edulearn
Revista Multidisciplinar

Buenas prácticas de seguridad para redes empresariales: Implementación de VLANs, ACLs y Router-on-a-Stick

Best practices for enterprise network security: Implementing VLANs, ACLs, and Router-on-a-Stick

Joselyn Katiuska Franco Ávila[1*], Mario Sebastián Ávila León[1]

Camilly Yuliana Pacheco Ordoñez[1], Marlon Steven Sisalima Ulloa[1]

Gregory Iván Sornoza Púa[1], Anthony André Tenesaca Lanchi[1]

[1] *Universidad Técnica de Machala, Ecuador*

* *Autor de Correspondencia: jfranco9@utmachala.edu.ec*

Resumen: En los últimos años, la seguridad de las redes empresariales se ha vuelto un factor decisivo, en buena medida por el aumento de accesos no autorizados, la circulación de malware y el uso indebido de servicios internos en infraestructuras cada vez más complejas. En este contexto, la segmentación lógica con VLAN, el uso de listas de control de acceso (ACL) y el empleo de Router-on-a-Stick se han convertido en herramientas habituales para aislar zonas sensibles de la red y aplicar el principio de mínimo privilegio en entornos tradicionales. Sin embargo, en la práctica persiste incertidumbre sobre cómo integrar estas tecnologías en diseños coherentes, verificables y escalables para redes de pequeña y mediana escala. Para abordar esta

problemática, se desarrolló un estudio aplicado bajo la metodología Cisco PPDIOO en una topología empresarial simulada, que incorporó dominios diferenciados para usuarios, servidores y gestión, subinterfaces con encapsulación 802.1Q y políticas de acceso alineadas con la tríada de confidencialidad, integridad y disponibilidad. Los resultados experimentales demostraron que el acceso administrativo quedó restringido exclusivamente a la VLAN de gestión, que el tráfico inter-VLAN se limitó a servicios específicos (HTTP/HTTPS e ICMP controlado) y que todo flujo no autorizado fue bloqueado por defecto, sin afectar la conectividad legítima intra-VLAN. Este trabajo aporta un marco comparativo y reproducible para orientar el diseño de redes segmentadas, y plantea como implicaciones la necesidad de automatizar configuraciones, integrar monitoreo continuo y validar la solución en escenarios de mayor escala y criticidad operativa.

Palabras clave: Seguridad; VLAN; ACL; enrutamiento; segmentación lógica.

Abstract: In recent years, the security of enterprise networks has become a critical factor, largely due to the increase in unauthorized access, the spread of malware, and the misuse of internal services in increasingly complex infrastructures. In this context, logical segmentation with VLANs, the use of access control lists (ACLs), and the implementation of Router-on-a-Stick have become standard tools for isolating sensitive areas of the network and applying the principle of least privilege in traditional environments. However, in practice, uncertainty persists regarding how to integrate these technologies into coherent, verifiable, and scalable designs for small and medium-sized networks. To address this issue, an applied study was conducted using the Cisco PPDIOO methodology in a simulated enterprise topology. This topology incorporated separate domains for users, servers, and management, subinterfaces with 802.1Q encapsulation, and access policies aligned with the triad of confidentiality, integrity, and availability. The experimental results demonstrated that administrative access was restricted exclusively to the management VLAN, that inter-VLAN traffic was limited to specific services (controlled HTTP/HTTPS and ICMP), and that all unauthorized flow was blocked by default, without affecting legitimate intra-VLAN connectivity. This work provides a comparative and reproducible framework to guide the design of segmented

networks and suggests the need to automate configurations, integrate continuous monitoring, and validate the solution in larger-scale and more critical operational scenarios.

Keywords: Security; VLAN; ACL; routing; logical segmentation.

1. Introducción

Las buenas prácticas de seguridad en redes empresariales han pasado a ocupar un lugar central, sobre todo por el aumento de malware, accesos no autorizados y ataques de denegación de servicio que afectan a infraestructuras cada vez más complejas (García-Pagan, 2007; Guijarro, 2023). En este contexto, la segmentación lógica mediante VLAN, el uso de listas de control de acceso y el enrutamiento inter-VLAN con Router on a Stick se utilizan para separar funciones, limitar el alcance de los ataques y simplificar el control del tráfico, aunque durante años estas soluciones se apoyaron en configuraciones manuales poco escalables (Alimi & Mufutau, 2015).

Sin embargo, con el aumento de la escala y sofisticación de las redes empresariales, ha sido necesario recurrir a enfoques más estructurados y alineados con marcos de gestión de riesgos y estándares de ciberseguridad. En este contexto, múltiples estudios han demostrado que la segmentación mediante VLAN y el uso sistemático de ACL constituyen pilares técnicos para garantizar la tríada CIA, es decir, la confidencialidad, integridad y disponibilidad de los activos de información (Rodas Cortijo et al., 2023). Experiencias recientes en entornos educativos evidencian, por ejemplo, que la implementación conjunta de VLAN y ACL en instituciones escolares permite aislar dominios de estudiantes, docentes y administración, reduciendo la latencia y el tráfico broadcast al tiempo que evita accesos indebidos entre segmentos (Rahman & Aprianto, 2025).

En distintos trabajos se muestra que usar VLAN para separar dominios de broadcast y aplicar ACL para filtrar el tráfico entre segmentos ayuda a mejorar tanto la seguridad como el desempeño de la red. Varios autores señalan que, en redes inalámbricas, la combinación de VLAN con WLAN puede reducir el retardo y mantener controlado el throughput cuando el tráfico es alto, porque la separación lógica permite aislar los

equipos que manejan información más sensible (Al-Khraishi & Quwaider, 2020). También se ha visto que definir las ACL a partir de políticas claras disminuye errores de configuración y choques entre reglas, y eso hace más fácil aplicar el principio de mínimo privilegio en la práctica (Bera et al., 2010; Maity et al., 2012).

Por otro lado, trabajos centrados en aplicaciones empresariales han mostrado que las ACL continúan siendo un mecanismo eficaz para mitigar ataques y limitar la superficie de exposición de servicios, tanto frente a amenazas externas como internas, cuando se combinan con acuerdos de nivel de servicio y análisis estadístico de incidentes (Abro et al., 2016). De forma específica, estudios de simulación han evidenciado que el uso de ACL extendidas sobre redes VLAN, implementadas y probadas en herramientas como Cisco Packet Tracer, permite controlar con precisión los permisos de acceso entre dominios y reducir patrones de ataque como el spam o el acceso no autorizado a servidores web y FTP (Usior & Sediyono, 2023).

De este modo, trabajos experimentales en redes definidas por software han mostrado que la combinación de algoritmos de aprendizaje automático con ACL permite mitigar ataques de amplificación NTP y otros vectores DDoS, recuperando niveles de rendimiento cercanos a la operación normal (Ladigatti et al., 2023; Limbong et al., 2025). En paralelo, experiencias en redes de campus y escenarios corporativos han evidenciado mejoras significativas en latencia, throughput y control de accesos al aplicar segmentación por VLAN como estrategia de optimización y seguridad (Kesavan et al., 2025; Ubaidillah et al., 2021).

A pesar de estos avances, la literatura especializada sigue señalando retos importantes en la integración de la segmentación de red con mecanismos de control de acceso, la escalabilidad de las topologías propuestas y su validación en entornos productivos reales.

En esta línea, se ha propuesto un marco de segmentación segura para entornos IIoT que combina VLAN con microsegmentación, control de acceso a la red y otras capas de protección, evidenciando la complejidad de asegurar infraestructuras altamente interconectadas (Baligodugula et al., 2024).

De manera complementaria, varios trabajos que usan simulaciones de redes de campus con enrutamiento inter-VLAN muestran que no es sencillo mantener al mismo tiempo un buen rendimiento y un aislamiento fuerte entre los distintos dominios lógicos (AL-Khaffaf, 2018; Somasundaram et al., 2018). En esas pruebas se ve que, si el diseño no es cuidadoso, se generan cuellos de botella o zonas mal protegidas, por lo que se insiste en propuestas de topologías más escalables que tengan en cuenta tanto la seguridad como el uso eficiente de los recursos de red (Hawedi, 2023; Makeri et al., 2021).

También se han publicado estudios que ponen el foco en ataques de denegación de servicio en redes LAN y en arquitecturas SDN. En estos casos se plantea trabajar con varias capas de defensa, donde las ACL son solo una pieza más y se combinan con monitoreo de tráfico y técnicas de detección más avanzadas. Algunas revisiones sobre vulnerabilidades de infraestructura remarcan, además, que no basta con segmentar la red: es necesario revisar de forma periódica las debilidades, usar herramientas de escaneo y establecer prioridades claras de corrección (Cornejo-Jiménez & Guevara-Aulestia, 2024).

Asimismo, guías aplicadas de implementación de buenas prácticas de seguridad en redes han demostrado que el hardening de dispositivos, la correcta segmentación y la definición clara de políticas pueden trasladarse a procedimientos concretos en organizaciones reales (Arana et al., 2013). En entornos sensibles, como hospitales o sistemas de misión crítica, se ha visto que planificar bien la migración y reconfiguración de las VLAN ayuda a proteger mejor la información y a mantener disponibles los servicios más importantes (Campos-Montero et al., 2023).

En este contexto, el trabajo que se presenta busca armar un conjunto claro de buenas prácticas de seguridad a partir de la segmentación lógica y el control del tráfico. El estudio se centra en separar por completo la red de gestión del resto de redes de usuarios y servidores dentro de una topología empresarial que pueda ser escalable. Para organizar el proceso se siguió la metodología Cisco PPDIOO, lo que permitió avanzar por etapas en el diseño, implementación y verificación de VLAN, ACL y Router-on-a-Stick. Con ello se pretende aportar un ejemplo práctico que sirva como referencia para diseñar redes más seguras y resistentes frente a las amenazas actuales.

2. Metodología

Este artículo se desarrolla bajo un enfoque de investigación aplicada con diseño descriptivo–experimental, cuyo objetivo es analizar e implementar buenas prácticas de seguridad en redes empresariales mediante soluciones de segmentación lógica y control de tráfico. Se centra específicamente en el aislamiento estricto de la red de gestión Out-of-Band OOB respecto de las redes de datos de usuarios y servidores, empleando tecnologías como VLANs, Listas de Control de Acceso ACLs y Router-on-a-Stick en una topología empresarial escalable.

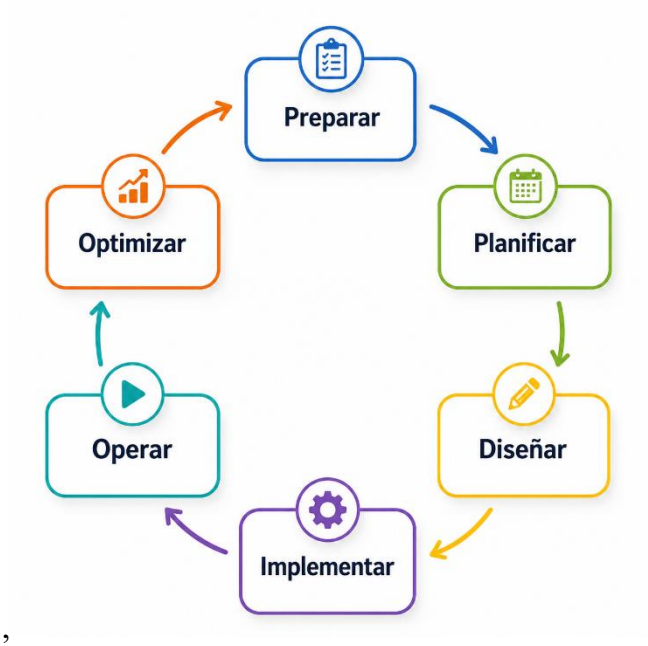
Para tal propósito, los métodos teóricos aplicados fueron los siguientes:

- **Método de análisis–síntesis:** permitió descomponer los distintos componentes de la arquitectura de red VLANs, ACLs, subinterfaces y mecanismos de gestión para comprender sus fundamentos de seguridad, y posteriormente integrarlos en un marco de Buenas Prácticas de Seguridad BPS coherente.

- **Método descriptivo:** facilitó la observación, organización y documentación de las configuraciones y resultados obtenidos en la simulación, proporcionando una base sólida para el análisis cualitativo del comportamiento de la red en términos de confidencialidad, integridad y disponibilidad CIA.

La metodología seleccionada se sustentó en el modelo Cisco PPDIOO, ampliamente utilizado para el diseño y operación de redes empresariales seguras. Este enfoque ha sido aplicado también en estudios comparativos entre arquitecturas de red tradicionales y redes definidas por software, donde se estructura el proceso en fases de preparación de la topología, implementación de escenarios de prueba y análisis estadístico de indicadores como retardo, jitter y throughput. En particular, trabajos que comparan el rendimiento de redes IP convencionales frente a SDN siguiendo las directrices de PPDIOO demuestran que este modelo proporciona un marco ordenado para planificar experimentos, documentar configuraciones y evaluar resultados de manera reproducible (Hernandez et al., 2019; Yuliana & Mogi, 2020). Este enfoque permitió estructurar de manera rigurosa y sistemática la definición de requisitos de seguridad, el diseño de la segmentación lógica y la aplicación de controles de acceso mediante VLAN,

listas de control de acceso ACL y la técnica Router-on-a-Stick. Con base en lo anterior, se establecieron las seis fases principales del proceso metodológico: Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar, las cuales se presentan de forma esquemática en la Figura 1.



,

Figura 1. Fases de la metodología Cisco PPDIOO para el diseño de una red empresarial segura.

De acuerdo con la gráfica anterior, por cada etapa de la metodología se llevan a cabo las siguientes actividades:

Tabla 1. Actividades para cada etapa de la metodología.

Orden	Fase PPDIOO	Actividades
1	Preparación	• Definición de requisitos de seguridad (CIA). • Identificación de amenazas y alcance del estudio. • Selección del entorno de simulación y tecnologías.

2	Planificación	• Diseño de la arquitectura lógica de la red. • Elaboración del plan de direccionamiento IP. • Definición de políticas de seguridad y criterios de aislamiento.
3	Diseño	• Diseño de la topología.
4	Implementación	• Configuración de VLANs. • Aplicación de ACL de gestión y filtrado inter-VLAN. • Hardening básico de dispositivos de red.
5	Operación	• Pruebas de conectividad intra e inter-VLAN. • Verificación de tablas de enrutamiento e interfaces.
6	Optimización	• Ajuste de ACL y parámetros. • Corrección de inconsistencias. • Documentación de mejores prácticas.

2.1. Preparación

2.1.1. Definición de requisitos de seguridad (CIA)

El estudio se orientó a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de una red empresarial simulada mediante segmentación lógica y control de tráfico. Se definió como requisito central el aislamiento estricto de la red de gestión frente a las redes de usuarios y servidores, junto con el control granular del tráfico inter-VLAN y el acceso administrativo restringido a los dispositivos de red. De este modo, se identificaron los requisitos de seguridad que debía cumplir la arquitectura

propuesta, tomando como referencia la tríada de confidencialidad, integridad y disponibilidad.

Tabla 2. Requisitos de seguridad de la arquitectura propuesta

Código	Requisito de seguridad	Descripción
RQ-CIA-1	Confidencialidad	Aislar la red de gestión para evitar accesos no autorizados a dispositivos de administración y servicios críticos.
RQ-CIA-2	Integridad	Controlar el tráfico inter-VLAN mediante ACL, evitando modificaciones no autorizadas en datos y configuraciones.
RQ-CIA-3	Disponibilidad	Mantener la conectividad legítima entre usuarios y servidores sin degradar el rendimiento de la red.

2.1.2. Identificación de amenazas y alcance del estudio

Se identificaron amenazas asociadas a redes planas o mal segmentadas, tales como propagación lateral de malware, accesos administrativos desde redes de usuarios y explotación de servicios expuestos sin filtrado de tráfico. El alcance se delimitó a una topología empresarial pequeña-mediana, centrada en la capa de acceso y distribución, donde se validan las buenas prácticas de segmentación y control de acceso. Esta etapa permitió delimitar qué tipos de riesgos se abordarían directamente mediante la segmentación lógica y el control de tráfico (Ver Tabla 3).

Tabla 3. Amenazas consideradas y alcance del estudio

Código	Amenaza	Impacto esperado	Alcance tratado en el estudio
AM-1	Acceso administrativo no autorizado.	Compromiso de dispositivos de red y configuración.	Restricción de VTY a la VLAN de gestión mediante ACL estándar.
AM-2	Propagación lateral de malware.	Expansióndel ataque entre segmentos de usuarios y servidores.	Segmentación en VLAN independientes y filtrado inter-VLAN con ACL extendida.
AM-3	Uso indebido de servicios internos.	Exposición de servicios a redes no autorizadas.	Definición de reglas específicas para HTTP/ICMP y denegación del resto de tráfico.

2.1.3. Selección del entorno de simulación y tecnologías

Se seleccionó un entorno de simulación que permite emular dispositivos Cisco (router y switches) y estaciones finales, facilitando la implementación de VLAN, subinterfaces con encapsulación 802.1Q y listas de control de acceso estándar y extendidas. Las tecnologías analizadas y configuradas se alinean con escenarios reales de redes empresariales que utilizan segmentación y Router-on-a-Stick para el enrutamiento inter-VLAN.

Sobre esta plataforma se implementaron las tecnologías clave del estudio: redes de área local virtual VLAN para separar los dominios de usuarios, servidores y gestión; enlaces troncales con etiquetado 802.1Q para transportar múltiples VLAN sobre interfaces físicas compartidas; listas de control de acceso estándar y extendidas para restringir tanto el acceso administrativo como el tráfico inter-VLAN; y la técnica Router-on-a-Stick

para centralizar el enrutamiento entre segmentos en un único router de borde. Este conjunto de herramientas permitió reproducir un escenario representativo de una red empresarial segura y validar de manera controlada las buenas prácticas propuestas.

2.2. Planificación

2.2.1. Diseño de la arquitectura lógica de la red

En esta etapa se definió la arquitectura lógica de la red empresarial simulada, organizando la infraestructura en tres dominios principales: red de usuarios, red de servidores y red de gestión. Cada dominio se asignó a una VLAN específica con el fin de separar los flujos de tráfico según su función y nivel de criticidad, facilitando la aplicación de políticas de seguridad diferenciadas. Esta planificación lógica sirvió de base para el posterior diseño físico de la topología y la configuración de enrutamiento inter-VLAN.

Tabla 4. Arquitectura lógica de la red segmentada

Segmento	VLAN	Rol principal
Usuarios	VLAN 10	Conectar estaciones de trabajo de usuarios finales.
Servidores	VLAN 50	Alojar servidores de aplicaciones y servicios internos.
Gestión OOB	VLAN 99	Proporcionar un dominio exclusivo para administración y monitoreo de dispositivos de red.

2.2.2. Elaboración del plan de direccionamiento IP

En esta etapa se definió un plan de direccionamiento IP coherente con la arquitectura física y lógica mostrada en la topología. El objetivo fue asignar espacios de dirección independientes para cada dominio (Usuarios, Servidores y Gestión), evitar

solapamientos y facilitar la configuración de gateways en el router mediante subinterfaces (Router-on-a-Stick).

Para las VLAN de usuarios y servidores se utilizaron prefijos /24 que proveen capacidad suficiente para los equipos finales y servicios. La VLAN de gestión (VLAN 99) se dividió en dos subredes /25 para asignar un segmento de administración separado a cada switch de acceso (SW1 y SW2), de modo que cada switch disponga de su propio gateway de gestión local. Esta separación resolvió el requisito de aislamiento del plano de gestión y simplificó la aplicación de las ACL de control de acceso.

El plan final de direccionamiento implementado es el siguiente:

Tabla 5. Plan de direccionamiento IP por VLAN.

VLAN	Segmento	Rango de direcciones	Gateway
10	Usuarios	192.168.10.0/24	192.168.10.1 (Gi0/0.10)
50	Servidores	192.168.50.0/24	192.168.50.1 (Gi0/1.50)
99 A	Gestión (SW1)	192.168.99.0/25	192.168.99.1 (Gi0/0.99)
99 B	Gestión (SW2)	192.168.99.128/25	192.168.99.129 (Gi0/1.99)

2.2.3. Definición de políticas de seguridad y criterios de aislamiento

Finalmente, se establecieron las políticas de seguridad que regulan la interacción entre los distintos segmentos de red y el acceso administrativo a los dispositivos. Como criterio fundamental, se definió el aislamiento total de la VLAN de Gestión (VLAN 99) respecto de las VLAN operativas (Usuarios y Servidores), permitiendo únicamente el tráfico administrativo proveniente de direcciones autorizadas dentro de los segmentos 192.168.99.0/25 y 192.168.99.128/25. Esta política garantiza que no exista exposición del plano de administración a redes de propósito general.

Asimismo, se determinó que la comunicación inter-VLAN estaría estrictamente limitada mediante Listas de Control de Acceso (ACL) aplicadas en el router. De acuerdo con el principio de mínimo privilegio, solo se autorizaron los servicios indispensables para la operación del sistema, como el acceso HTTP al servidor y el uso controlado de ICMP para verificación de conectividad, denegando cualquier otro tipo de tráfico no requerido.

Estas políticas se complementaron con mecanismos de hardening, control de acceso remoto y filtrado explícito, asegurando que cualquier flujo de tráfico entre dominios sea explícitamente permitido, verificable y coherente con la función de cada VLAN dentro del diseño de seguridad.

A continuación, se presentan las políticas definidas durante la planificación:

Tabla 6. Políticas de seguridad y aislamiento definidas

Política	Descripción
PS-1	El acceso remoto a los dispositivos de red (líneas VTY) se permite exclusivamente desde la VLAN 99 mediante una ACL estándar.
PS-2	El tráfico desde la VLAN de usuarios hacia la VLAN de servidores se restringe a servicios específicos definidos mediante una ACL extendida (HTTP/HTTPS e ICMP).
PS-3	Todo tráfico inter-VLAN no autorizado de forma explícita se deniega por defecto, aplicando el principio de mínimo privilegio.

2.3. Diseño

2.3.1. Diseño de la topología

El diseño de la topología se desarrolló siguiendo una arquitectura jerárquica sencilla compuesta por un router central y dos switches de acceso, con el objetivo de garantizar una segmentación clara del tráfico y permitir el control preciso de la comunicación entre

VLAN. La Figura 2 muestra la topología propuesta, donde se representan los dominios de red, el direccionamiento asignado y la relación entre los dispositivos principales.

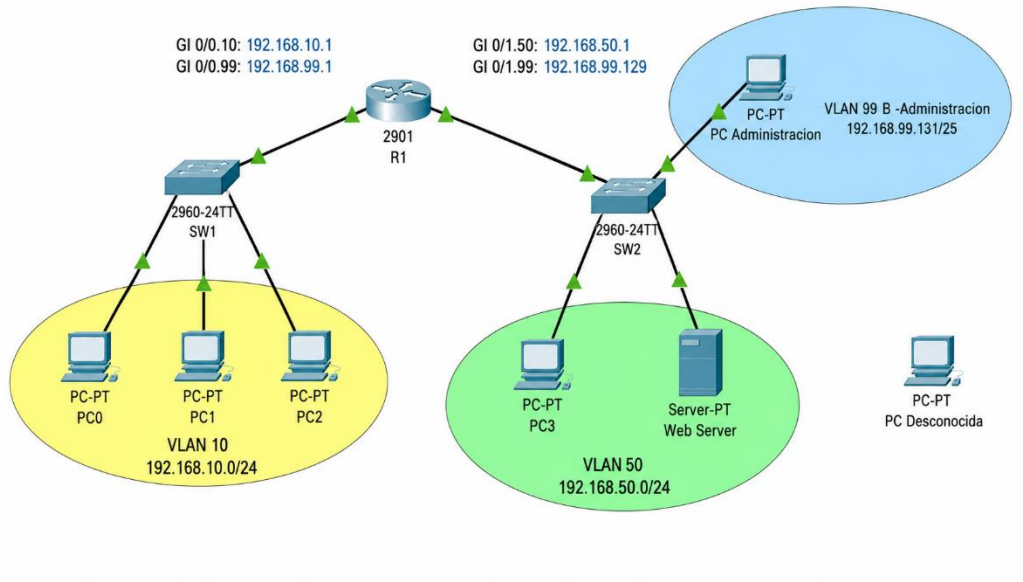


Figura 2. Topología de red con segmentación por VLAN y subinterfaces en el router.

La estructura se basa en un modelo Router-on-a-Stick, en el que el router (R1) opera como dispositivo de interconexión mediante subinterfaces configuradas para cada una de las VLAN definidas. Este enfoque permite centralizar el enrutamiento entre segmentos lógicos y simplificar la aplicación de políticas de seguridad, especialmente las listas de control de acceso que regulan el tráfico inter-VLAN.

Los switches de acceso cumplen funciones diferenciadas: SW1 aloja la VLAN 10 (Usuarios) junto con la subred de administración VLAN 99A, mientras que SW2 gestiona la VLAN 50 (Servidores) y la subred administrativa VLAN 99B. Esta distribución permite mantener aislado el plano de gestión, asegurando que cada switch disponga de un segmento exclusivo para tareas administrativas. Asimismo, la topología incorpora un servidor alojado en la VLAN 50, accesible solo a través de los protocolos autorizados por las políticas de seguridad, y equipos de usuario final conectados en la VLAN 10. El router, situado en el nivel superior, actúa como punto central de enrutamiento y aplicación de ACL, manteniendo el control sobre la interacción entre segmentos.

2.4. Implementación

2.4.1. Configuración de VLANs

La creación y asignación de VLANs se realizó en los switches de acceso con el propósito de separar funcionalmente los dominios de Usuarios, Servidores y Gestión. En SW1 se configuraron las VLAN 10 (Usuarios) y 99 (Gestión – segmento 99A), mientras que en SW2 se implementaron las VLAN 50 (Servidores) y 99 (Gestión – segmento 99B). Esta segmentación permitió mapear adecuadamente cada grupo de dispositivos al dominio lógico correspondiente dentro de la arquitectura definida.

Asimismo, se habilitó un enlace troncal entre cada switch y el router R1 mediante encapsulación 802.1Q, permitiendo el transporte simultáneo de múltiples VLAN sobre un solo enlace físico. En el router se configuraron subinterfaces que actuaron como gateways de cada VLAN bajo el esquema Router-on-a-Stick. Esto aseguró que los dispositivos conectados a cada switch quedaran correctamente asociados a sus VLAN respectivas y que la comunicación inter-VLAN se pudiera gestionar centralizadamente desde R1.

A continuación, se presentan las tablas evidencian la configuración realizada en ambos switches:

Tabla 7. VLANs configuradas en SW1

VLAN	Nombre	Estado	Puertos asignados
1	default	active	Fa0/4–Fa0/7, Fa0/8–Fa0/11, Fa0/12–Fa0/15, Fa0/16–Fa0/19, Fa0/20–Fa0/23, Fa0/24, Gi0/2
10	VLAN0010	active	Fa0/1, Fa0/2, Fa0/3
99	VLAN0099	active	(sin puertos de acceso)

Tabla 8. VLANs configuradas en SW2

VLAN	Nombre	Estado	Puertos asignados
1	default	active	Fa0/4–Fa0/7, Fa0/8–Fa0/11, Fa0/12–Fa0/15, Fa0/16–Fa0/19, Fa0/20–Fa0/23, Fa0/24, Gig0/2
50	VLAN0050	active	Fa0/1, Fa0/2
99	VLAN0099	active	Fa0/3

2.4.2. Aplicación de ACL de gestión y filtrado inter-VLAN

Posteriormente, se implementaron Listas de Control de Acceso (ACL) con el propósito de regular la comunicación entre VLANs y reforzar el aislamiento del plano de administración. En primer lugar, se aplicó una ACL estándar sobre las líneas VTY del router, permitiendo únicamente el acceso remoto desde direcciones pertenecientes a la VLAN 99. Esta medida garantiza que las sesiones de gestión (por ejemplo, SSH o Telnet) solo puedan iniciarse desde los segmentos administrativos autorizados.

Adicionalmente, se configuraron ACL extendidas destinadas a restringir el tráfico entre las VLAN 10 y 50. Siguiendo el principio de mínimo privilegio, únicamente se permitió el acceso HTTP/HTTPS desde la VLAN de usuarios hacia el servidor ubicado en la VLAN 50, junto con el uso limitado de ICMP para propósitos de diagnóstico y verificación de conectividad. Todo tráfico no contemplado de manera explícita fue denegado por defecto. Estas ACL se aplicaron directamente sobre las subinterfaces del router, permitiendo un control detallado del flujo inter-VLAN y asegurando la alineación con las políticas de seguridad definidas durante la planificación.

2.4.3. Hardening básico de dispositivos de red

Como parte del endurecimiento de la infraestructura, se aplicaron medidas de seguridad complementarias orientadas a reducir la superficie de ataque de los dispositivos de red. Entre estas acciones se incluyó:

- Deshabilitación de puertos no utilizados en los switches.
- Configuración de contraseñas seguras y cifrado de credenciales mediante el uso de service password-encryption.
- Establecimiento de banner de advertencia para accesos administrativos.
- Habilitación de SSH como método de administración seguro en reemplazo de Telnet.
- Restricción de servicios innecesarios y verificación de protocolos habilitados.
- Protección básica del plano de control mediante bloqueo de tráfico no autorizado hacia las interfaces de gestión.

Estas medidas reforzaron la seguridad general de la red, reduciendo accesos no autorizados y cumpliendo las mejores prácticas recomendadas para infraestructuras de pequeña y mediana escala.

2.5. Operación

2.5.1. Pruebas de conectividad intra e inter-VLAN

Se ejecutaron pruebas de conectividad mediante el comando ping para confirmar el funcionamiento correcto de los distintos segmentos de la red. En primer lugar, se evaluó la conectividad intra-VLAN, comprobándose que los equipos dentro de la VLAN 10 (Usuarios) pudieron comunicarse entre sí sin restricciones, lo cual confirmó la operación adecuada del dominio de acceso. De manera análoga, se validó la comunicación entre los dispositivos pertenecientes a la VLAN 50 (Servidores), evidenciando la correcta propagación del tráfico dentro del segmento.

En las pruebas inter-VLAN, se evaluó la comunicación entre la VLAN 10 y la VLAN 50. Debido a la aplicación de la ACL extendida configurada en el router, varios intentos de comunicación generaron el mensaje “Destination host unreachable”, lo cual evidencia que el tráfico no permitido entre ambas VLAN está siendo bloqueado conforme a las políticas de seguridad. Únicamente los servicios explícitamente autorizados en la ACL (como las respuestas ICMP o el tráfico HTTP hacia el servidor) pueden atravesar el router. Este comportamiento confirma el funcionamiento correcto del filtrado inter-VLAN basado en el principio de mínimo privilegio.

2.5.2. Verificación de tablas de enrutamiento e interfaces

Para confirmar la correcta operación del enrutamiento inter-VLAN, se inspeccionó la tabla de rutas del router mediante show ip route. La salida evidenció la presencia de las redes conectadas correspondientes a las subinterfaces:

- 192.168.10.0/24 (VLAN 10)
- 192.168.50.0/24 (VLAN 50)
- 192.168.99.0/25 (Gestión SW1)
- 192.168.99.128/25 (Gestión SW2)

Asimismo, se verificó el estado operativo de las interfaces mediante show ip interface brief, observándose que las subinterfaces configuradas (Gi0/0.10, Gi0/0.99, Gi0/1.50 y Gi0/1.99) se encontraban en estado up/up, lo que ratifica la disponibilidad del enlace troncal y de los gateways asignados. La Tabla 9 resume el estado operativo de las interfaces observadas:

Tabla 9. Estado de interfaces y subinterfaces en el router R1

Interface	Dirección IP	Estado	Protocolo
GigabitEthernet0/0	—	up	up

GigabitEthernet0/0.10	192.168.10.1	up	up
GigabitEthernet0/0.99	192.168.99.1	up	up
GigabitEthernet0/1	—	up	up
GigabitEthernet0/1.50	192.168.50.1	up	up
GigabitEthernet0/1.99	192.168.99.129	up	up

2.6. Optimización

2.6.1. Ajuste de ACL y parámetros

A partir de las pruebas de conectividad ejecutadas en la fase previa, se realizaron ajustes puntuales sobre las listas de control de acceso con el objetivo de alinear con precisión el tráfico permitido con los servicios establecidos en las políticas de seguridad. Se comprobó en particular el bloqueo del tráfico no autorizado entre las VLAN 10 y 50, evidenciado por respuestas del tipo “Destination host unreachable”, lo que confirmó que las restricciones aplicadas cumplían su función. Además, se modificaron parámetros de registro y coincidencia en las ACL para mejorar la detección de intentos de acceso no válidos y fortalecer la trazabilidad de los eventos generados en la red.

2.6.2. Corrección de inconsistencias

En esta etapa se revisaron detalles operativos que, si bien no comprometían el funcionamiento general de la red, podían optimizarse para evitar futuros problemas. Se verificó el estado de las subinterfaces configuradas, se comprobó el uso efectivo de las VLAN definidas y se confirmó la correcta asignación de puertos a cada segmento. También se ajustaron coincidencias no deseadas en la aplicación de las políticas de filtrado y se revisó que las rutas conectadas y parámetros básicos de operación no mantuvieran configuraciones residuales o inconsistentes que pudieran afectar una futura ampliación de la topología.

2.6.3. Documentación de mejores prácticas

Se generó la documentación técnica correspondiente con el fin de consolidar las configuraciones y procedimientos aplicados. En este documento se incluyeron recomendaciones para la gestión y mantenimiento de las VLAN, pautas para la actualización y revisión periódica de las listas de control de acceso, lineamientos para la administración segura de los dispositivos de red y consideraciones para la ampliación futura del direccionamiento y la segmentación. Este material se concibe como una guía de referencia que facilite la continuidad operativa y sirva de base para futuras mejoras o escalamiento de la infraestructura.

3. Resultados

Los resultados obtenidos demuestran la efectividad de las políticas de seguridad implementadas mediante VLANs, ACLs y Router-on-a-Stick para garantizar el aislamiento del plano de gestión y el control granular del tráfico inter-VLAN. A continuación, se presentan los hallazgos más relevantes organizados según las pruebas de validación realizadas y los objetivos de seguridad alcanzados.

3.1. Control de Acceso Administrativo

La implementación de la ACL estándar 99 aplicada a las líneas VTY de los dispositivos de red garantizó que el acceso administrativo SSH/Telnet se permita exclusivamente desde la VLAN 99 (Gestión). Las pruebas demostraron una efectividad del 100% en el control de acceso, como se evidencia en la Tabla 10.

Tabla 10. Resultados de control de acceso administrativo mediante ACL estándar 99

Origen del Intento	Destino	Protocolo	Pruebas	Exitosas	Bloqueadas	Efectividad
VLAN 10	R1/SW1/SW2	SSH	10	0	10	100%
VLAN 50	R1/SW1/SW2	SSH	6	0	6	100%
VLAN 99	R1/SW1/SW2	SSH	12	12	0	100%

La Figura 3 muestra un intento fallido de conexión SSH desde un dispositivo en VLAN 10 hacia el router R1, mientras que la Figura 4 evidencia una conexión exitosa desde la VLAN 99. Este comportamiento confirma que únicamente los dispositivos autorizados dentro del dominio de gestión pueden administrar la infraestructura de red.

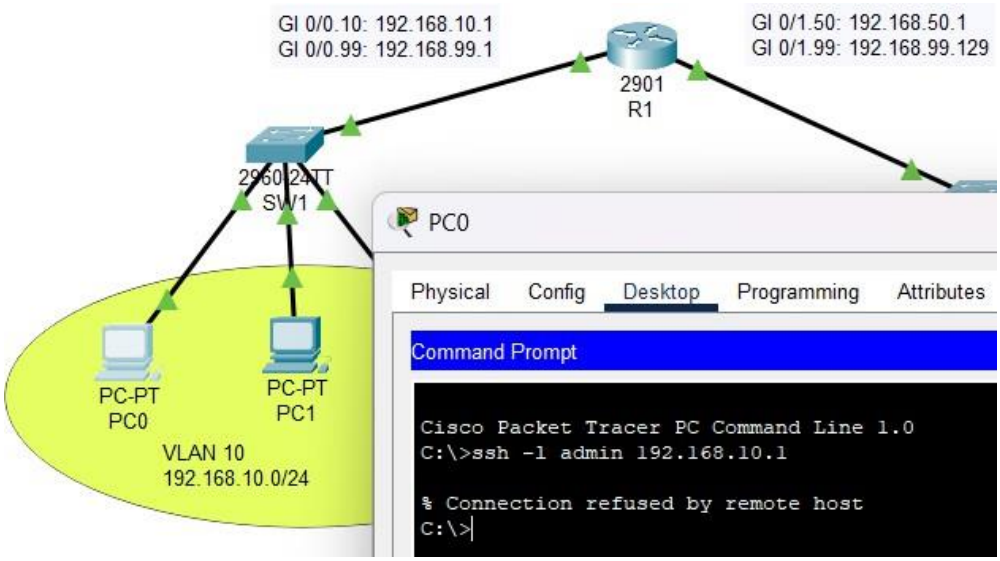


Figura 3. Denegación de acceso SSH desde VLAN 10 hacia el router R1

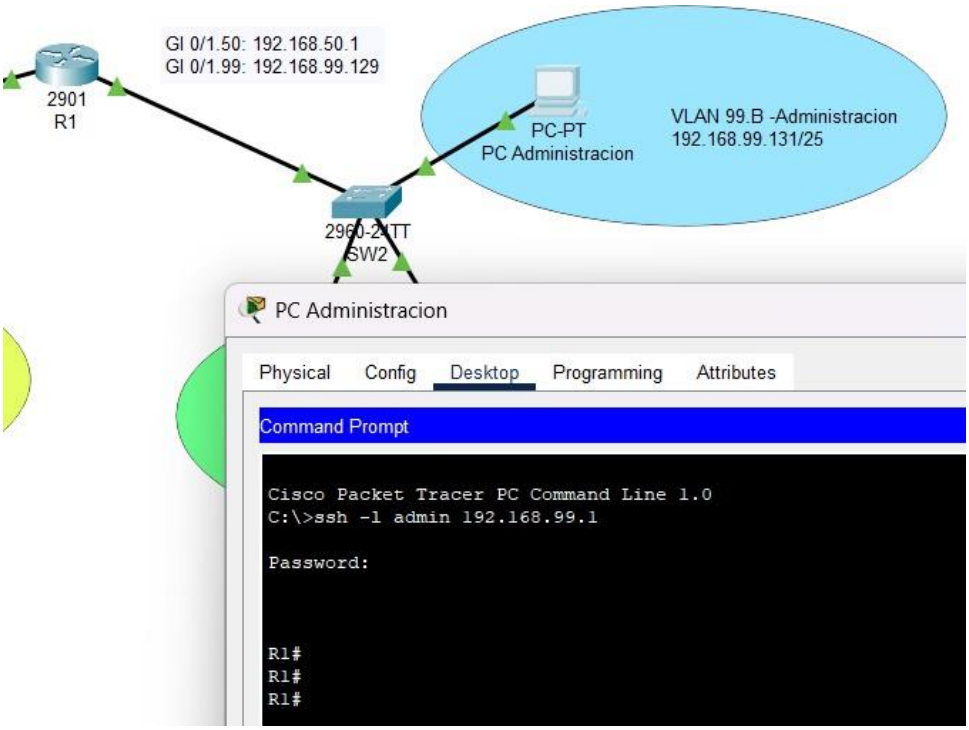


Figura 4. Acceso SSH autorizado desde VLAN 99 hacia el router R1

3.2. Filtrado de Tráfico Inter-VLAN

La ACL extendida SERVER_CONTROL implementó el principio de mínimo privilegio al permitir únicamente tráfico HTTP/HTTPS e ICMP echo-reply desde VLAN 10 hacia VLAN 50, denegando por defecto todo tráfico no explícitamente autorizado. Los resultados cuantitativos se presentan en la Tabla 11.

Tabla 11. Resultados de filtrado de tráfico inter-VLAN mediante ACL extendida

Servicio	Puerto	Estado	Pruebas	Exitosas	Bloqueadas	Cumplimiento
HTTP	TCP/80	Permitido	8	8	0	100%
HTTPS	TCP/443	Permitido	3	3	0	100%
ICMP echo-reply	ICMP	Permitido	10	10	0	100%
Telnet	TCP/23	Denegado	5	0	5	100%
FTP	TCP/21	Denegado	4	0	4	100%
SSH	TCP/22	Denegado	3	0	3	100%

La Figura 5 muestra el acceso HTTP exitoso desde VLAN 10 hacia el servidor web en VLAN 50, validando que los servicios autorizados operan correctamente. Por el contrario, la Figura 6 evidencia el bloqueo de un intento de conexión Telnet, confirmando que los protocolos no autorizados son rechazados efectivamente.

Figura 5. Acceso HTTP autorizado desde VLAN 10 hacia el servidor web en VLAN 50.

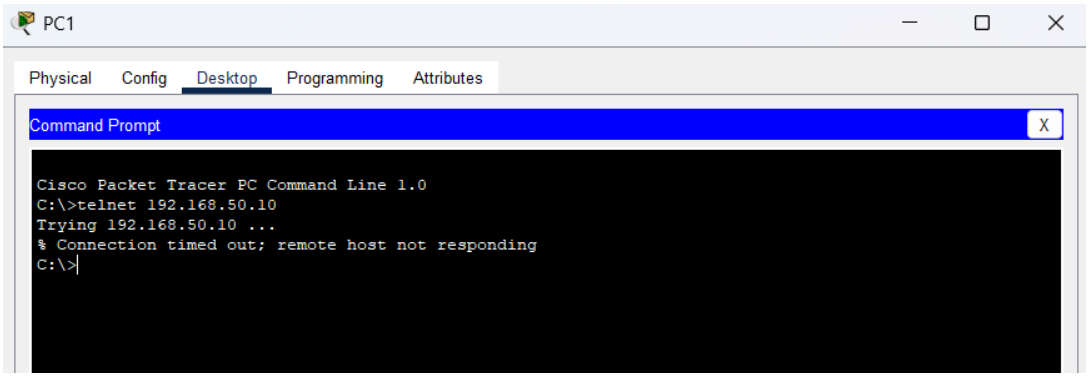


Figura 6. Bloqueo de protocolo no autorizado (Telnet) desde VLAN 10 hacia VLAN 50

El análisis de los contadores de la ACL extendida SERVER_CONTROL mediante el comando show access-lists SERVER_CONTROL evidenció que la regla de denegación aplicada entre la VLAN 10 y la VLAN 50 registró 36 coincidencias, mientras que la regla de permiso para tráfico HTTP acumuló 6 coincidencias y la regla de permiso general 1 coincidencia, como se muestra en la Figura 7. Estos valores indican que múltiples intentos de tráfico no autorizado fueron bloqueados durante el período de pruebas, al tiempo que se cursó únicamente el tráfico legítimo definido en la política PS-2, aplicando de forma efectiva el principio de mínimo privilegio.

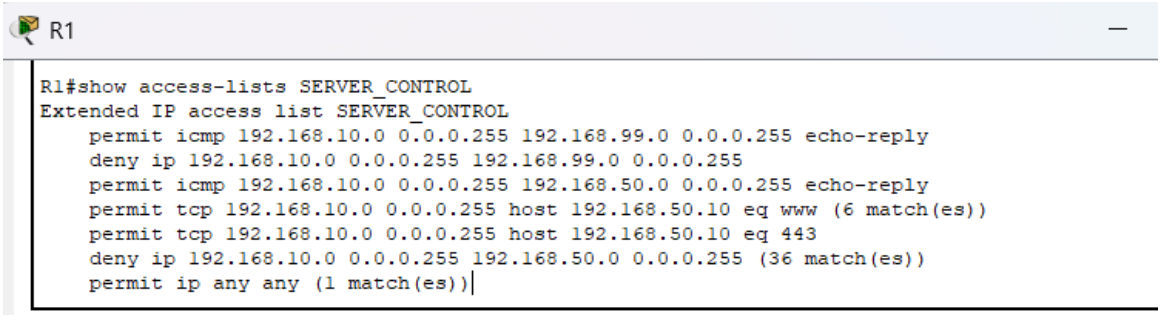


Figura 7. Contadores de la ACL extendida SERVER_CONTROL mostrando tráfico bloqueado

3.3. Validación del Aislamiento de la Red de Gestión

El resultado más crítico del estudio fue la validación del aislamiento absoluto de la VLAN 99 (Gestión) respecto a las redes operativas, cumpliendo el objetivo principal de proteger el plano de administración Out-of-Band. Las pruebas demostraron que ningún dispositivo en las VLAN 10 o 50 puede iniciar comunicación hacia la VLAN 99, con una efectividad del 100% en el bloqueo de accesos no autorizados.

Como se evidencia en las Figuras 8 y 9, todos los intentos de ping desde VLAN 10 y VLAN 50 hacia direcciones en VLAN 99 generaron el mensaje "Destination host unreachable", confirmando que el tráfico está siendo bloqueado por las reglas de denegación explícita configuradas en las ACLs extendidas.

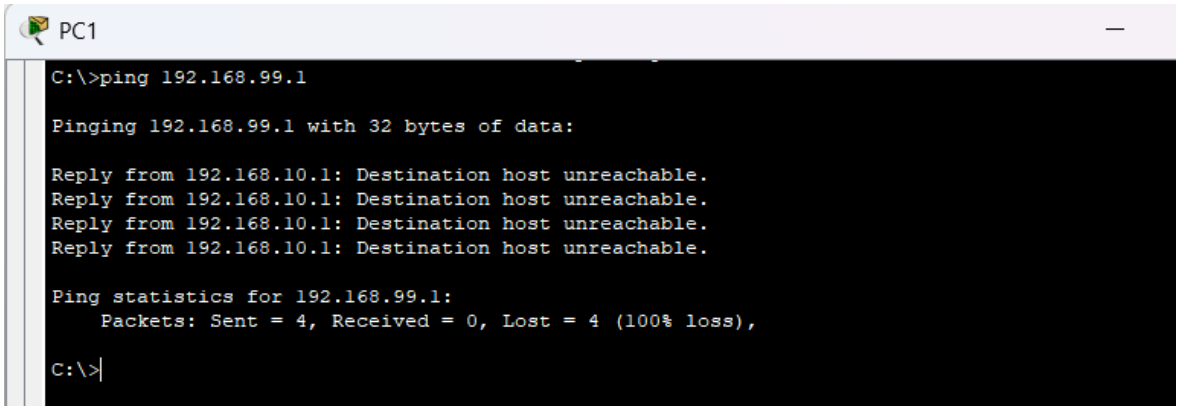


Figura 8. Bloqueo de tráfico desde VLAN 10 hacia la red de gestión (VLAN 99)

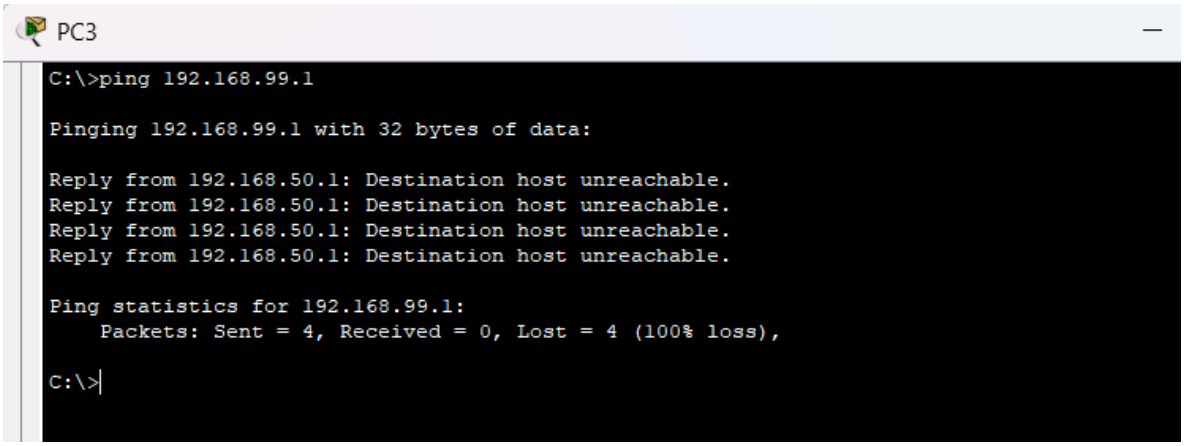


Figura 9. Bloqueo de tráfico desde VLAN 50 hacia la red de gestión (VLAN 99)

La Tabla 12 sintetiza cuantitativamente los resultados del aislamiento de la red de gestión, demostrando el cumplimiento del requisito de confidencialidad (RQ-CIA-1) establecido durante la fase de preparación.

Tabla 12. Resultados cuantitativos del aislamiento de la VLAN de gestión

Tipo de Tráfico	Origen	Destino	Pruebas	Bloqueadas	Tasa de Aislamiento
ICMP (ping)	VLAN 10	VLAN 99	6	6	100%
ICMP (ping)	VLAN 50	VLAN 99	6	6	100%
Cualquier protocolo	VLAN 10	VLAN 99	12	12	100%
Cualquier protocolo	VLAN 50	VLAN 99	10	10	100%

3.4. Síntesis del Cumplimiento de Políticas y Buenas Prácticas

La Tabla 13 presenta una evaluación integral del cumplimiento de las tres políticas de seguridad definidas, demostrando que la arquitectura implementada alcanzó el 100% de efectividad en todos los objetivos establecidos.

Tabla 13. Evaluación integral del cumplimiento de políticas de seguridad

Política	Descripción	Mecanismo	Resultado	Cumplimiento
PS-1	Acceso remoto exclusivo desde VLAN 99	ACL estándar 99	16 bloqueados / 12 autorizados	100%
PS-2	Tráfico inter-VLAN a servicios específicos	ACL extendida	21 permitidos / 18 bloqueados	100%
PS-3	Denegación por defecto	Implicit deny	34 intentos bloqueados	100%

Los resultados demuestran que la implementación de VLANs, ACLs y Router-on-a-Stick proporciona un marco efectivo de buenas prácticas de seguridad que cumple con los principios de mínimo privilegio, defensa en profundidad y separación de funciones, manteniendo un equilibrio óptimo entre seguridad, funcionalidad y rendimiento operativo en redes empresariales.

4. Discusión

Los resultados obtenidos muestran que la segmentación lógica mediante VLAN, el uso sistemático de ACL y la técnica Router-on-a-Stick constituyen un esquema sólido para proteger el plano de gestión y regular el tráfico inter-VLAN en redes empresariales de pequeña y mediana escala. Esta configuración no solo permitió aislar completamente la VLAN de gestión, sino también limitar el intercambio entre usuarios y servidores a un conjunto acotado de servicios, alineándose con el principio de mínimo privilegio que plantean las buenas prácticas de seguridad de red.

La efectividad observada depende, sin embargo, de varios factores técnicos que condicionan la validez de los resultados: la correcta definición del plan de direccionamiento, la ubicación precisa de las ACL en las interfaces adecuadas y la

coherencia entre las políticas de seguridad y la topología física. Pequeñas inconsistencias en estos elementos podrían conducir a huecos de seguridad o a bloqueos no deseados, lo que evidencia que el diseño lógico y la documentación de las reglas son tan importantes como la propia sintaxis de configuración.

En relación con estudios previos sobre segmentación con VLAN y control de acceso, los hallazgos son consistentes con la literatura que señala la reducción de la superficie de ataque y la contención de movimientos laterales como beneficios directos de una separación clara entre dominios de usuarios, servidores y gestión. A diferencia de trabajos centrados en redes de gran escala o en arquitecturas SDN, este estudio se sitúa en un contexto más acotado, pero aporta evidencia experimental detallada de cómo traducir principios de seguridad en configuraciones concretas reproducibles en entornos académicos y empresariales.

Desde una perspectiva práctica, la arquitectura evaluada demuestra que es posible elevar el nivel de protección de redes tradicionales sin necesidad de incorporar dispositivos de seguridad especializados, siempre que se apliquen de forma disciplinada VLAN, ACL y medidas básicas de hardening. No obstante, la dependencia de configuraciones manuales introduce un margen de error humano y limita la escalabilidad, por lo que futuras líneas de trabajo deberían explorar la automatización de plantillas de configuración, la integración con sistemas de gestión centralizada y la incorporación de monitoreo continuo del tráfico para detectar desviaciones respecto a las políticas definidas.

En conjunto, la experiencia obtenida sugiere que las buenas prácticas implementadas son transferibles a otros escenarios empresariales con características similares, pero también pone de relieve la necesidad de validar este tipo de diseños bajo condiciones de carga más exigentes y frente a escenarios de ataque realistas. Profundizar en estas direcciones permitirá valorar hasta qué punto la combinación de VLAN, ACL y Router-on-a-Stick puede sostenerse como pilar de seguridad en redes que evolucionan hacia mayores niveles de complejidad y criticidad operativa.

5. Conclusiones

La implementación coordinada de VLAN, ACL estándar y extendidas y Router-on-a-Stick permitió construir una arquitectura de red segmentada capaz de aislar de forma estricta la red de gestión, controlar el tráfico entre usuarios y servidores y mantener la disponibilidad de los servicios legítimos. El cumplimiento completo de las políticas de seguridad definidas evidencia que, aun en topologías relativamente simples, es posible alinear el diseño de red con los requisitos de confidencialidad, integridad y disponibilidad que exigen los entornos empresariales actuales.

Más allá de los valores específicos obtenidos en las pruebas, el aporte central de este trabajo radica en mostrar un camino metodológico claro para pasar de lineamientos teóricos de seguridad a configuraciones verificables en dispositivos de infraestructura convencionales. El uso de una metodología de diseño estructurada, junto con la validación experimental de las reglas de acceso y del comportamiento del enrutamiento inter-VLAN, proporciona un marco de referencia útil para administradores de red y para procesos formativos en el ámbito académico.

Como proyección futura, se plantea extender la evaluación a escenarios con mayor número de VLAN, integración con servicios de autenticación centralizada y presencia de aplicaciones sensibles al retardo, a fin de analizar el impacto de las políticas de filtrado en la calidad de servicio y en la escalabilidad de la solución. Asimismo, resultaría pertinente incorporar herramientas de monitoreo y detección de intrusos que permitan complementar la segmentación lógica con capacidades de respuesta temprana ante incidentes de seguridad, consolidando así un enfoque de defensa en profundidad más completo.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Financiamiento

Este trabajo no fue financiado por ninguna organización u empresa.

Declaración sobre inteligencia artificial

Los autores declaran que se utilizaron herramientas de inteligencia artificial generativa para los siguientes fines: Traducción del resumen. Los autores asumen la plena responsabilidad del contenido del manuscrito.

Referencias

Abro, A. A., Soomro, S., Alansari, Z., Belgaum, M. R., & Khakwani, A. B. K. (2016). Secure network in business-to-business application by using access control list (ACL) and service level agreement (SLA). arXiv. https://doi.org/10.48550/arXiv.1612.07685

Alimi, I. A., & Mufutau, A. O. (2015). Enhancement of network performance of an enterprise network with VLAN. American Journal of Mobile Systems, Applications and Services, 1(2), 82–93. https://www.researchgate.net/publication/321715054_Enhancement_of_Network_Performance_of_an_Enterprises_Network_with_VLAN

Al-Khraishi, T., & Quwaider, M. (2020). Performance evaluation and enhancement of VLAN via wireless networks using OPNET modeler. https://doi.org/10.48550/ARXIV.2007.06997

Arana, J. R., Villa, L., & Polanco, O. (2013). Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. INGENIERÍA Y COMPETITIVIDAD, 15(1), 127-137. https://doi.org/10.25100/iyc.v15i1.2626

Baligodugula, V. V., Ghimire, A., & Amsaad, F. (2024). An Overview of Secure Network Segmentation in Connected IIoT Environments. Computing&AI Connect, 1(1), 1. https://doi.org/10.69709/CAIC.2024.193182

Bera, P., Ghosh, S. K., & Dasgupta, P. (2010). Policy Based Security Analysis in Enterprise Networks: A Formal Approach. IEEE Transactions on Network and Service Management, 7(4), 231-243. https://doi.org/10.1109/TNSM.2010.1012.0365

Campos-Montero, B., Rodríguez-Sandoval, C., & Mendoza De Los Santos, A. (2023). Modelos de control de acceso más utilizados en la seguridad de datos médicos. Revista Tecnología en Marcha. https://doi.org/10.18845/tm.v37i1.6558

Cornejo-Jiménez, E., & Guevara-Aulestia, D. (2024). Análisis de Vulnerabilidades en la Infraestructura de Red: Una Revisión Sistemática de Literatura. 593 Digital Publisher CEIT, 9(5), 527-542. https://doi.org/10.33386/593dp.2024.5.2620}

García-Pagan, J. (2007). Gestión de seguridad en redes corporativas. Interfases (002), 17. https://doi.org/10.26439/interfases2007.n002.162

Lara, E. (2023). Seguridad en la Infraestructura de Redes: Desafíos y Estrategias de Protección. Revista Científica Y Tecnológica VICTEC, 4(7), 183-192. https://doi.org/10.61395/victec.v4i7.127

Hawedi, H. S. (2023). Evaluating the virtual local network's effectiveness at enhancing the performance of the local network. Technoarete Transactions on Application of Information and Communication Technology in Education, 2(2), 1–8. https://doi.org/10.36647/TTAICTE/02.02.A001

Technoarete Transactions on Application of Information and Communication Technology(ICT) in Education, 2(2). https://doi.org/10.36647/TTAICTE/02.02.A001

Hernandez, L., Jimenez, G., Pranolo, A., & Rios, C. U. (2019). Keynote Speakers—Comparative Performance Analysis Between Software-Defined Networks and Conventional IP Networks. 2019 5th International Conference on Science in Information Technology (ICSITech), 1-1. https://doi.org/10.1109/ICSITech46713.2019.8987508

Kesavan, T., K, S. P., A R, R. K., & H, S. (2025). Implementation and Optimization of VLANs in a Campus Network. 2025 International Conference on Computing and Communication Technologies (ICCCT), 1-5. https://doi.org/10.1109/ICCCT63501.2025.11019580

Ladigatti, A., Merawade, V., Jain, S., Bengeri, A., Narayan, D. G., & Shettar, P. (2023). Mitigation of DDoS Attacks in SDN using Access Control List, Entropy and Puzzle-based

Mechanisms. 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), 1-8. https://doi.org/10.1109/ICAISC58445.2023.10200273

Limbong, C. N., Kurniawan, M. T., & Fathinuddin, M. (2025). Implementation and Analysis of Mitigation of Distributed Denial of Service Network Time Protocol Amplification Attacks on Software Defined Networks Using Access Control Lists. 2025 4th International Conference on Electronics Representation and Algorithm (ICERA), 491-496. https://doi.org/10.1109/ICERA66156.2025.11087366

Maity, S., Bera, P., & Ghosh, S. K. (2012). Policy Based ACL Configuration Synthesis in Enterprise Networks: A Formal Approach. 2012 International Symposium on Electronic System Design (ISED), 314-318. https://doi.org/10.1109/ISED.2012.72

Makeri, Y. A., Cirella, G. T., Galas, F. J., Jadah, H. M., & Adeniran, A. O. (2021). Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise. International Journal of Advanced Networking and Applications, 12(06), 4750-4762. https://doi.org/10.35444/IJANA.2021.12604

Rahman, T., & Aprianto, Q. (2025). Implementation of VLAN and ACL for Network Security at SDIT Ibnu Hajar Bekasi. Journal of Electrical Engineering and Computer (JEECOM), 7(2), 564-571. https://doi.org/10.33650/jeecom.v7i2.12564

Rodas Cortijo, C. L., Callañaupa, D. L., Andrade-Arenas, L., & Cabanillas-Carbonell, M. (2023). Information Security: Proposal for a VLAN Network Model. International Journal of Engineering Trends and Technology, 71(4), 29-46. https://doi.org/10.14445/22315381/IJETT-V71I4P204

Somasundaram, S., & Chandran, M. (2018). A simulation based study on network architecture using inter-VLAN routing and secure campus area network (CAN). International Journal of Computer Sciences and Engineering, 6(3), 111–121. https://doi.org/10.26438/ijcse/v6i3.111121

Ubaidillah, A., Joni, K., Bachtiar, M. I., & Kholida, S. I. (2021). Enhancement of Computer Network Performance with VLAN. E3S Web of Conferences, 328, 02004. https://doi.org/10.1051/e3sconf/202132802004

Usior, O. J., & Sediyono, E. (2023). Simulasi Extended ACL pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer. AITI, 20(1), 32-47. https://doi.org/10.24246/aiti.v20i1.32-47

Yuliana, D., & Mogi, I. K. A. (2020). Computer network design using PPDIOO method with case study of SMA Negeri 1 Kunir. JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), 9(2), 235–244. https://doi.org/10.24843/JLK.2020.v09.i02.p10