**17- ¿Qué es un Firewall?:**

Un firewall es un dispositivo de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. El propósito principal de un firewall es establecer una barrera entre una red interna confiable y redes externas no confiables.

Los firewalls vienen en formas de hardware y software, y funcionan inspeccionando paquetes de datos y determinando si los permiten o bloquean en función de un conjunto de reglas. Las organizaciones pueden configurar estas reglas para permitir o denegar el tráfico en función de varios criterios, como direcciones IP de origen y destino, números de puerto y tipo de protocolo.

Los firewalls son la base de la [seguridad de la red](https://www.fortinet.com/lat/resources/cyberglossary/what-is-network-security), protegiendo la red del acceso no autorizado. Evitan que los actores maliciosos, piratas informáticos, bots y otras amenazas, sobrecarguen o se infiltren en una red privada para robar datos sensibles.

Afortunadamente, las tecnologías de firewall de vanguardia con servicios impulsados por IA están acelerando la seguridad de la red. Combinando las fortalezas de las herramientas tradicionales con las capacidades innovadoras de las nuevas soluciones, los proveedores de firewall modernos ayudan a las organizaciones a defenderse incluso contra las estrategias de ataque más complejas.

Los firewalls regulan el tráfico entrante y saliente, protegiendo la red de:

* **Amenazas externas** como virus, puertas traseras, correos electrónicos de suplantación de identidad y ataques de denegación de servicio (DoS). Los firewalls filtran los flujos de tráfico entrantes, evitando el acceso no autorizado a datos sensibles y frustrando posibles infecciones de malware.
* **Amenazas internas** como actores maliciosos conocidos o aplicaciones riesgosas. Un firewall puede aplicar reglas y políticas para restringir ciertos tipos de tráfico saliente, lo que ayuda a identificar actividades sospechosas y mitigar la exfiltración de datos.

Fuente [https://www.fortinet.com/lat/resources/cyberglossary/firewall]

**18- ¿Qué es una DMZ?**

Una DMZ o zona desmilitarizada es una red perimetral que protege y agrega una capa adicional de seguridad a la red de área local interna de una organización del tráfico no confiable.

El objetivo final de una red de zona desmilitarizada es permitir que una organización acceda a redes no confiables, como Internet, mientras garantiza que su red privada o LAN permanezca segura. Por lo general, las organizaciones almacenan servicios y recursos externos, así como servidores para el [Sistema de nombres de dominio (DNS),](https://www.fortinet.com/lat/resources/cyberglossary/what-is-dns) el [Protocolo de transferencia de archivos (FTP),](https://www.fortinet.com/lat/resources/cyberglossary/file-transfer-protocol-ftp-meaning) correo, proxy, el Protocolo de voz sobre Internet (VoIP) y los servidores web, en la DMZ.

Estos servidores y recursos están aislados y tienen acceso limitado a la LAN para garantizar que se pueda acceder a ellos a través de Internet, pero la LAN interna no puede hacerlo. Como resultado, un enfoque de DMZ hace que sea más difícil para un hacker obtener acceso directo a los datos y servidores internos de una organización a través de Internet.

Las empresas con un sitio web público que utilizan los clientes deben hacer que su servidor web sea accesible a Internet. Para proteger la red de área local corporativa, el servidor web se instala en una computadora separada de los recursos internos. La DMZ permite la comunicación entre recursos comerciales protegidos, como bases de datos internas y tráfico calificado de Internet.

Una DMZ permite que los visitantes del sitio web obtengan ciertos servicios mientras proporcionan un búfer entre ellos y la red privada de la organización. Como resultado, ofrece también beneficios de seguridad adicionales, tales como:

1. Habilitación del control de acceso: Las empresas pueden proporcionar a los usuarios acceso a servicios fuera de los perímetros de su red a través de Internet pública. La DMZ permite el acceso a estos servicios mientras implementa la [*segmentación de red*](https://www.fortinet.com/lat/resources/cyberglossary/network-segmentation) para hacer que sea más difícil para un usuario no autorizado llegar a la red privada.
2. Prevenir el reconocimiento de la red: Al proporcionar un búfer entre Internet y una red privada, una DMZ evita que los atacantes realicen el trabajo de reconocimiento que realizan en la búsqueda de posibles objetivos. Los servidores dentro de la DMZ están expuestos públicamente, pero un firewall ofrece otra capa de seguridad que evita que un atacante pueda ver dentro de la red interna.
3. Bloqueo de la falsificación de protocolo de Internet (IP): los atacantes intentan encontrar formas de obtener acceso a los sistemas falsificando una [dirección IP](https://www.fortinet.com/lat/resources/cyberglossary/what-is-ip-address) y suplantando un dispositivo aprobado que inició sesión en una red. Una DMZ puede descubrir y detener estos intentos de suplantación de identidad, ya que otro servicio verifica la legitimidad de la dirección IP.

Los servicios de una DMZ incluyen:

* Servidores DNS
* Servidores FTP
* Servidores de correo
* Servidores proxy
* Servidores web

Fuente[https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz]

**19- ¿Qué es un Gateway?**

Un **Gateway** actúa como un enlace entre dos redes, permitiendo que los dispositivos de una red se comuniquen con los de otra. La presencia de **Gateways** es fundamental para acceder a Internet, facilitando la comunicación y transferencia de datos entre diferentes redes. Estas pasarelas pueden ser implementadas completamente a través de **software, hardware** o una **combinación de ambos**. Dado que las pasarelas de red suelen situarse en el extremo de una red, su funcionalidad se extiende para integrar capacidades como **cortafuegos**y**servidores proxy.**

Un Gateway tiene tarjetas de interfaz de red (NICs – Network Interface Cards), entradas y salidas (generalmente Ethernet), junto con software para traducir protocolos de red entre las diferentes redes que interconecta. Las funciones del Gateway también pueden implementarse mediante software. Cada vez más se están integrando en routers y otros equipos físicos.

En base a las funcionalidades que habilita, puede haber una gran variedad de Gateways, entre los que destacan los siguientes:

* **Gateway de red**: Es el más común y sirve de interfaz entre dos redes que usan protocolos diferentes. Cuando solo se menciona Gateway, nos solemos estar refiriendo a este tipo.
* **Gateway de almacenamiento en cloud**: Este tipo de Gateway funciona como un intermediario entre las solicitudes de almacenamiento API SOAP o REST y los servicios de almacenamiento en la nube. Su función esencial radica en facilitar la integración del almacenamiento privado en la nube en las aplicaciones existentes sin requerir la migración de estas aplicaciones a una nube pública. Esto simplifica la transferencia de datos y la comunicación, asegurando una mejor interoperabilidad.
* **Gateway IoT**: Conecta dispositivos IoT locales a la red, permitiendo la recopilación, procesamiento y transmisión de datos entre los dispositivos y la nube o sistemas centrales.
* **Gateway de seguridad:** Protege una red interna de amenazas externas, como ataques cibernéticos, filtrando el tráfico no autorizado y aplicando políticas de seguridad.
* **Gateway de voz:** Facilita la comunicación de voz sobre protocolos de Internet (VoIP), convirtiendo señales de voz analógicas en datos digitales para su transmisión a través de redes IP.
* **Gateway de mensajería:** Sirve como intermediario entre diferentes protocolos de mensajería, como SMS, correo electrónico y mensajes instantáneos, para facilitar la comunicación entre ellos.
* **Gateway de servicios web:** Permite la interoperabilidad entre aplicaciones y servicios web al traducir solicitudes y respuestas entre diferentes protocolos y formatos de datos.
* **Gateway de API:** Facilita el acceso y la integración de servicios y datos de aplicaciones a través de interfaces de programación de aplicaciones (API), permitiendo la comunicación entre sistemas heterogéneos.

Fuente[https://conectividadiot.telefonicatech.com/gateway/]

**20- Según Microsoft, ¿qué significa NBL?**

El NBL (Network Load Balancing) o Equilibrio de carga de red mejora la disponibilidad y escalabilidad de las aplicaciones de servidor de Internet tales como las usadas en servidores web, servidores FTP, servidores firewall, servidores proxy, servidores de redes privadas virtuales (VPN) y otros servidores con una importancia decisiva.

La característica de equilibrio de carga de red (NLB) distribuye el tráfico por distintos servidores mediante el protocolo de red TCP/IP. Al combinar en un solo clúster virtual dos o más equipos que ejecutan aplicaciones, NLB ofrece confiabilidad y rendimiento para los servidores web y otros servidores con una importancia decisiva.

Los servidores de un clúster NLB se denominan *hosts* y cada host ejecuta una copia independiente de las aplicaciones de servidor. NLB distribuye las solicitudes de cliente entrantes entre los hosts que forman el clúster. Se puede configurar la carga que administrará cada host. También se pueden agregar hosts de manera dinámica al clúster para administrar los aumentos de carga. NLB también puede dirigir todo el tráfico a un host único designado, que se denomina *host predeterminado*.

NLB permite que todos los equipos del clúster se dirijan al mismo conjunto de direcciones IP y mantiene un conjunto de direcciones IP exclusivas y dedicadas para cada host.

NLB se instala como un componente estándar del controlador de redes de Windows Server. Sus operaciones son transparentes para la pila de redes TCP/IP.

Fuente [https://learn.microsoft.com/es-es/windows-server/networking/technologies/network-load-balancing]

**21- Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT.**

1. **Explique cada uno de estos tipos de enlace.**

**MPLS:**

El switching de etiquetas multiprotocolo (MPLS) es un protocolo diseñado para llevar paquetes de datos a sus destinos de manera rápida y eficiente. Debido a que envía datos directamente a su destino, es superior al enrutamiento regular del protocolo de Internet (IP), que rebota datos por Internet antes de enviarlos finalmente a su destino final.

“Multiprotocolo” significa que el sistema no depende de ningún protocolo en particular para operar. Es una superposición, que le permite reenviar una variedad de diferentes tipos de datos, independientemente del protocolo utilizado para organizarlos.

**Ventajas:**

* Mejor rendimiento
* Mejor administración del trafico
* Seguridad mejorada

**Desventajas:**

* Dependencia de un operador
* Gasto
* Falta de cobertura integral

Fuente [https://www.fortinet.com/lat/resources/cyberglossary/mpls]

**LAN TO LAN:**

Es un servicio de transmisión de datos punto a punto basado en protocolo IP que permite interconectar dos o más redes de área local. Está diseñada específicamente para comunicar dos ubicaciones mediante una conexión privada entre ellas sin necesidad de pasar por internet. En esencia, una LAN puede enlazarse a otra igual para formar una red LAN to LAN, creando una conexión entre dos sitios distintos de manera privada y dedicada.

Esta conexión permite que los equipos como impresoras, laptops y computadoras de escritorio que trabajan en diferentes oficinas funcionen como si estuvieran en un mismo espacio físico.

Al ser una conexión exclusiva, toda la capacidad es únicamente para la empresa, lo que evita la congestión de tráfico. Resulta más segura, pues para interceptarla se necesitaría violar la infraestructura física. Los datos no viajan por internet público sino por una línea dedicada, proporcionando mayor confidencialidad. Cuando un colaborador comparte información, ésta no sale de manera abierta, sino que viaja por la red privada del negocio.

Las arquitecturas de las redes LAN to LAN pueden configurarse en diferentes topologías según las necesidades:

Punto a punto: conecta directamente dos ubicaciones, creando un enlace exclusivo entre ellas.

Punto-multipunto: permite que una ubicación central se conecte con múltiples sitios remotos.

Malla: interconecta todos los puntos entre sí, ofreciendo mayor redundancia.

Fuente: [https://www.servnet.mx/blog/redes-lan-to-lan-que-es-funcionamiento]

**MICROONDAS:**

Un enlace de microondas es un sistema de comunicaciones que utiliza un haz de ondas de radio en el rango de frecuencia de microondas para transmitir información entre dos puntos fijos en la Tierra. Son cruciales para muchas formas de comunicación e impactan en una amplia gama de industrias:

* Los proveedores de servicios de internet inalámbrico utilizan enlaces de microondas para proporcionar a sus clientes acceso a internet de alta velocidad sin necesidad de conexiones por cable.
* Las empresas y los organismos gubernamentales los utilizan para proporcionar redes de comunicaciones entre instalaciones cercanas dentro de una organización, como una empresa con varios edificios en una ciudad.

Una de las razones por las que los enlaces de microondas son tan adaptables es su banda ancha. Esto significa que pueden transmitir grandes cantidades de información a alta velocidad. Otra cualidad importante de los enlaces de microondas es que no requieren equipos ni instalaciones entre los dos puntos terminales, por lo que instalar un enlace de microondas suele ser más rápido y económico que una conexión por cable. Finalmente, se pueden utilizar prácticamente en cualquier lugar, siempre que la distancia a cubrir esté dentro del alcance operativo del equipo y haya una ruta despejada (es decir, sin obstáculos sólidos) entre las ubicaciones. Las microondas también pueden atravesar la lluvia, la niebla y la nieve, lo que significa que el mal tiempo no interrumpe la transmisión.

Un enlace de microondas unidireccional simple incluye cuatro elementos principales: un transmisor, un receptor, líneas de transmisión y antenas. Estos componentes básicos existen en todos los sistemas de radiocomunicaciones, incluyendo teléfonos celulares, radios bidireccionales, redes inalámbricas y radiodifusión comercial.

Fuente [https://ethw.org/Microwave\_Link\_Networks]

**VSAT:**

Los sistemas **VSAT** (Very Small Aperture Terminal), son redes de comunicación por satélite que, empleando antenas de pequeñas dimensiones, permiten el establecimiento de una gran variedad de servicios de comunicaciones entre un gran número de puntos o estaciones remotas, pudiendo estar supervisadas por una estación principal llamada Hub, NOC o Telepuerto.

Gracias a su flexibilidad, rápida implementación y bajos costos de instalación y operación, la tecnología VSAT se utiliza cada vez más en el despliegue de redes para aplicaciones privadas, públicas/gubernamentales y corporativas.

En todos los sectores del mercado que requieren tareas cruciales y un sistema de comunicación altamente confiable, se utiliza la tecnología VSAT. Las redes basadas en tecnología VSAT se dividen en dos categorías principales: servicios dedicados y compartidos. Los servicios compartidos (TDMA) permiten que varias estaciones remotas compartan la misma red por división de tiempo. Los servicios dedicados se comunican entre sí sin necesidad de un concentrador y con una sola portadora por canal.

**Ventajas:**

* Facilidad y rapidez para la puesta en operación y la incorporación de nuevas terminales
* Acceso a lugares donde no está disponible otra infraestructura terrestre, por razones físicas o económicas
* Salvan prácticamente la totalidad de los obstáculos geográficos
* Alta calidad y disponibilidad de los enlaces
* Gestión centralizada y dependencia de un único Operador de Servicios
* Coste de terminales a la baja

Fuentes:[https://satcomdefensa.com/que-es-vsat/| https://www.icarusnet.it/en/vsat-technology/]

1. **Agregue dos tipos de enlaces, no mencionados anteriormente.**

**Fibra Óptica:**

Un enlace de fibra óptica suele ser parte de un sistema [de comunicaciones de fibra óptica](https://www.rp-photonics.com/optical_fiber_communications.html) que proporciona una conexión de datos entre dos puntos ( conexión punto a punto ). Consiste esencialmente en un transmisor de datos, una [fibra de transmisión](https://www.rp-photonics.com/fibers.html)  y un receptor. Incluso para distancias de transmisión muy largas, se pueden alcanzar velocidades de datos extremadamente altas, de muchos Gbit/s o incluso varios Tbit/s.

La capacidad de manejo de grandes cantidades de datos, el evitar el ruido asociado y el aislamiento eléctrico son sólo pocas de las características que hacen que la tecnología de la fibra óptica se ideal para usarse en los sistemas industriales y comerciales.

Fuentes [https://microcompbajio.com/enlaces-de-fibra-optica/ | https://www.rp-photonics.com/fiber\_optic\_links.html]

**Wifi Punto a Punto:**

Se utilizan antenas direccionales para establecer una conexión inalámbrica de alta velocidad y baja latencia entre dos dispositivos. Estos enlaces pueden emplearse para conectar edificios, redes, dispositivos móviles, zonas rurales, entre otros.

En general, los enlaces punto a punto son una solución efectiva para conectar dispositivos y redes en diferentes entornos, ya que ofrecen una comunicación directa y eficiente sin la necesidad de dispositivos intermedios, lo que puede mejorar la velocidad y la fiabilidad de la conexión.

Una de las principales aplicaciones de los enlaces Wifi punto a punto es conectar dos edificios separados por una distancia considerable. Esto se utiliza comúnmente en instalaciones industriales, campus universitarios, áreas rurales, entre otros. Al conectar los edificios a través de un enlace Wifi punto a punto, es posible compartir información y recursos, así como comunicarse entre ellos sin la necesidad de instalar cableado adicional.

Los enlaces Wifi punto a punto también se utilizan en la implementación de sistemas de vigilancia y seguridad. Por ejemplo, se pueden conectar cámaras de seguridad ubicadas en diferentes puntos de un campus universitario o una instalación industrial para monitorear la seguridad de una zona en particular. De esta manera, se puede compartir información de manera rápida y eficiente y mejorar la respuesta ante posibles amenazas.

Fuente [https://eltecnic.net/redes/que-es-un-enlace-punto-a-punto/?srsltid=AfmBOopTcTNyiLIDkblyiB7WLW-it7QL4Gt2RmvuphgdAoTmpIc4eLMB]

1. **Ranking de enlaces según lo pedido (de uno a seis, siendo uno el mejor): Por económico, performance, mayor capacidad, mayor o mejor configuración de restricciones, soporte a mayor distancia, menor esfuerzo de configuración.**

**Ranking por categorías:**

**1. Económico (menor costo de implementación y operación)**

1. Wi-Fi punto a punto (equipos baratos, poca infraestructura).
2. LAN to LAN (si ya hay cableado, solo se requiere interconexión).
3. Microonda (costo medio, depende de las torres).
4. Fibra Óptica (infraestructura cara de instalar).
5. MPLS (servicio contratado a un proveedor, no suele ser barato).
6. VSAT (carísimo por uso de satélite y mantenimiento).

**2. Performance (latencia y estabilidad)**

1. Fibra Óptica (mejor latencia y estabilidad).
2. LAN to LAN (muy estable en entornos locales).
3. MPLS (bueno, pero depende del proveedor).
4. Microonda (puede verse afectado por el clima).
5. Wi-Fi punto a punto (estable, pero menos robusto que microonda).
6. VSAT (latencia muy alta por la distancia al satélite GEO).

**3. Mayor capacidad (ancho de banda soportado)**

1. Fibra Óptica (terabits por segundo).
2. LAN to LAN (limitado al estándar Ethernet, pero muy alto).
3. MPLS (depende del contrato, pero muy capaz).
4. Microonda (varios Gbps, pero limitado por espectro).
5. Wi-Fi punto a punto (cientos de Mbps, máximo Gbps en casos).
6. VSAT (muy limitado en capacidad).

**4. Mayor o mejor configuración de restricciones (QoS, priorización, seguridad)**

1. MPLS (soporta QoS, priorización, VPNs).
2. Fibra Óptica (gran flexibilidad de configuración, especialmente en enlaces dedicados).
3. LAN to LAN (seguro y configurable en redes privadas).
4. Microonda (depende del proveedor/equipo, configurable).
5. Wi-Fi punto a punto (configurable, pero con más limitaciones).
6. VSAT (muy limitado en QoS por latencia y compartición).

**5. Soporte a mayor distancia**

1. VSAT (cubre miles de km, incluso zonas remotas).
2. Microonda (decenas de km por salto, se puede encadenar).
3. MPLS (depende del proveedor, puede abarcar ciudades/países).
4. Fibra Óptica (puede recorrer grandes distancias con repetidores, pero es caro).
5. Wi-Fi punto a punto (hasta decenas de km en condiciones ideales).
6. LAN to LAN (muy limitado, solo dentro de una misma red o con cableado físico).

**6. Menor esfuerzo de configuración (fácil de instalar y operar)**

1. LAN to LAN (prácticamente plug-and-play en la misma red).
2. Wi-Fi punto a punto (configuración inicial sencilla).
3. MPLS (proveedor lo entrega ya configurado).
4. Fibra Óptica (requiere instalación, pero después es estable).
5. Microonda (alineación de antenas y permisos, más complejo).
6. VSAT (requiere instalación, alineación al satélite y soporte técnico).

**d. Elija un tipo de enlace para los siguientes escenarios:**

**1 d. Conectividad de varios de call centers con un data center central.**

**MPLS**:

Porque permite conectar múltiples sedes a un mismo centro de datos con calidad de servicio (priorización de voz/datos), seguridad y gestión centralizada.

**2 d. Conectar los datos de los pozos petroleros durante 15 minutos por día.**

**VSAT**:

Ideal para zonas alejadas donde no llega fibra, microonda ni móvil. Aunque tiene alta latencia y costo, es perfecto para transmitir datos de forma puntual en lugares inhóspitos.

**3 d. Comunicar dos edificios enfrentados en la misma calle.**

**Wi-Fi punto a punto**:

Económico, fácil de instalar, y suficiente para distancias cortas. Alternativamente se podría usar **Fibra Óptica** si se busca algo más robusto, pero wifi es la solución más práctica.

**22- Describir la tecnología LTE.**

Long-Term Evolution o LTE es un**estándar inalámbrico de cuarta generación (4G)** que proporciona mayor capacidad de red y velocidad para teléfonos móviles y otros dispositivos celulares en comparación con la tercera generación (3G), pero con menor rendimiento (velocidad, retardo de propagación, etc.) que la tecnología 4G pura.

LTE ofrece velocidades máximas de transferencia de datos de**hasta 100 Mbps de bajada y 30 Mbps de subida**. Proporciona latencia reducida, capacidad de ancho de banda escalable y compatibilidad con versiones anteriores de la tecnología existente del Sistema Global para Comunicaciones Móviles (GSM) y del Servicio Universal de Telecomunicaciones Móviles (UMTS). La evolución LTE-Advanced (LTE-A) consigue tasas de hasta 300 Mbps.

LTE es una tecnología muy buena y estable con tres características clave: permite altas tasas de bits con baja latencia, es barato y fácil de desplegar por los operadores, y evita la fragmentación por el tipo de duplexación.

TE ofrece a los usuarios varias funcionalidades que los estándaresanteriores como 2G y 3G no son capaces de ofrecer:

1. **Transmisión de audio y vídeo:**LTE tiene velocidades de descarga y subida más rápidas que 2G y 3G.
2. **Conexión en tiempo real a los servicios:** con voz sobre LTE, los usuarios pueden hablar con otras personas sin experimentar retrasos ni fluctuaciones
3. **Velocidades aún más rápidas con LTE-Advanced:** las velocidades de descarga y subida son dos o tres veces más rápidas que las del LTE estándar. Todos los dispositivos LTE-Advanced son compatibles con versiones anteriores del LTE estándar.
4. **Agregación de portadoras de frecuencia:**esta característica de LTE-Advanced mejoró la capacidad de la red, agregando un ancho de banda de hasta 100 MHz en cinco portadoras (bandas) con un ancho de banda de 20 MHz cada una. Los teléfonos LTE-A combinan frecuencias de múltiples portadoras para mejorar la señal, la velocidad y la confiabilidad.

Fuentes [https://www.unir.net/revista/ingenieria/lte-que-es/ | <https://www.xataka.com/moviles/que-es-lte> | https://es.digi.com/blog/post/what-is-lte]

**23- Explique la solución de Microsoft Teams. Si quieren describir otra solución de otra empresa es también válido.**

Microsoft Teams es la aplicación más sofisticada de mensajería para su organización. Se trata de un espacio de trabajo pensado para la colaboración en tiempo real y la comunicación, las reuniones, el uso compartido de archivos y aplicaciones, e incluso para los ocasionales emojis. Todo en un único lugar, en equipo, y con todo a disposición de todos.

En su forma más básica, Microsoft Teams es una forma para que las organizaciones agilicen sus actividades, abran las líneas de comunicación, protejan sus datos confidenciales y, en última instancia, operen a una mayor capacidad.

Fuentes [https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-microsoft-teams-3de4d369-0167-8def-b93b-0eb5286d7a29 | https://antares.solutions/what-we-do/modern-workplace-solutions/microsoft-teams-solution/]

**24- ¿Qué significa aplicar calidad en un enlace MPLS?**

Aplicar calidad a un enlace MPLS significa utilizar la tecnología para garantizar un rendimiento predecible y optimizado, priorizando el tráfico sensible como la voz o el video para reducir latencia y jitter (fluctuación de la señal), asignando diferentes clases de servicio (CoS) y ancho de banda según la importancia de la aplicación. Esto se logra mediante la implementación de mecanismos de Calidad de Servicio (QoS) que clasifican el tráfico y lo enrutan por rutas predefinidas y con recursos asignados, asegurando una experiencia consistente para los usuarios.

**33- ¿Qué experiencia tienen en redes?**

En lo personal, no tengo experiencia con redes. Mis únicos acercamientos fueron en el tercer cuatrimestre de la carrera, donde vimos un poco de redes, en la materia ‘TIC’ y luego esta materia de ‘Programación sobre redes’.