

Trabajo Práctico Integrador - Seguridad en los sistemas mediante segmentación de redes

Alumnos: Barroeta Victor Manuel Email: vcmanuelbarroeta@gmail.com

Beauvallet Pablo Nahuel Email: pablonahuelbeauvallet@gmail.com

Materia: Arquitectura y Sistemas Operativos

Profesor: Mauricio Gabriel Pasti

Docente tutor: David Roco

Fecha de Entrega: 05 de junio de 2025

Índice

1. Introducción
2. Marco Teórico
3. Caso Práctico
4. Metodología Utilizada
5. Resultados Obtenidos
6. Conclusiones
7. Bibliografía
8. Anexos

1- INTRODUCCIÓN

La segmentación de redes es uno de los mecanismos más importantes para proteger una red de posibles amenazas de ciberseguridad. En este trabajo intentamos poner en valor la importancia del concepto de segmentación mostrando dos casos prácticos a través de esquemas en Packet Tracer, analizando sus ventajas y desafíos.

Entendemos que, por ser estudiantes de la Tecnicatura en Programación, un aspecto importante es la seguridad, por lo cual la segmentación de redes no sería un tema menor para tener en cuenta tanto sea en el desarrollo de aplicaciones, software en general y la administración de sistemas.

El objetivo primordial es probar a través de una topografía la incomunicación entre distintas subredes la mejora en cuanto a seguridad limitando el acceso entre diferentes partes de una red mediante diferentes métodos de segmentación reduciendo el riesgo de ataques, así como también la facilitación de la administración.

2- MARCO TEÓRICO

¿Qué es la segmentación de redes?

La segmentación de redes es una estrategia de seguridad que consiste en dividir una red informática en subredes más pequeñas o segmentos (Kayleigh, 2023). Esto es tomar una red plana en donde todos los equipos se encuentran en una misma red y partir dicha red en múltiples redes de modo que la comunicación entre ciertos equipos no sea directa.

Cada segmento opera como una entidad independiente, con sus propias políticas de seguridad y control de tráfico, lo que permite limitar el movimiento lateral de amenazas dentro de la red y mejorar el rendimiento general (Frankel, 2022). Por ende, si existiera una brecha de seguridad por la infestación con un ransomware o bien cualquier otro malware no se extendería por toda la red.

La segmentación funciona controlando el flujo de tráfico entre las partes. Se puede optar por impedir que el tráfico de una parte llegue a otra, o limitar el flujo por tipo de tráfico, origen, destino y muchas otras opciones añadiendo firewalls, listas de control de accesos (ACLs) o restricción de permiso en las IPs o MAC de los dispositivos.

Existen dos enfoques principales para la segmentación de redes:

- **Segmentación física:** Implica el uso de hardware separado, como routers y switches, para dividir la red en segmentos distintos.
- **Segmentación lógica:** Utiliza tecnologías como VLANs y listas de control de acceso (ACLs) para crear segmentos virtuales dentro de la misma infraestructura física. (Gowda, 2025)

Tipos de segmentación de red

Además de la segmentación física y lógica, existen otros métodos que se adaptan a diferentes necesidades de seguridad y rendimiento (Gowda, 2025):

- **VLANs (Redes de Área Local Virtuales):** Permiten agrupar dispositivos en segmentos lógicos, independientemente de su ubicación física, facilitando la gestión y mejorando la seguridad. Cada VLAN actúa como una subred separada, lo que mejora la seguridad y la organización de la red. Al asignar dispositivos a diferentes VLANs, se puede controlar el acceso y el flujo de

tráfico entre segmentos.

- **Microsegmentación**: Ofrece un control más granular al aplicar políticas de seguridad a nivel de máquina o aplicación, lo que es especialmente útil en entornos de centros de datos y nubes .
- **Segmentación mediante firewalls internos**: Utilizar firewalls para controlar el tráfico entre segmentos de red, aplicando políticas específicas que determinan qué tipo de tráfico está permitido o denegado .

Beneficios de la segmentación de redes

Implementar una segmentación adecuada en la red conlleva múltiples ventajas (Cisco,2023):

- **Mejora de la seguridad**: Limita la propagación de amenazas al contenerse dentro de un segmento específico.
- **Optimización del rendimiento**: Reduce la congestión al disminuir la cantidad de dispositivos en cada segmento, lo que mejora la eficiencia del tráfico de red.
- **Facilitación del cumplimiento normativo**: Permite aplicar controles de acceso más estrictos y proteger datos sensibles, ayudando a cumplir con regulaciones como PCI-DSS (Payment Card Industry Data Security Standard) u otras normas como las ISO.
- **Simplificación de la gestión**: Al dividir la red en segmentos más pequeños, se facilita la administración y el monitoreo de la infraestructura

Listas de Control de Acceso (ACLs)

Las ACLs son conjuntos de reglas que controlan el tráfico de red permitiendo o denegando paquetes basados en criterios como direcciones IP, protocolos y puertos. Se utilizan para implementar políticas de seguridad específicas y controlar el acceso entre segmentos de red (Kayleigh, 2023). Existen dos tipos principales:

- **ACLs estándar**: Filtran el tráfico basándose únicamente en la dirección IP de origen.
- **ACLs extendidas**: Permiten un control más detallado al considerar tanto la dirección IP de origen como la de destino, así como el protocolo y el puerto .

En el contexto de VLANs, las ACLs pueden aplicarse en interfaces de routers o switches multicapa para controlar el tráfico entre VLANs específicas.

Firewalls

Los firewalls son dispositivos o programas que monitorean y controlan el tráfico de red entrante y saliente basándose en reglas de seguridad predefinidas. Actúan como una barrera entre redes confiables y no confiables, como Internet, y son fundamentales para proteger la red contra accesos no autorizados y amenazas externas (Gowda, 2025).

Existen diferentes tipos de firewalls:

- **Firewalls de red**: Protegen el perímetro de la red y controlan el tráfico entre diferentes redes.
- **Firewalls de host**: Se instalan en dispositivos individuales para controlar el tráfico hacia y desde ese dispositivo específico.
- **Firewalls de próxima generación (NGFW)**: Ofrecen funcionalidades avanzadas como inspección profunda de paquetes, prevención de intrusiones y control de aplicaciones.

La implementación de firewalls internos entre segmentos de red permite aplicar políticas de seguridad más estrictas y controlar el tráfico lateral dentro de la red.

Ejemplos de segmentación de redes

En las siguientes imágenes se muestra un esquema de una red plana y sus conexiones con la red, en la segunda imagen vemos el mismo esquema, pero con una correcta segmentación de las redes.

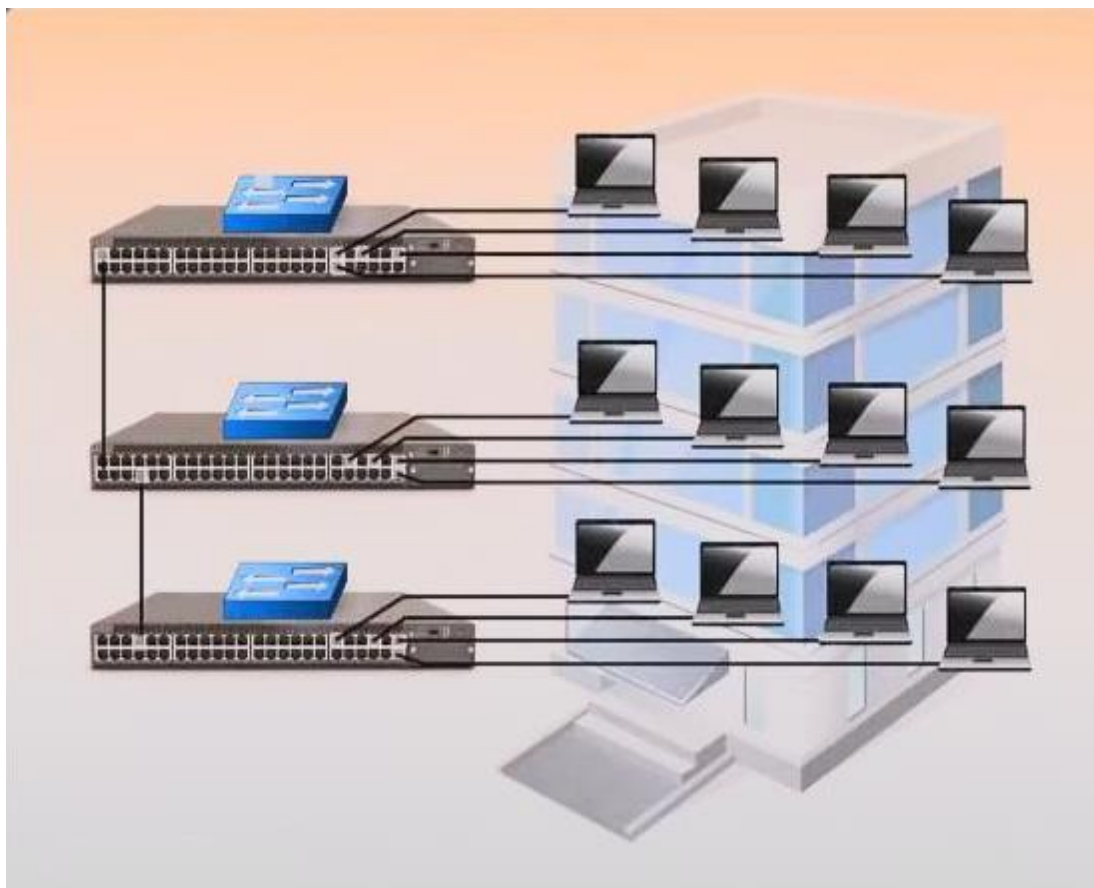


Figura 1. topografía sin segmentación de redes

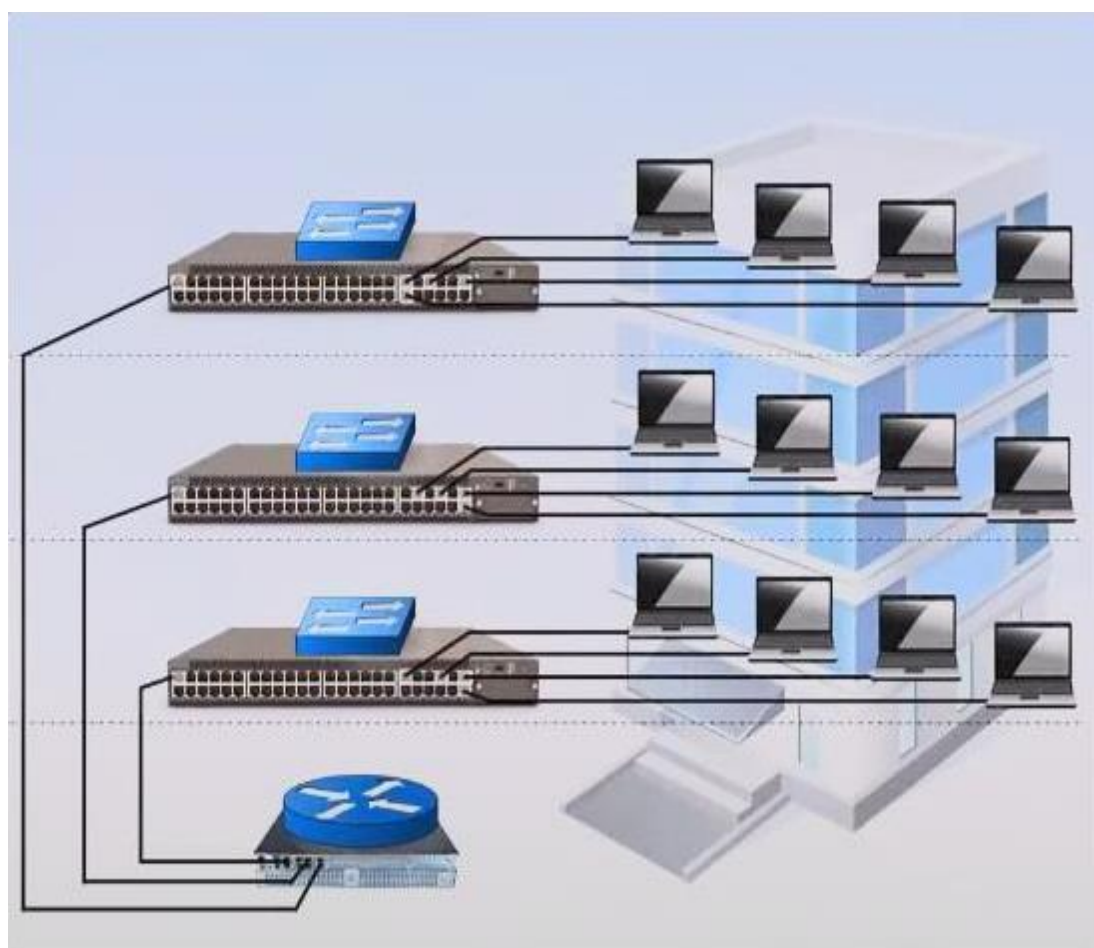


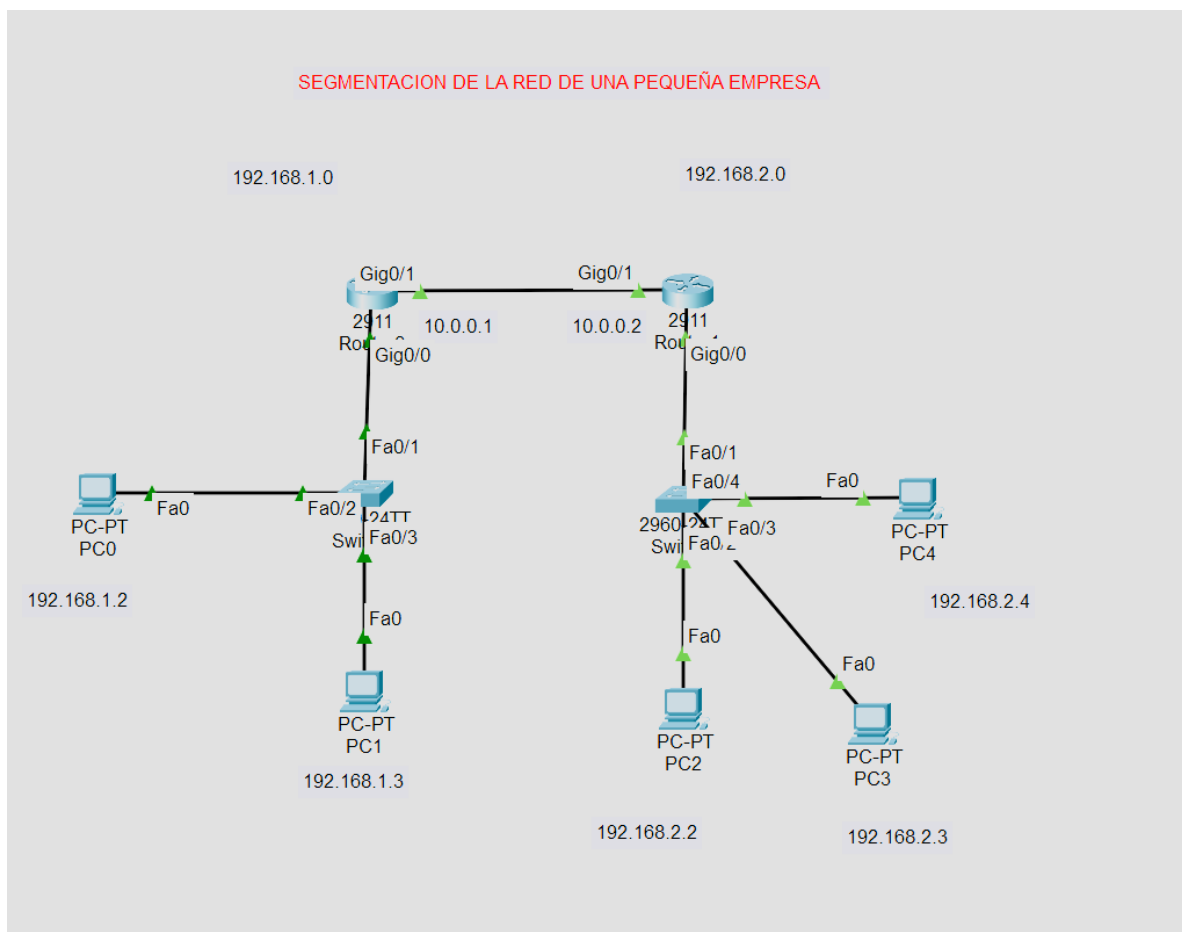
Figura 2. topografía con segmentación de redes

Ambas topologías son claras, en la primera los switches se interconectan entre sí directamente, no hay router ni firewalls, todos los equipos forman parte de la misma VLAN, así como también formarán parte de la misma red IP. La segunda imagen muestra una red parecida, pero con una gran diferencia, esto es que cada switch se conecta únicamente con el router y por este motivo para que un equipo de un switch se pueda comunicar con otro equipo de otro switch, tendrá que pasar indefectiblemente por el router. Este es el fiel reflejo de segmentar físicamente una red.

3- CASO PRÁCTICO

Teniendo como situación concreta la de mejorar la seguridad de una red de una pequeña empresa se planteó dos diferentes escenarios para crear una segmentación segura, utilizamos Cisco Packet Tracer para realizar dos esquemas de diferentes maneras de cómo podríamos segmentar una red.

Caso 1: Segmentación de red mediante subredes y router intermedio



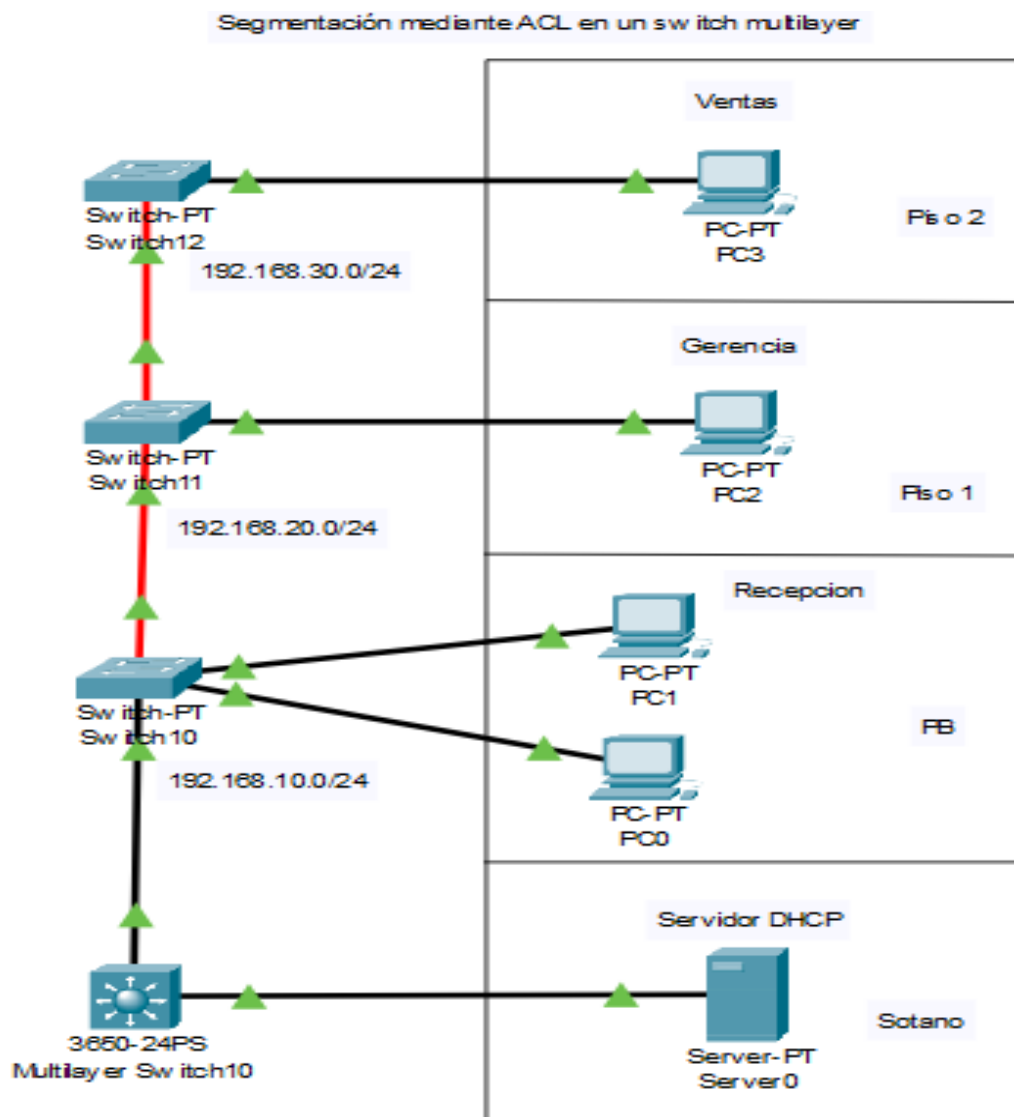
En este primer caso se diseñó una topología de red para ilustrar la segmentación mediante el uso de subredes IP separadas y un router intermedio. La propuesta parte de una situación donde todos los dispositivos se encontraban inicialmente en una red plana, compartiendo el mismo dominio de broadcast. En el diagrama de red muestra una configuración segmentada, la cual se divide dicha red en dos subredes (192.168.1.0/24 y 192.168.2.0/24), de esta manera, se mejora la seguridad y eficiencia, permitiendo una mejor organización en los dispositivos que conforman la red, así como también un control más preciso en el tráfico.

Cada subred se conectó a un switch independiente, y ambos switches fueron conectados a un router central. Esta configuración obliga a que cualquier comunicación entre equipos de distintas subredes pase obligatoriamente por el router, lo que permite implementar políticas de control y aislamiento si fuese necesario.

Esta segmentación es representativa de una configuración básica pero efectiva, al aislar las dos subredes él una de la otra se reduce la exposición ante posibles ataques cibernéticos o programas maliciosos afecten a toda la empresa. A su vez, mejora el control del tráfico entre las secciones.

Esta red se podría complejizar aún más añadiendo firewalls de red en cada subred o en cada host para restringir el acceso entre segmentos, permitiendo solo el tráfico que la empresa quiera desde y hacia la red.

Caso 2: Segmentación mediante VLANs y ACL en un switch multic



En este segundo caso práctico se simuló un escenario de red en otra pequeña empresa con otra infraestructura ya que es un edificio, donde se buscaba aplicar una segmentación lógica más avanzada utilizando VLANs (Redes de Área Local Virtuales) y una Lista de Control de Acceso (ACL) para reforzar la seguridad interna. La topología fue diseñada en el mismo programa antes mencionado e implementando una switch multicapa (Capa 3) que se utilizó para enrutar el tráfico entre las VLANs y para aplicar las políticas de control mediante el ACL anteriormente nombrado, a su vez un servidor DHCP que asigna direcciones IP de forma automática.

El objetivo fue impedir que la red de Recepción (VLAN 10, 192.168.10.0/24) accediera a los recursos de las áreas de Gerencia (VLAN 20, 192.168.20.0/24) y Ventas (VLAN 30, 192.168.30.0/24), asegurando así una segmentación que refuerce la confidencialidad y reduzca los riesgos de acceso no autorizado entre sectores.

Esta red se podría complejizar aún más añadiendo firewalls de red en cada VLAN o en cada host para restringir más los accesos, permitiendo solo el tráfico que la empresa quiera desde y hacia la red.

4- METODOLOGÍA APLICADA

Para el desarrollo de este trabajo, en principio se planteó una metodología en varias etapas, combinando el estudio conceptual con la simulación práctica de escenarios. A continuación, se describen los pasos seguidos:

- **Investigación previa**

En primer lugar, se llevó a cabo una investigación teórica sobre el concepto de segmentación de redes, sus tipos (física, lógica, por VLANs, por ACLs, etc.), y su importancia dentro del campo de la ciberseguridad ya que el tema de interés tenía que tener relación con la seguridad de sistemas. Se consultaron fuentes académicas, documentación oficial de Cisco, bibliografía del curso y contenidos complementarios (videos y presentaciones).

Durante esta etapa, se comprendió que la segmentación de redes no solo mejora la organización y eficiencia del tráfico, sino que es una medida clave para contener amenazas y limitar el movimiento lateral de los atacantes dentro de una red comprometida.

- **Etapas de diseño y prueba del código**

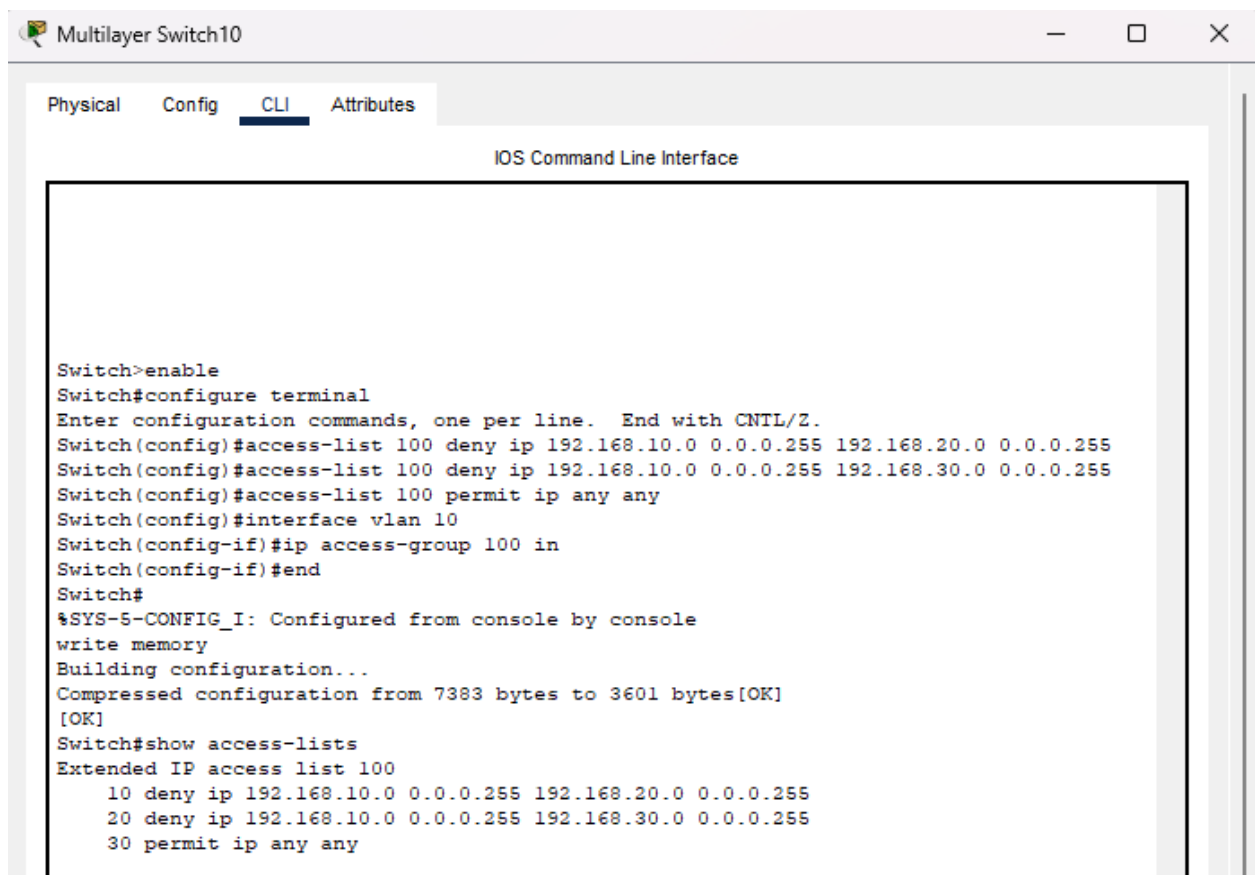
Una vez consolidada la información teórica, se diseñaron dos escenarios prácticos en programa Cisco Packet Tracer para lo cual tuvimos que ahondar más sobre la configuración de dispositivos. Las pruebas del diseño fueron realizadas en el mismo programa a través del envío de paquetes utilizando el comando ping

- En el **primer caso**, se verificó que las PC de distintas subredes no podían

comunicarse entre sí, si no estaban conectadas a través del router.

- En el **segundo caso**, los ping desde Recepción hacia Gerencia y Ventas fueron bloqueados por la ACL, mientras que los ping dentro de la misma VLAN (Recepción ↔ Recepción) funcionaron correctamente entregados.

Para evitar que los dispositivos de Recepción se conecten con los dispositivos de Gerencia y Ventas se aplicó un ACL en el CLI del multiplayer Switch podemos ver la siguiente configuración:



```
Multilayer Switch10
Physical Config CLI Attributes
IOS Command Line Interface

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Switch(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Switch(config)#access-list 100 permit ip any any
Switch(config)#interface vlan 10
Switch(config-if)#ip access-group 100 in
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Switch#show access-lists
Extended IP access list 100
 10 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
 20 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
 30 permit ip any any
```

```
access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

```
access-list 100 permit ip any any
```

Esta lista bloquea cualquier intento de comunicación desde la VLAN 10 hacia las VLANs 20 y 30. Luego se aplicó la ACL en la interfaz VLAN correspondiente:

```
interface vlan 10
```

```
ip access-group 100 in
```

A su vez, se aseguró que los dispositivos de la VLAN 10 tengan acceso a Internet, este también sería posible gracias a la última regla permit ip any any.

- **Trabajo colaborativo**

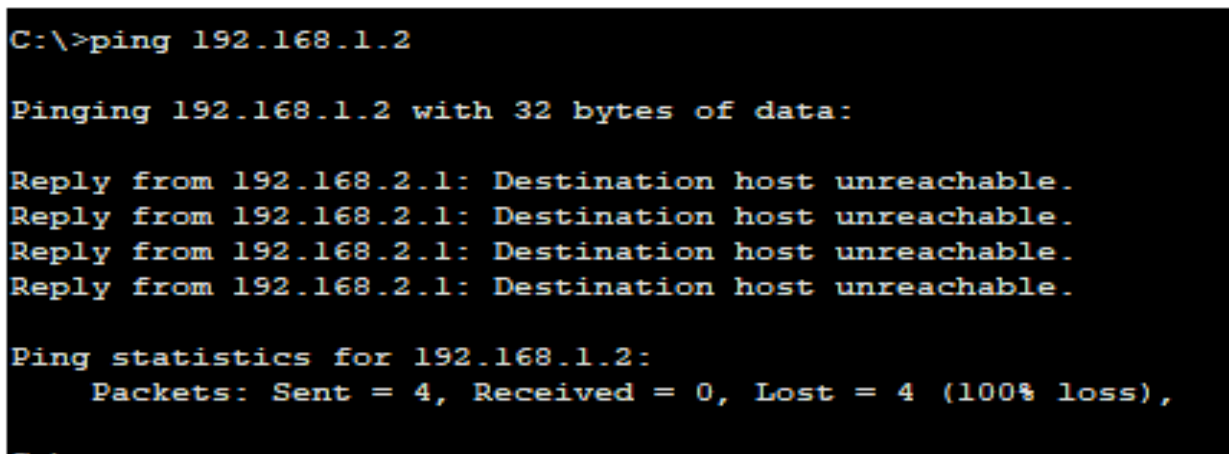
El trabajo colaborativo tuvo como eje la prueba y testeo de diferentes esquemas, aprendiendo y enriqueciéndonos sobre la marcha a través de intercambio que se fueron dando tanto como en esta etapa así también como en posteriores que respondieron a la puesta en escena de la topografía en el trabajo práctico.

La repartición de las tareas del grupo en la parte del marco teórico fue equitativo el aporte de información y nos separados dos casos a plantear para dos diferentes tipos de segmentaciones anotando cada uno la metodología a realizar y los resultados que se obtuvieron y reunión toda la información explicando todo lo teórico e integrándolo todo.

5- RESULTADOS OBTENIDOS

El resultado obtenido nos parece satisfactorio. A través del esquema del Caso 1, configuramos los distintos dispositivos que conforman ambas subredes con sus respectivas direcciones IP. Con ello, intentamos proporcionar un marco teórico claro sobre la segmentación de redes, explicando su importancia y funcionamiento en la práctica. En el Caso 2, aplicamos lo aprendido durante el trabajo práctico para diseñar una topología más compleja, integrando nuevos conceptos y técnicas.

En el **Caso 1**, verificamos la conectividad entre dispositivos utilizando el comando ping, una herramienta útil para comprobar la comunicación dentro de una red. Desde el host PC2, con la dirección IP 192.168.2.3, ejecutamos el comando ping hacia el host PC0, con IP 192.168.1.2, ubicado en la otra subred. El resultado obtenido muestra que los paquetes no llegan a su destino, lo que indica que no existe comunicación entre ambas subredes.

A screenshot of a Windows command prompt window with a black background and white text. The text shows a user entering the command 'C:\>ping 192.168.1.2'. The system responds with 'Pinging 192.168.1.2 with 32 bytes of data:'. This is followed by four lines of 'Reply from 192.168.2.1: Destination host unreachable.'. Finally, it shows 'Ping statistics for 192.168.1.2:' followed by 'Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),'.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

A diferencia del caso a que refiere la imagen anterior en la siguiente captura, si realizamos un ping hacia una IP que corresponde a un dispositivo de la misma subred, se puede verificar la conectividad a través del envío de paquetes tal como demuestra la próxima captura en la que desde la PC2 cuya IP es 192.168.2.2 se realiza un ping hacia la PC3 IP 192.168.2.3.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

En el **Caso 2**, se construyó una topología más avanzada basada en VLANs gestionadas por una switch multicapa, con un servidor se creó un servidor DHCP dedicado para automatizar la creación de IP en para cada segmento (Recepción, Gerencia y Ventas) a este servidor fue llamado Server0. A través de la implementación de una ACL extendida, se restringió el acceso de la VLAN de Recepción a las otras dos VLANs, garantizando así una segmentación lógica con control de acceso personalizado.

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 192.168.0.0

Subnet Mask: 255.255.255.0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	T S
VLAN30	192.168.30.1	0.0.0.0	192.168.30.5	255.255.255.0	250	0.0.
VLAN20	192.168.20.1	0.0.0.0	192.168.20.5	255.255.255.0	251	0.0.
VLAN10	192.168.10.1	0.0.0.0	192.168.10.5	255.255.255.0	251	0.0.
serverPool	0.0.0.0	0.0.0.0	192.168.0.0	255.255.255.0	512	0.0.

Con la realización de un ping en la consola de un host en la VLAN de recepción se logró constatar que ese segmento estaba aislado de todas las demás VLANs

Mientras que en el propio segmento de la VLAN de recepción si se podía pasar

paquetes desde un host a otro.

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

En cuanto a las dificultades que enfrentamos, la mayoría estuvieron relacionadas con la configuración de dispositivos en Packet Tracer más que todo en el caso de switch multicapa y la ACL. Estas fueron superadas a través del trabajo colaborativo e investigación lo que nos permitió encontrar soluciones de manera eficiente.

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>ping 192.168.30.5

Pinging 192.168.30.5 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Otra dificultad importante fue definir el enfoque adecuado para el tema elegido, ya que la segmentación de redes es un concepto amplio. Sin embargo, logramos delimitar el alcance y estructurar el contenido de manera coherente.

6- CONCLUSIONES

A lo largo de este trabajo, hemos analizado la segmentación de redes y su impacto en la seguridad informática. Entendemos que, en entornos donde existe información sensible plausible de tener un valor, la segmentación es un factor clave para mejorar la protección de los datos. Sin embargo, también reconocemos que, por sí sola, no es suficiente.

Para garantizar una seguridad informática integral, la segmentación debe complementarse con otras estrategias y mecanismos. Entre ellos, se destacan la implementación de políticas de acceso, el uso de firewalls tal como se hizo mención en este trabajo práctico.

Entendemos que como todo está en permanente cambio, es indispensable continuar explorando y adaptando medidas de seguridad que estén a la altura de las nuevas amenazas que vayan surgiendo. La segmentación de redes, el tema que nos interesó y elegimos es un punto de partida, un comienzo para este mundo tan complejo que es el de la ciberseguridad.

7- BIBLIOGRAFÍA

- Andrew S. Tanenbaum, Nick Feamster, David Wetherall (2023) Redes de computadoras.
- Canal de Youtube "NASeros"
https://www.youtube.com/results?search_query=NASEROS
- Material estudio de la materia Arquitectura y Sistemas Operativos módulo 4 - Redes. Tecnicatura Universitaria en Programación a Distancia (2025). Universidad Tecnológica Nacional.
- Material estudio de la materia Arquitectura y Sistemas Operativos módulo 8 - Seguridad en los sistemas. Tecnicatura Universitaria en Programación a Distancia (2025). Universidad Tecnológica Nacional.
- Cisco. (2023). *What Is Network Segmentation?*. Recuperado de <https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html>
- AlgoSec. (2023). Network segmentation vs. VLAN explained. Recuperado de <https://www.algosec.com/post/network-segmentation-vs-vlan>
- Amir Frankel.(25 de septiembre de 2022). Network segmentation: All you need to know about its benefits. Zero Networks. Recuperado de <https://zeronetworks.com/blog/network-segmentation-all-you-need-to-know>
- CrowdStrike. (2023). What is Network Segmentation?. Recuperado de <https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/network-segmentation/>
- Kayleigh (27 de marzo de 2023). What is network segmentation: Understanding the basics. Jimber. Recuperado de <https://jimber.io/blog/what-is-network-segmentation-understanding-the-basics-b>
- Prajwal Gowda (29 de marzo de 2025). Exploring the 7 Types of Network Segmentation and How Each Method Enhances Network Security. Ampcus

Cyber. Recuperado de <https://www.ampcuscyber.com/blogs/types-of-network-segmentation/>