:

Propósito: Transmitir datos digitales entre dispositivos para compartir información, archivos y recursos.

Ejemplo: Redes LAN y WAN utilizadas en oficinas, hogares y en Internet.

Redes de Voz:

Propósito: Transportar señales de voz y permitir la comunicación telefónica.

Ejemplo: Redes telefónicas conmutadas y VoIP (Voz sobre Protocolo de Internet).

Redes de Video:

Propósito: Transmitir señales de video en tiempo real.

Ejemplo: Redes de televisión por cable, transmisión en vivo por Internet.

Redes de Almacenamiento:

Propósito: Facilitar el acceso y el almacenamiento de datos en servidores y dispositivos de almacenamiento.

Ejemplo: SAN (Storage Area Network), NAS (Network Attached Storage).

Redes de Control Industrial:

Propósito: Controlar y supervisar procesos industriales y maquinaria.

Ejemplo: Redes utilizadas en la automatización industrial y en la fabricación.

4. Arquitectura de red

a. Concepto

La arquitectura de red se refiere a la estructura y diseño de una red de computadoras. Esta estructura proporciona un marco para el funcionamiento, la administración y el crecimiento de una red de manera eficiente y segura.

b. Características

La arquitectura de red incluye varios componentes y tecnologías que permiten la comunicación y el intercambio de datos entre dispositivos dentro de una red.

Algunos de los aspectos clave de la arquitectura de red incluyen:

- **Topología de Red:** Se refiere a la disposición física o lógica de los dispositivos de red y cómo están interconectados. Ejemplos comunes de topologías incluyen la topología en estrella, en bus, en anillo y en malla.
- **Protocolos de Comunicación:** Los protocolos son reglas y estándares que permiten a los dispositivos en una red comunicarse entre sí. Ejemplos incluyen TCP/IP (el protocolo fundamental de Internet), HTTP (para la web) y SMTP (para correos electrónicos).
- **Dispositivos de Red:** Incluyen routers, switches, hubs y puntos de acceso inalámbricos. Estos dispositivos facilitan la transferencia de datos y la gestión del tráfico en la red.
- **Direccionamiento IP:** Cada dispositivo en una red tiene una dirección IP única que se utiliza para identificarlo y permitir la comunicación con otros dispositivos en la red.

- **Seguridad de Red:** Involucra medidas para proteger la red y los datos que se transmiten a través de ella. Esto incluye firewalls, sistemas de detección de intrusiones, autenticación y cifrado de datos.
- **Ancho de Banda:** Se refiere a la capacidad máxima de datos que pueden ser transmitidos a través de la red en un período de tiempo dado. Un mayor ancho de banda permite una transmisión de datos más rápida y eficiente.
- **Escalabilidad:** Una buena arquitectura de red debe ser capaz de crecer y adaptarse para acomodar nuevos dispositivos y usuarios sin comprometer el rendimiento.
- **Gestión de Red:** Implica la supervisión y administración de los recursos de red para garantizar un rendimiento óptimo y solucionar problemas en caso de que surjan.

c. Topología (física y lógica)

La topología física y la topología lógica son dos aspectos importantes a considerar al diseñar una red de computadoras. Aunque a menudo están interrelacionadas, tienen significados diferentes:

Topología Física:

La topología física se refiere a la disposición física real de los dispositivos y cables en la red. Describe cómo están conectados los dispositivos y cómo se colocan físicamente en un lugar determinado. La topología física se ocupa de aspectos tangibles y visibles de la red. Algunos ejemplos comunes de topologías físicas incluyen la topología en estrella, la topología en bus, la topología en anillo y la topología en malla, como se describen en la respuesta anterior.

Topología Lógica:

La topología lógica se refiere al camino que los datos siguen en una red, cómo se comunican los dispositivos en la red y cómo se gestionan los datos a través de la red. Representa la forma en que los datos se transmiten entre los nodos de una red, independientemente de la disposición física de los dispositivos. La topología lógica define cómo los dispositivos se comunican a través de la red y cómo se establecen las rutas para la transmisión de datos.

Es importante destacar que la topología lógica puede diferir de la topología física. Por ejemplo, en una topología en estrella física, todos los datos pueden pasar a través de un nodo central, como un switch, lo que crea una topología lógica en estrella. Sin embargo, si se utiliza un protocolo de enrutamiento que permita que los datos se transmitan de un nodo a otro en la red, la topología lógica puede parecerse más a una topología en malla.

d. Tipos de topología (bus, estrella, anillo, malla, árbol, mixta). Ventajas e inconvenientes de cada uno

Las topologías de red se refieren a la disposición física o lógica de los dispositivos en una red y cómo están interconectados entre sí. Existen varias topologías comunes que se utilizan en entornos de red. Aquí hay una descripción de algunas de las topologías de red más conocidas:

- **Topología en Estrella:** En una topología en estrella, todos los dispositivos están conectados a un nodo central, como un concentrador (hub) o un switch. Todas las comunicaciones entre dispositivos pasan a través del nodo central. Si un

dispositivo desea comunicarse con otro, envía los datos al nodo central, que luego los retransmite al dispositivo de destino.

- **Topología en Bus:** En una topología en bus, todos los dispositivos comparten un solo canal de comunicación. Cada dispositivo está conectado a un cable único, y los datos viajan por el cable hasta que alcanzan el dispositivo de destino. Los datos pasan a través del cable y son recibidos por todos los dispositivos, pero solo el dispositivo para el cual están destinados procesa los datos.
- **Topología en Anillo:** En una topología en anillo, cada dispositivo está conectado a dos dispositivos vecinos, formando un anillo o circuito cerrado. Los datos se transmiten en una dirección a lo largo del anillo. Cada dispositivo en el anillo recibe los datos y pasa los datos al siguiente dispositivo en el anillo hasta que los datos alcanzan su destino.
- **Topología en Malla:** En una topología en malla, cada dispositivo está conectado a todos los demás dispositivos en la red. Esto crea múltiples rutas para que los datos viajen de un dispositivo a otro. Las topologías de malla pueden ser parciales (los dispositivos están conectados a algunos, pero no a todos los demás dispositivos) o completas (cada dispositivo está conectado a todos los demás dispositivos).
- **Topología en Árbol:** La topología en árbol es una combinación de la topología en estrella y la topología en bus. Los dispositivos están organizados en una estructura jerárquica similar a un árbol. Un nodo central se conecta a nodos secundarios que, a su vez, pueden estar conectados a nodos adicionales. Los datos se transmiten desde el nodo central a través de los nodos secundarios hasta llegar al dispositivo de destino.

5. Internet, intranet y extranet

Que es Intranet:

Es una red interna, a la que no puede acceder cualquiera. Permite compartir información, servicios o utilizar sistemas operativos dentro de esa red informática. Este tipo de redes suele ser utilizada por organizaciones. Por ejemplo, puede ser una empresa que ofrece a sus trabajadores acceso a determinada información, documentos o servicios.

Puntos básicos:

- Se trata de una red interna
- La utilizan normalmente organizaciones y empresas
- Utiliza servidores locales
- Requiere de autenticación para poder acceder a ella

Que es extranet:

Tiene una función similar a la de Intranet. Podemos decir que sigue siendo una red cerrada, como en el caso anterior. Sin embargo, esta vez sí admite el acceso de usuarios externos. Es una red limitada a un número concreto de usuarios, pero podemos acceder a ella desde cualquier punto del mundo, por ejemplo, una empresa podría facilitar un usuario y contraseña a sus clientes permitiéndoles acceder la red.

Puntos básicos:

- Sirve para ampliar los límites de intranet

- Útil para empresas
- Puede tener un uso semiprivado

Que es internet:

Es el gran conjunto de redes de comunicación descentralizado. Gracias a esta gran plataforma podemos navegar por la red desde cualquier lugar y estar en constante comunicación con el mundo. Es sencillamente una red mundial que engloba todas las redes locales que hay distribuidas por el mundo. Está abierto a todo el mundo, a diferencia de la Intranet y Extranet. Podemos acceder sin necesidad de contar con un usuario y contraseña para ello. Simplemente necesitamos los recursos necesarios, como es contar con un dispositivo compatible y tener acceso a Internet, así como el software requerido para ello.

Puntos básicos:

- Gran cantidad de redes
- Abierto a todo el mundo
- Gran abanico de opciones
- Varias partes de internet

- a. Conexión a internet: cable, DSL, fibra óptica, líneas dedicadas, comunicaciones por satélite. Diferencias y ejemplos de uso.

La elección del tipo de conexión a Internet depende de diversos factores, como la ubicación geográfica, la disponibilidad de servicios y las necesidades individuales. Aquí hay una descripción de varios tipos de conexiones a Internet, sus diferencias y ejemplos de uso:

- **Conexión por cable:**
Tipo de conexión: Utiliza el cable coaxial para transmitir datos.
Velocidad: Ofrece velocidades de banda ancha, generalmente más lentas que la fibra óptica pero más rápidas que DSL.
Ejemplos de uso: Uso doméstico y comercial para navegación web, streaming de video, juegos en línea y transferencia de datos.
- **DSL (Línea de abonado digital):**
Tipo de conexión: Utiliza líneas telefónicas tradicionales para transmitir datos.
Velocidad: Proporciona velocidades moderadas, generalmente más lentas que el cable y la fibra óptica.
Ejemplos de uso: Uso doméstico y comercial para actividades en línea como la navegación web, correo electrónico y streaming de video.
- **Fibra óptica:**
Tipo de conexión: Utiliza cables de fibra óptica que transmiten datos a través de pulsos de luz.
Velocidad: Ofrece velocidades extremadamente altas, superando a las conexiones por cable o DSL.
Ejemplos de uso: Ideal para aplicaciones intensivas en datos, como videoconferencias, descargas y transmisiones de alta definición, y servicios en la nube.
- **Líneas dedicadas:**
Tipo de conexión: Ofrece una conexión directa y no compartida con el proveedor de servicios.

Velocidad: La velocidad puede variar según las necesidades del cliente y la infraestructura disponible.

Ejemplos de uso: Empresas que requieren conexiones de alta velocidad y alta fiabilidad, como empresas que alojan servidores web, realizan videoconferencias o transmiten grandes volúmenes de datos.

- **Comunicaciones por satélite:**

Tipo de conexión: Utiliza satélites en órbita para transmitir datos entre el proveedor y el usuario.

Velocidad: La velocidad puede ser más lenta que otras opciones, y la latencia suele ser más alta.

Ejemplos de uso: Útil en áreas rurales o remotas donde las conexiones terrestres no están disponibles. Se utiliza para servicios de Internet, telefonía y televisión satelital.

- b. Elementos que hacen que una red sea confiable (tolerancia a fallos, seguridad, escalabilidad, calidad de servicio)

Una red confiable se caracteriza por su capacidad para mantener la disponibilidad, integridad y confidencialidad de la comunicación y los datos, incluso en situaciones adversas. Varios elementos contribuyen a la confiabilidad de una red, incluyendo:

- **Tolerancia a fallos:**

Redundancia: Utilizar componentes duplicados o rutas de comunicación alternativas para garantizar que la red continúe funcionando en caso de fallos.

Detección y recuperación automática: Implementar sistemas de monitoreo y mecanismos de recuperación que identifiquen fallos y los resuelven automáticamente sin intervención humana.

Balanceo de carga: Distribuir el tráfico entre múltiples servidores o rutas para evitar la congestión y mantener la disponibilidad.

- **Seguridad:**

Autenticación: Requerir que los usuarios se autenticuen antes de acceder a la red o los recursos.

Encriptación: Proteger la confidencialidad de los datos mediante la encriptación de la información transmitida.

Cortafuegos y sistemas de detección de intrusiones: Implementar medidas de seguridad para prevenir y detectar amenazas, como malware y ataques de red.

Actualizaciones y parches: Mantener los dispositivos de red y el software actualizado para mitigar vulnerabilidades conocidas.

- **Escalabilidad:**

Diseño modular: Crear una infraestructura de red escalable mediante la segmentación de la red en módulos o segmentos independientes.

Capacidad de crecimiento: Seleccionar equipos y tecnologías que permitan la expansión de la red para adaptarse a las necesidades cambiantes.

Implementar protocolos y estándares abiertos: Facilitar la integración de nuevos dispositivos y servicios sin depender de tecnologías propietarias.

- **Calidad de servicio:**

Priorización del tráfico: Asignar prioridades al tráfico de red para garantizar que las aplicaciones críticas tengan un rendimiento óptimo.

Ancho de banda suficiente: Asegurarse de que haya suficiente ancho de banda para satisfacer las demandas de la red, especialmente en momentos de carga pesada.

Control de congestión: Implementar mecanismos que gestionen la congestión y mantengan un rendimiento constante.

- **Planificación y documentación:**

Documentación detallada: Mantener registros y documentación precisa de la topología de la red, las configuraciones y los procedimientos de recuperación.

Plan de continuidad del negocio: Tener un plan de recuperación ante desastres que incluya medidas para mantener la operatividad de la red en caso de interrupciones graves.

- **Capacitación del personal:**

Personal competente: Contar con personal capacitado que comprenda la infraestructura de red y sepa cómo administrarla y solucionar problemas.

Pruebas y simulacros: Realizar pruebas periódicas y simulacros de respuesta a incidentes para garantizar que el personal esté preparado para afrontar situaciones de fallos o ataques.

[Link1](http://ccnadesdecero.es): ccnadesdecero.es

[Link2](http://redeszone.net): redeszone.net

6. Protocolos y estándares de red:

6.1. Diferencia entre protocolo y estándar

6.1.1. Estándar es una serie de guías que se le comunican a los fabricantes para que todos sigan una estructura básica y que los dispositivos sean compatibles entre sí.

6.1.2. Protocolo es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información.

6.2. Organismos de estandarización más importantes

6.2.1. IEEE (Institute of Electrical and Electronic Engineers)

6.2.2. ISO (International Organization for Standardization)

6.2.3. ITU (International Telecommunication Union)

6.2.4. IETF (Internet Engineering Task Force)

6.2.5. ANSI (American National Standards Institute)

6.2.6. ETSI (European Telecommunications Standards Institute)

6.2.7. AENOR (Asociación Española de Normalización)

6.3. Modelos de redes:

6.3.1. Modelo de referencia OSI: capas.

6.3.1.1. Capa 1 - La capa física

Corresponde a los equipos físicos que posibilitan la transferencia de datos, como cables y enrutadores instalados en la red. En esta capa

los estándares son imprescindibles porque sin ellos la comunicación se complicaría de forma innecesaria por incompatibilidades.

6.3.1.2. Capa 2 - La capa de enlace de datos

La capa de enlace de datos es la responsable de la transferencia de información en la misma red. El enlace de datos convierte los paquetes recibidos en la capa de red en marcos. Al igual que la capa de red, la capa de enlace de datos es la responsable del control de los errores y el flujo de datos para garantizar una correcta transmisión.

6.3.1.3. Capa 3 - La capa de red

La capa de red es la que se encarga de dividir los datos en el dispositivo del remitente y de recomponerlos en el dispositivo del destinatario cuando la transmisión ocurre entre dos redes diferentes. Al comunicarse dentro de la misma red, la capa de red es innecesaria, pero la mayoría de los usuarios se conectan a otras redes, como las redes basadas en la nube. Cuando los datos viajan a través de diferentes redes, la capa de red es la responsable de crear pequeños paquetes de datos que se redirigen a sus destinos y después se reconstruyen en el dispositivo del destinatario.

6.3.1.4. Capa 4 - La capa de transporte

La capa de transporte se encarga de tomar los datos y dividirlos en partes más pequeñas. Para hacer las transferencias más eficientes y rápidas, la capa de transporte divide los datos en segmentos más pequeños. Estos segmentos más pequeños contienen información de encabezado que se pueden volver a ensamblar en el dispositivo objetivo. Los datos segmentados también cuentan con control de errores para informar a la capa de transporte que restablezca la conexión si los paquetes no se transfieren totalmente al destinatario objetivo.

6.3.1.5. Capa 5 - La capa de sesión

Para comunicarse entre dos dispositivos, una aplicación debe antes crear una sesión. Una sesión es única para el usuario y lo identifica en el servidor remoto. Cuando se transfieren grandes volúmenes de datos, la sesión es la que se encarga de garantizar que el archivo se transfiera en su totalidad, y de que la retransmisión se restablezca si los datos están incompletos.

6.3.1.6. Capa 6 - La capa de presentación

La capa de presentación es la que prepara los datos para que estos puedan mostrarse al usuario. La capa de presentación es la responsable de la codificación y decodificación de la información, de

modo de que puede mostrarse en texto simple. La capa de presentación también es responsable de la compresión y descompresión de los datos, a medida que estos viajan de un dispositivo a otro.

6.3.1.7. Capa 7 - La capa de aplicación

La capa de aplicación es con la que está familiarizada la mayoría de la gente, porque es la que se comunica directamente con el usuario. Es en la que se presentan los datos transportados al usuario.

[referencia](https://proofpoint.com): proofpoint.com

6.3.2. Modelo de protocolo TCP/IP: capas.

6.3.2.1. Capa 1 - Capa de acceso a la red

Esta es la capa inicial donde se gestiona toda la infraestructura física de los ordenadores para comunicarse entre sí a través de Internet. Por ejemplo: módems, cables Ethernet, antenas satelitales, antenas repetidoras de señal, controladores de dispositivo y, por supuesto, ordenadores de todo tipo. Por tanto, esta capa involucra toda la parte técnica y de hardware dentro del modelo TCP/IP. Asimismo, las señales para la transmisión de datos entre dispositivos.

6.3.2.2. Capa 2 - Capa de Internet

Esta capa es la que se ocupa del enrutamiento de los paquetes de datos. O, en otras palabras, aquí es donde se asignan las direcciones IP y redirecciones de los datos. Aquí es donde se establece la mejor ruta para que los datos lleguen a su destino.

En otras palabras, controla los movimientos y direcciones de los paquetes una vez en la red.

6.3.2.3. Capa 3 - Capa de transporte

Esta capa es la responsable de la comunicación entre dispositivos, donde los paquetes son enviados entre dos dispositivos. Asimismo, esta capa se asegura de que los datos lleguen a sus destinos y estos sean recibidos y confirmados por el destinatario.

6.3.2.4. Capa 4 - Capa de aplicaciones

Este es el tramo final, el que utilizas en tu día a día para acceder a la web. Aquí es donde el usuario puede acceder directamente a la red y enviar y recibir datos según sus solicitudes. Aquí el usuario puede interactuar con la red por diferentes medios, ya sea por aplicaciones webs, aplicaciones de mensajería, servicios de almacenamiento en la nube, correos electrónicos, entre otros servicios.

[Referencia:](#) Avast.com

[Referencia:](#) thepowermba.com

[Referencia:](#) ibm.com

6.3.3. Comparación entre los modelos OSI y TCP/IP.

OSI es un modelo teórico que se utiliza para el sistema informático, mientras que TCP/IP es un modelo de servidor de cliente que se emplea para la transmisión de datos a través de Internet.