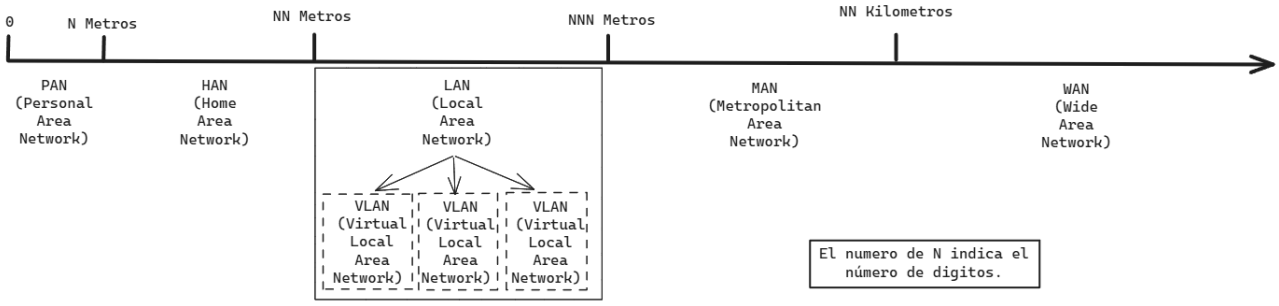
# Unidad didáctica 03. Introducción a los sistemas en red

# Módulo: Sistemas informáticos

## Tarea 1. Tipos de redes, modelos y protocolos

1. Realiza una infografía o esquema donde de un vistazo sea posible ver los diferentes alcances de las redes (PAN, LAN...) y añade datos sobre el alcance de las mismas, no hace falta que sea preciso. Por ejemplo: PAN <10 metros / red de muy corto alcance.




Fuentes:

Extensión de las redes

2. Vimos lo que es una VPN. Ahora, investiga:
   2.1. ¿Qué tipos de VPN hay?

   Tipos de VPN ordenadas por casos de uso:

   - VPN de acceso remoto.

     Conecta al usuario a una red de forma segura. Usada en ámbito profesional y personal. Ejemplos de este tipo de redes son NordVPN o Surfshark. Te conectas a uno de sus servidores y desde ahí sales a internet

   - VPN de sitio a sitio.

     Existen dos subtipos de esta red.

     - De sitio a sitio básicas. Permiten conectar dos o mas redes entre si, usadas por grandes empresas que tienen varias redes distribuidas por un territorio. Para que estas redes simulen ser solo una.

- Basadas en Extranet. Limita los datos de una red a los que accede la otra. Usada por empresas para conectar redes de clientes, proveedores y socios comerciales externos.

Tipos de VPN según su arquitectura:

- Basadas en cliente. Son las más comunes, te descargas una aplicación en el dispositivo que quieras usar la vpn y esta se conecta a un servidor del proveedor del servicio.
- Basadas en servidor. Son más complejas y menos usadas aunque permiten una mayor flexibilidad. Instalas la aplicación en un servidor y después te conectas a él.

2.2. ¿Qué protocolos utilizan?

- WireGuard: Nuevo protocolo VPN. Originalmente lanzado para el kernel de Linux ahora ya es multiplataforma. Aún está en desarrollo. Una de sus principales ventajas es que ocupa muchas menos lineas de código por lo que puede ser auditado por una sola persona, tarea imposible para otros protocolos. Las ventajas de este protocolo son: criptografía de última generación, proyecto código abierto, seguridad y velocidad de transferencia.
- OpenVPN:

  **De código abierto.** Utilizan la biblioteca de OpenSSL y los protocolos TLS (y otras tecnologías). Es el protocolo estándar en la industria. Su ventaja es que es muy configurable. Está disponible a través de la mayoría de software de terceros. La conexión se establece entre un *open-vpn-server* y un *open-vpn-client.*

- IPSec/L2TP:

  ***Internet Protocol Security*** asegura la conexión a internet a través de la autenticación de la sesión y encripta cada paquete de datos durante la conexión. Tiene dos modos de trabajo:

  - Modo de transporte.

    Encripta el mensaje en el paquete de datos.

  - Modo de túnel.

    Encripta todo el paquete de datos.

  ***Layer 2 Tunneling Protocol*** es un protocolo que se combina con otro de seguridad como es IPSec para crear una conexión altamente segura. Sucesor del protocolo ***PPTP.***

  Diferencia entre IPSec y L2TP → El primero cifra los datos y maneja la comunicación segura entre los extremos del túnel y el segundo crea un túnel entre dos puntos de conexión.

- SSTP:

***Secure Socket Tunneling Protocol***. Estándar de Microsoft muy similar a OpenVPN, tiene las mismas ventajas, pero se integra mejor con el ecosistema Windows. Puede pasar a través de la mayoría de *Firewall* usando el puerto 443. Está mas pensado para el acceso remoto de clientes que para crear túneles VPN. Tiene autenticación de usuarios pero no admite la de dispositivos, o lo que es lo mismo puede comprobar que eres un usuario autorizado a través de contraseñas y otros métodos pero no puede comprobar si el dispositivo está autorizado por si mismo.

La diferencia entre SSTP y IPSEC es que SSTp utiliza ssl 3.0

- IKEv2 :

  ***Internet key exchange*** en su segunda versión se utiliza para negociar una asociación de seguridad al principio de la sesión ***IPSEC.***

- PPTP:

  ***Protocolo de túnel punto a punto.*** Crea un túnel y encapsula el paquete de datos. Utiliza un protocolo punto a punto (***PPP Point-to-point-protocol***). Es de los más longevos llevo en uno desde *Windows95*. Usado también por *Linux* y *Mac.*

Fuentes:

VPN

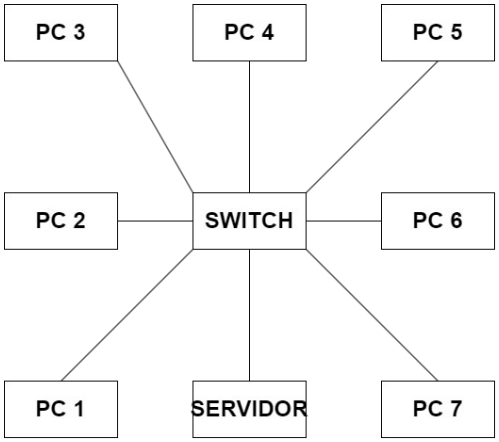
Protocolos-VPN

Protocolo SSTP

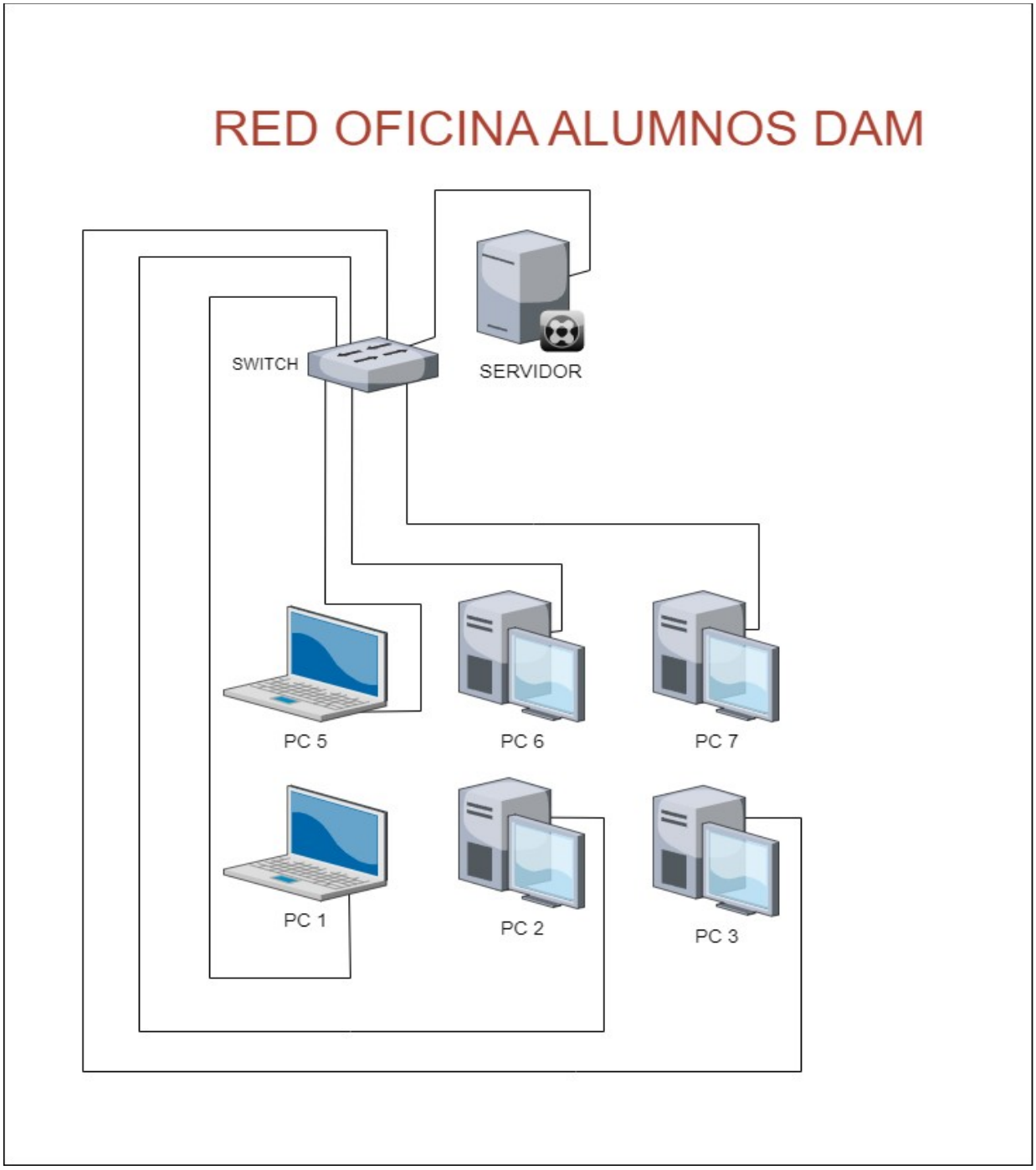
Protocolo WireGuard

3. Años después de estudiar juntos, un grupo de antiguos alumnos del ciclo de DAM deciden montar una empresa. Compran 7 ordenadores, un servidor físico, un switch, contratan internet y alquilan una oficina. Elige una topología de red y escribe 3-4 frases justificando tu elección.

   En esta situación elegiría una topología en estrella puesto que facilita el montaje y es altamente escalable. Salvo que falle el nodo central, cualquier fallo en los nodos satelites es transparente para los demás equipos.



4. Haz un mapa físico del ejercicio anterior.




Fuentes:

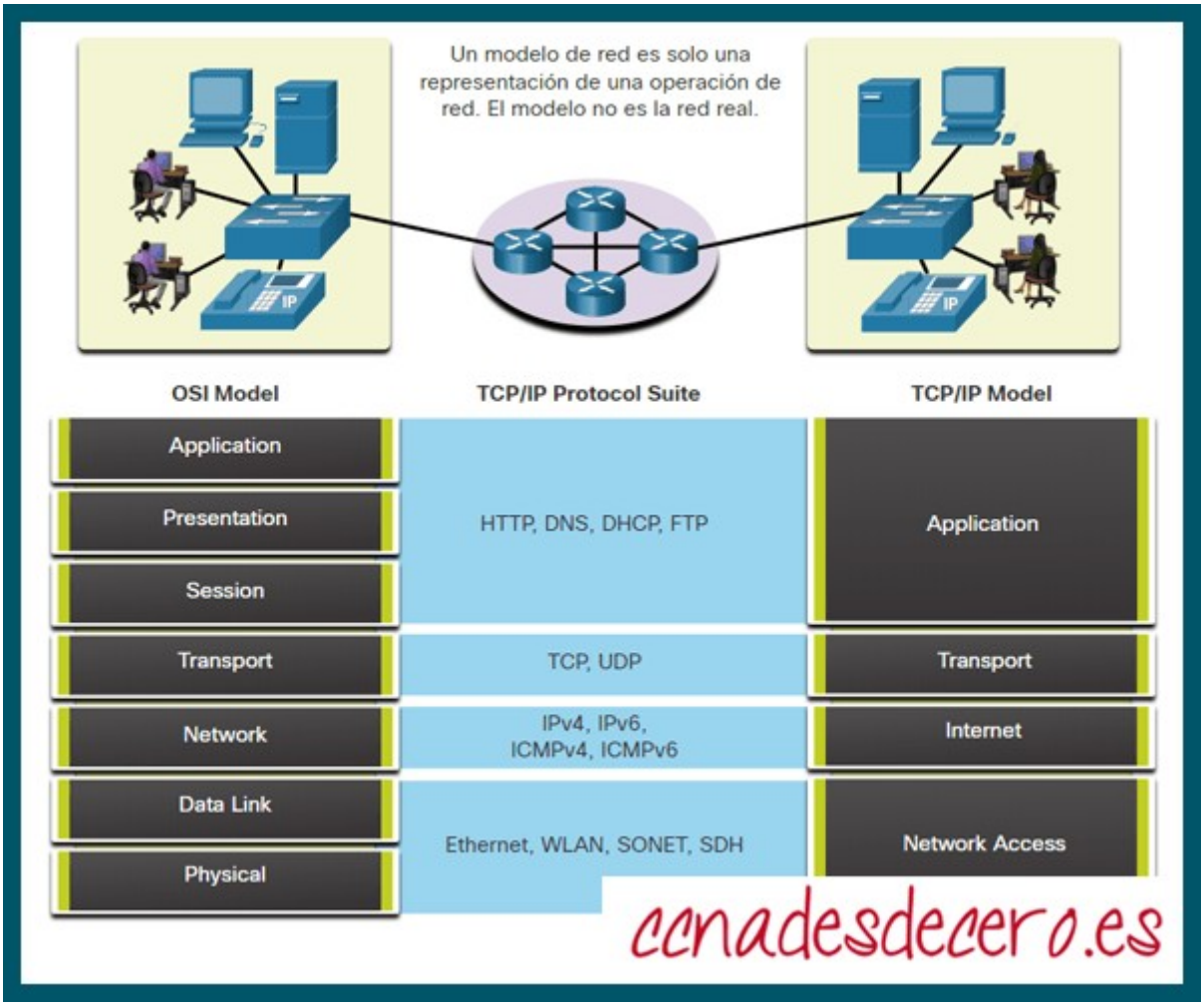
Esquemas creados con la extensión para draw.io  de Visual Studio Code.

Creación de esquemas

5. 5 Hemos visto en clase qué es el modelo OSI, pero... ¿Cuál es su historia (Se breve)? ¿Por qué es importante? Establece la relación entre las capas del modelo OSI y las del modelo TCP/IP.

El modelo de interconexión de sistemas abiertos (***O**pen **S**ystems **I**nterconection*) es un modelo de referencia para los protocolos de red. Surge en la década de 1980, en este momento las redes estaban popularizándose y cada empresa y compañía tenía su propio tecnología de conexiones. En consecuencias las comunicaciones se hacían complicadas y tediosas, ante esta necesidad la ***ISO*** investigó modelos de conexión como la red de ***D**igital **E**quipement **C**orporation DECnet*, la ***S**ystem **N**etwork **A**rquitecture SNA, y **TCPI/IP***.

Basándose en el resultado de este estudio, desarrollaron un modelo de red que ayudaría a los fabricantes a crear redes compatibles, de ahí su importancia.




Como se puede apreciar en la imagen el modelo OSI es un modelo teórico para orientarnos, en la práctica el protocolo TCP/IP engloba alguna de sus partes en una sola.

Modelo OSI (Aplicación, Presentación y Sesión) → TCP/IP (Aplicación)

Modelo OSI (Enlace, Física) → TCP/IP (Acceso a la red)

La función mas relevante del modelo OSI en orientar sobre que partes debe tener un protocolo de comunicación. En la implementación los pocesos pueden agruparse, pero al tener este modelo de referencia podemos unificar la forma de trabajar de los diferentes modelos y las fases de todos ellos.

Fuentes:

Historia modelo OSI

Comparativa OSI-TCP/IP

6. ¿En qué se diferencian rsync y rcp? ¿Ventajas y desventajas de cada uno?

El protocolo ***rsync*** solo copia los archivos diferentes mientras que ***rcp*** los copia todos y los sobrescribe si es necesario → ***rsync*** es más rápido, además ***rcp*** es inseguro puesto que no utiliza *ssh.* Fue sustituido por el protocolo ***scp*** que si lo usa. ***Rsync*** también puede trabajar sin encriptación aunque no es recomendable.

Fuentes:

RSync