

2025



Cómo funciona la segmentación de red: **Componentes y Capacidades clave**

Magdalena Gonzalez 4-819-1590

Irvin Martinez 4-834-1736

Justing He 8-1045-2230

Adrian Jimenez 4-839-2413



Introducción

La segmentación de red es una estrategia fundamental en la seguridad y administración de redes modernas. Su principal objetivo es dividir una red en segmentos más pequeños o subredes, con el fin de mejorar el control del tráfico, optimizar el rendimiento y reforzar la seguridad frente a amenazas.

Esta técnica permite aislar diferentes áreas de la red, limitar el acceso no autorizado y prevenir el movimiento lateral de atacantes en caso de una brecha.

Para lograrlo, se utilizan diversos componentes clave como los cortafuegos internos, las listas de control de acceso (ACL), las VLAN y las subredes, que trabajan en conjunto para garantizar un entorno seguro y ordenado dentro de la infraestructura de red.





Funcionamiento de la Segmentación de red

La segmentación de red representa una estrategia de ciberseguridad que divide un entorno de red amplio en subredes más pequeñas, cada una con políticas y controles propios. Esta práctica no solo refuerza la protección de los recursos, sino que también facilita la administración, optimiza el rendimiento y reduce los riesgos asociados a accesos no autorizados o movimientos laterales de atacantes.

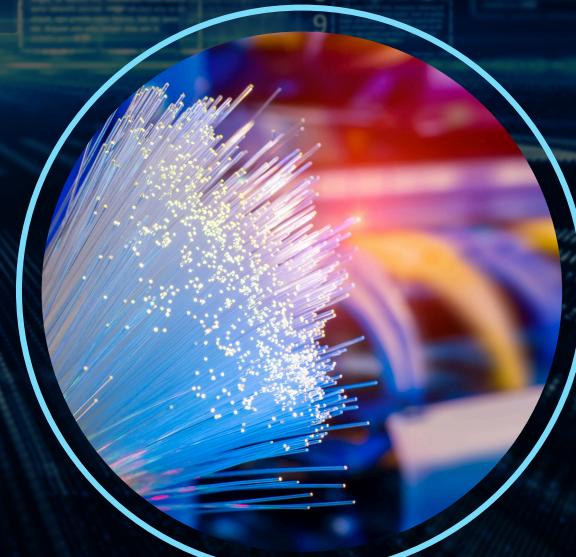
**OFRECE UN ESQUEMA
ROBUSTO**



Controles Fundamentales



Los firewalls internos funcionan como guardianes que supervisan el tráfico entre segmentos.

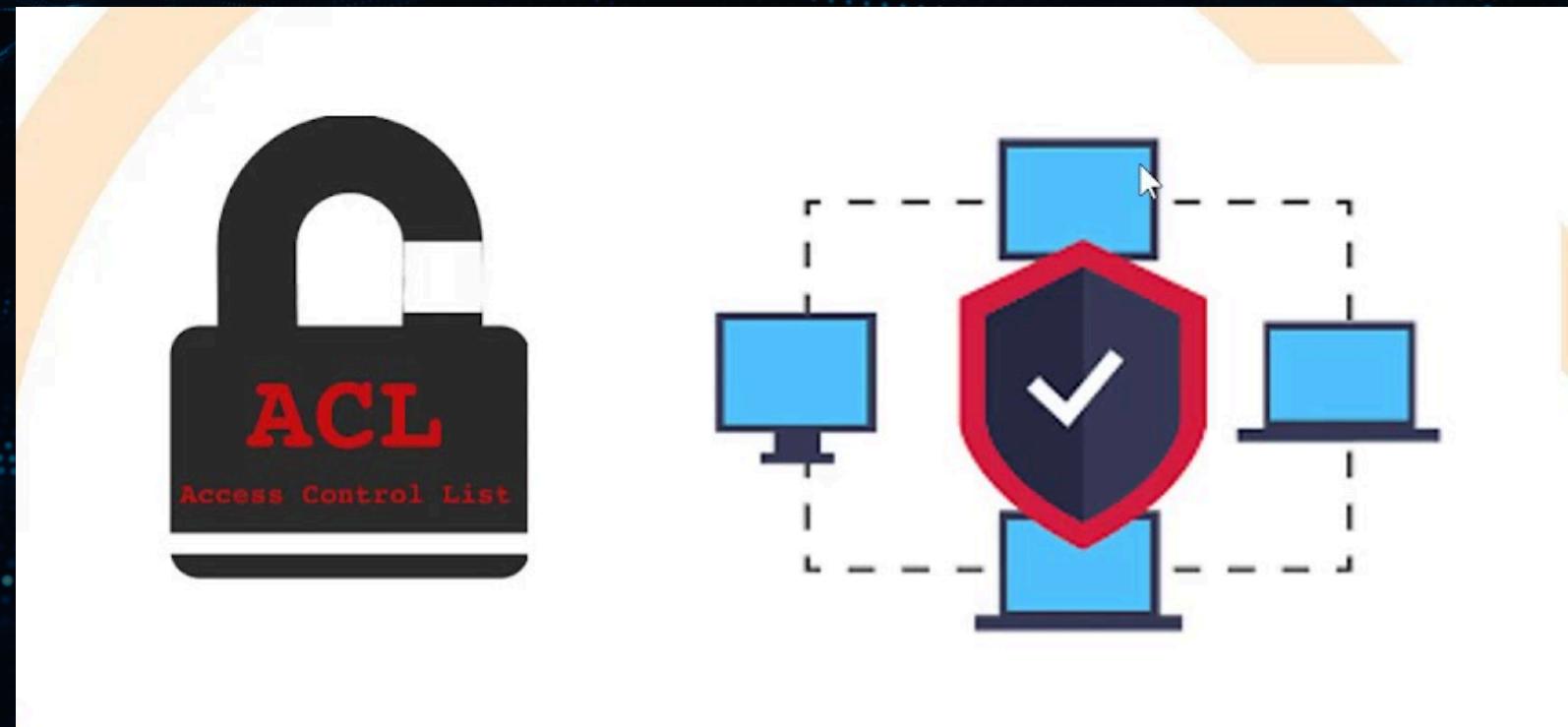


Estos dispositivos deciden qué comunicaciones están permitidas y cuáles deben bloquearse, evitando que actores maliciosos se desplacen lateralmente de una subred a otra.

ACLs

Definen reglas basadas en IP, puerto, protocolo o identidad de usuario, permitiendo solo tráfico autorizado.

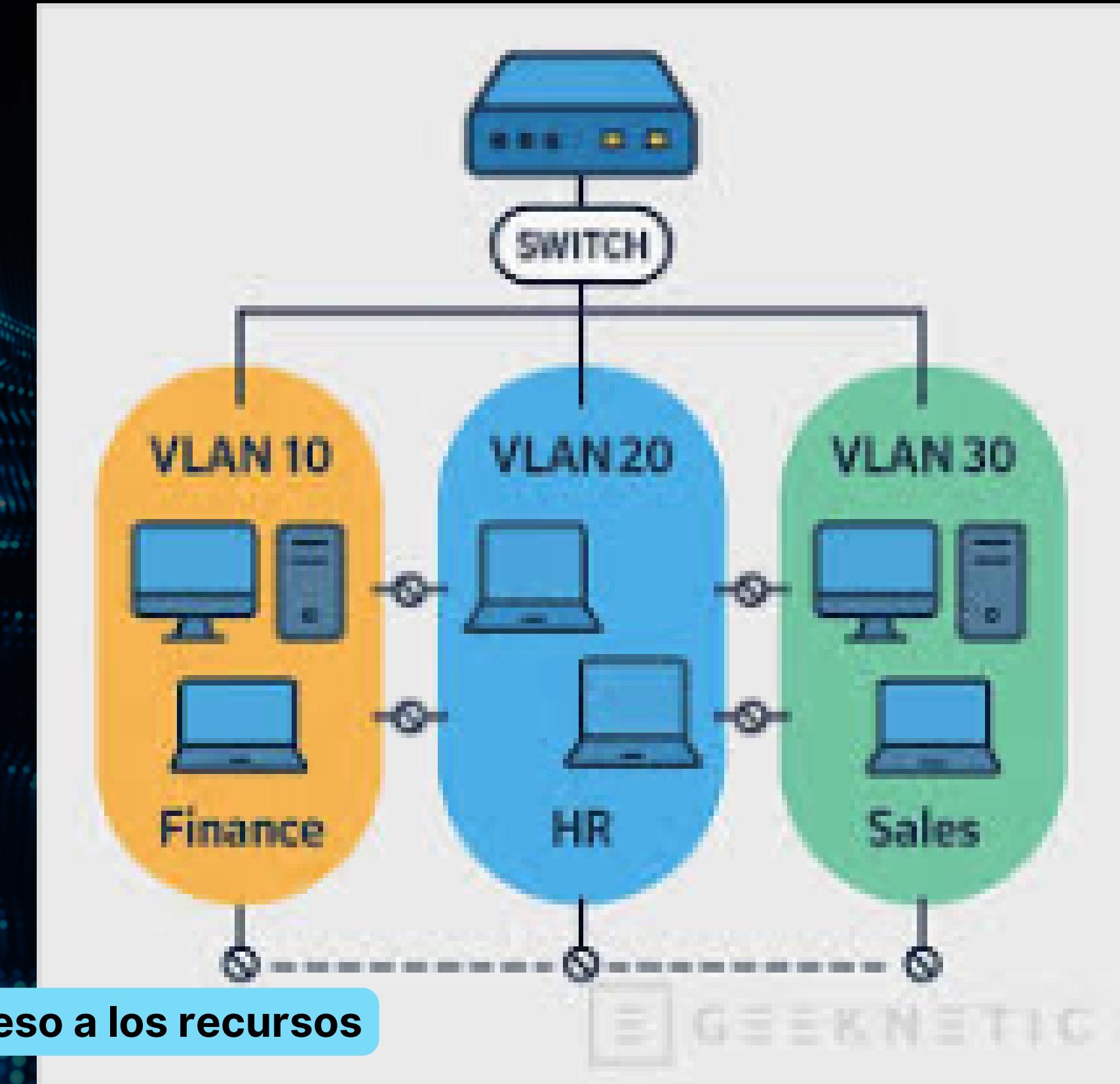
- **Ejemplo:** Si un atacante compromete un equipo en finanzas, las ACLs y firewalls internos evitan que acceda al servidor de recursos humanos.



VLANs y subredes

- **VLANs:** Agrupan usuarios, puertos o switches específicos, aislando el tráfico entre ellas.
- **Subredes:** Asignan rangos de direcciones IP independientes, aplicando políticas de seguridad por segmento.

Aislar el tráfico entre VLAN y controlar el acceso a los recursos



Ejemplo práctico



Situación:

Una empresa de servicios financieros maneja información sensible de clientes, como datos bancarios, historiales crediticios y documentos legales. La red corporativa incluye varias áreas: administración, desarrollo, atención al cliente y servidores críticos de bases de datos.

VLANs para segmentación lógica

- Se crean VLANs separadas para cada área: administración, desarrollo y atención al cliente.

Firewalls internos

- Entre cada VLAN se instalan firewalls internos que aplican políticas de acceso estrictas.

Listas de Control de Acceso (ACLs)

- Se configuran ACLs que permiten o bloquean el tráfico según IP, puerto y protocolo.



Conclusion

En resumen, la segmentación de red es una práctica esencial para proteger y gestionar eficazmente las redes empresariales.

Mediante el uso de cortafuegos internos y ACL, se controlan los flujos de tráfico entre subredes; y gracias a las VLAN y subredes, se logra una organización lógica y segura del entorno.

Estos mecanismos no solo fortalecen la seguridad al limitar el acceso y aislar amenazas, sino que también permiten una administración más eficiente, reduciendo riesgos y mejorando la resiliencia ante ataques.

Implementar una segmentación adecuada es, por tanto, una de las mejores defensas frente a la complejidad y vulnerabilidades de las redes modernas.



REFERENCIAS

Frankel, A. (2025, 11 junio). Network segmentation: All you need to know about its benefits.
<https://zeronetworks.com/blog/network-segmentation-all-you-need-to-know>



Gracias