PLAN	☐
DOCUMENTO	☐
MANUAL	☐
INSTRUCTIVO	☒
PROCEDIMIEN	☐
REGLAMENTO	☐
ARTÍCULO	☐

INSTRUCTIVO PARA LA ELABORACIÓN DE PERFIL DE PROYECTO DE GRADO

PERFIL DEL PROYECTO DE TITULACIÓN

QUITO - ECUADOR

2025

PERFIL DEL PROYECTO DE TITULACIÓN

.

CARRERA:

TECNOLOGÍA SUPERIOR EN ELECTRÓNICA

TEMA:

IMPLEMENTACIÓN DE LISTAS DE CONTROL DE ACCESO (ACLS) EXTENDIDAS PARA LA GESTIÓN DE TRÁFICO IPV4 Y LA SEGMENTACIÓN SEGURA ENTRE VLANS EN ENTORNOS DE RED CISCO

AUTORES:

CAIZA BARRAGÁN JOSÉ ANDRÉS

NARANJO BRITO JONATHAN STALIN

TUTOR:

BOHÓRQUEZ PÉREZ MARÍA GABRIELA

FECHA:

04 - SEPTIEMBRE - 2025

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. EL PROBLEMA DE INVESTIGACIÓN

1.1.Formulación y planteamiento del Problema

El creciente número de dispositivos conectados a las redes y la adopción generalizada de VLANs para segmentar el tráfico plantean nuevos desafíos de seguridad y gestión. La ausencia o la configuración incorrecta de Listas de Control de Acceso (ACLs) extendidas para IPv4 puede permitir movimientos laterales no autorizados entre segmentos, generar saturación de enlaces por tráfico no filtrado y dejar expuestos servicios y protocolos críticos , lo que incrementa el riesgo de accesos indebidos y afectaciones al rendimiento.

En este contexto, surge la necesidad de definir y aplicar políticas de control de tráfico específicas que restrinjan las comunicaciones inter-VLAN sin impedir las funciones de gestión y diagnóstico necesarias. Por tanto, el problema central de este trabajo es determinar si la implementación de ACLs extendidas IPv4, aplicadas en un diseño router-on-a-stick con siete VLANs, permite garantizar un aislamiento efectivo entre segmentos y mitigar accesos no autorizados sin degradar de forma significativa la latencia y el rendimiento de la red.

Para abordar este problema, se diseña y aplica unas políticas de control que permite tráfico dirigido y, autoriza exclusivamente el flujo o deniega otros intercambios no autorizados entre las VLANs involucradas. La solución se valida en dos fases: simulación y replicación en hardware real para comparar resultados y evaluar el impacto operativo. Con ello, se busca entregar un procedimiento replicable que asegure el aislamiento entre VLANs, prevenga accesos no autorizados y preserve la confidencialidad y disponibilidad de los sistemas de la red.

1.2. Objetivos

1.2.1. Objetivos general

Implementar listas de control de acceso extendidas (ACLs) , en redes basadas en el protocolo IPv4, con el fin de gestionar eficientemente el tráfico de datos y restringir el acceso no autorizado entre VLANs, garantizando la seguridad, segmentación y continuidad operativa de la red sin afectar su rendimiento de la infraestructura de la red.

1.2.2. Objetivos específicos

- Analizar los fundamentos teóricos y técnicos del protocolo IPv4 y las listas de control de acceso (ACLs) extendidas en redes segmentadas mediante VLANs, implementadas en equipos de red Cisco, con el fin de identificar su impacto en la seguridad, el control del tráfico y la eficiencia en el diseño de infraestructuras de red.

- Diseñar una topología de red que integre múltiples VLANs donde se gestione con un dispositivo de capa 3, con el propósito de aplicar listas de control de acceso (ACLs) extendidas que permitan establecer políticas de filtrado orientadas a regular el tráfico inter-VLAN conforme a criterios de seguridad y eficiencia operativa.

- Evaluar el impacto de la implementación de listas de control de acceso (ACLs) extendidas en redes segmentadas mediante VLANs bajo protocolo IPv4, analizando su efecto sobre la seguridad, la segmentación del tráfico y el rendimiento de la red, a través de simulación o entornos de prueba controlados.

1.3. Justificación de la propuesta tecnológica

En el contexto de las arquitecturas de red modernas donde el número de dispositivos y servicios conectados crece de forma acelerada la segmentación mediante VLANs y el control granular del tráfico se han convertido en prácticas indispensables para mantener la seguridad y la disponibilidad. La implementación de Listas de Control de Acceso (ACLs) extendidas para IPv4 constituye un mecanismo fundamental para controlar comunicaciones inter-VLAN, limitar movimientos laterales no autorizados y proteger servicios críticos sin afectar la operatividad de la red. Las ACLs extendidas permiten definir políticas precisas (por dirección origen/destino, protocolo, puerto y tipo de ICMPv4) que mitiguen amenazas de intrusión de terceros a la red y optimicen el consumo de recursos de los enlaces.

Este estudio utiliza Cisco Packet Tracer como laboratorio de diseño para una topología router-on-a-stick con siete VLANs, donde se aplican ACLs extendidas (nombradas o numeradas) sobre las subinterfaces del router y, cuando procede, en los límites de la red. Adicionalmente, se incorporan buenas prácticas de administración: autenticación de acceso administrativo, acceso remoto seguro (SSH), segregación de la gestión en una VLAN dedicada y políticas de contraseñas seguras. La validación incluye mediciones de latencia, rendimiento y pruebas funcionales (ping, traceroute, escaneo de puertos), y se replica la configuración en hardware real para evaluar su impacto operativo.

La pertinencia de la investigación reside en ofrecer un procedimiento técnico y replicable que apoye a administradores y personal académico en la implementación eficaz de ACLs extendidas IPv4, proporcionando un punto de partida sólido para proteger entornos académicos y PYMEs y facilitar posteriores ampliaciones en entornos corporativos.

1.4. Alcance

Este proyecto abarca la implementación y validación de Listas de Control de Acceso (ACLs) extendidas sobre IPv4 en una red segmentada mediante VLANs, con el propósito de limitar, de forma precisa y eficiente, el tráfico entre dominios lógicos. Se incluyen la selección, instalación y configuración de un router Cisco 1921 y el switch Catalyst 3560 v2 compatibles con IPv4, capaces de soportar políticas de filtrado avanzadas. La topología será desplegada tanto en Cisco Packet Tracer como en un entorno de laboratorio físico, replicando las condiciones de una infraestructura real para garantizar la reproducibilidad de resultados.

Los dispositivos y la arquitectura propuesta cumplen los siguientes requisitos esenciales:

- Soporte explícito para IPv4 y sintaxis de ACLs extendidas (wildcard masks, posibilidad de ip prefix-list u objetos según versión IOS).
- Gestión segura por SSH y políticas administrativas reforzadas mediante contraseñas y ACLs de control de acceso a la capa de gestión.

Adicionalmente, el proyecto contempla la elaboración de una guía práctica que cubre:

- **Aplicación en interfaces:** configuración de ACLs extendidas en subinterfaces dot1Q del router para segmentar el tráfico inter-VLAN.
- **Validación y pruebas:** ejecución de escenarios de conectividad (ping, traceroute), pruebas de rendimiento (throughput) y escaneo de puertos IPv4, tanto en simulación como en hardware real, para asegurar el correcto funcionamiento de las políticas de filtrado sin degradar la calidad del servicio.

1.5.Métodos de investigación

Para el desarrollo de esta investigación se empleó una metodología basada en el enfoque experimental y descriptivo, orientada a la implementación y evaluación de listas de control de acceso (ACLs) extendidas en entornos IPv4. Inicialmente, se realizó una revisión bibliográfica exhaustiva sobre los fundamentos teóricos del protocolo IPv4, ACLs extendidas y segmentación mediante VLANs, con el propósito de establecer una base conceptual sólida.

- **Método Experimental:** Se intervendrá activamente el entorno de red del laboratorio para implementar las ACLs diseñadas. Se manipularán variables (reglas de la ACL) para observar y medir su efecto en el comportamiento de la red (conectividad, tráfico permitido/denegado).
- **Método Analítico-Descriptivo:** Se analizará en detalle la topología de red actual, las tablas de enrutamiento y los flujos de tráfico. Se describirán los procedimientos de configuración y los resultados obtenidos de manera sistemática y detallada.
- **Método de Simulación:** Previo a la implementación en equipos físicos, se utilizará software de simulación (como Cisco Packet Tracer o GNS3) para modelar el diseño de las ACLs, validar la lógica de las reglas y prever posibles conflictos.
- **Método de Pruebas y Validación:** Se ejecutarán pruebas de conectividad (ping, telnet, tracert) y uso de herramientas de análisis (como comandos show access-lists, debug ip packet) para verificar el correcto funcionamiento de cada ACL implementada, comparando los resultados con el comportamiento esperado.

1.5. Marco Teórico

1.5.1. Listas de Control de Acceso (ACLs)

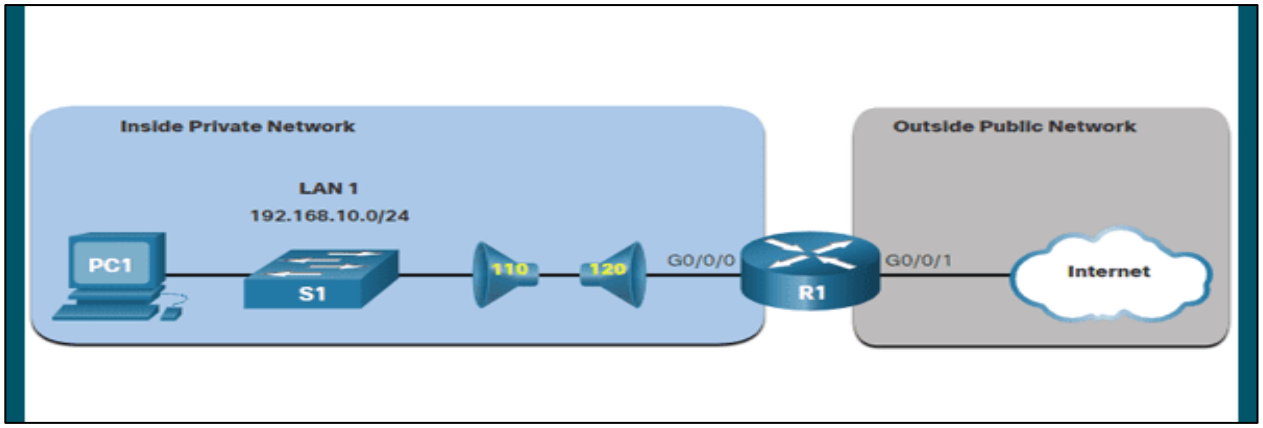
Las ACLs son una secuencia ordenada de reglas de permitir (permit) o denegar (deny) que se utilizan para filtrar el tráfico de red basado en criterios como direcciones IP de origen/destino, protocolos y números de puerto. Las ACLs estándar filtran solo basado en la dirección IP de origen, mientras que las ACLs extendidas, objeto de este proyecto, permiten un filtrado mucho más granular basado en dirección IP de origen y destino, protocolo (IP, TCP, UDP, ICMP) y puerto de destino/origen. Se aplican en interfaces de router para controlar el tráfico entrante (in) o saliente (out).

Principios clave a considerar:

- El orden de las entradas en la ACL es significativo ya que se evalúan de arriba hacia abajo y la primera coincidencia aplica.
- Existe un implicit deny (deny ip any any) al final de cada ACL si no se especifica lo contrario, por lo que se deben listar primero las sentencias permit necesarias.
- La ubicación de la ACL (placement) debe orientarse a aplicarla lo más cerca posible de la fuente del tráfico indeseado para optimizar el uso de recursos de red (Cisco Systems, 2019).
- Las ACLs en IPv4 también requieren una documentación clara y un mantenimiento periódico, ya que las redes evolucionan constantemente y las políticas de filtrado deben adaptarse a nuevas aplicaciones, servicios y amenazas emergentes (Cisco Systems, 2019).

Figura 1

Esquema de funcionamiento de una ACL extendida.



Nota: El diseño de este ejemplo muestra que el ACL 110, que fue configurado previamente, filtrará el tráfico de la red privada interna.

1.5.2. Protocolo de Internet versión 4 (IPv4)

IPv4 es la versión ampliamente utilizada del protocolo de Internet que utiliza direcciones de 32 bits para identificar dispositivos en una red.

Figura 2

Estructura de un paquete IPv4

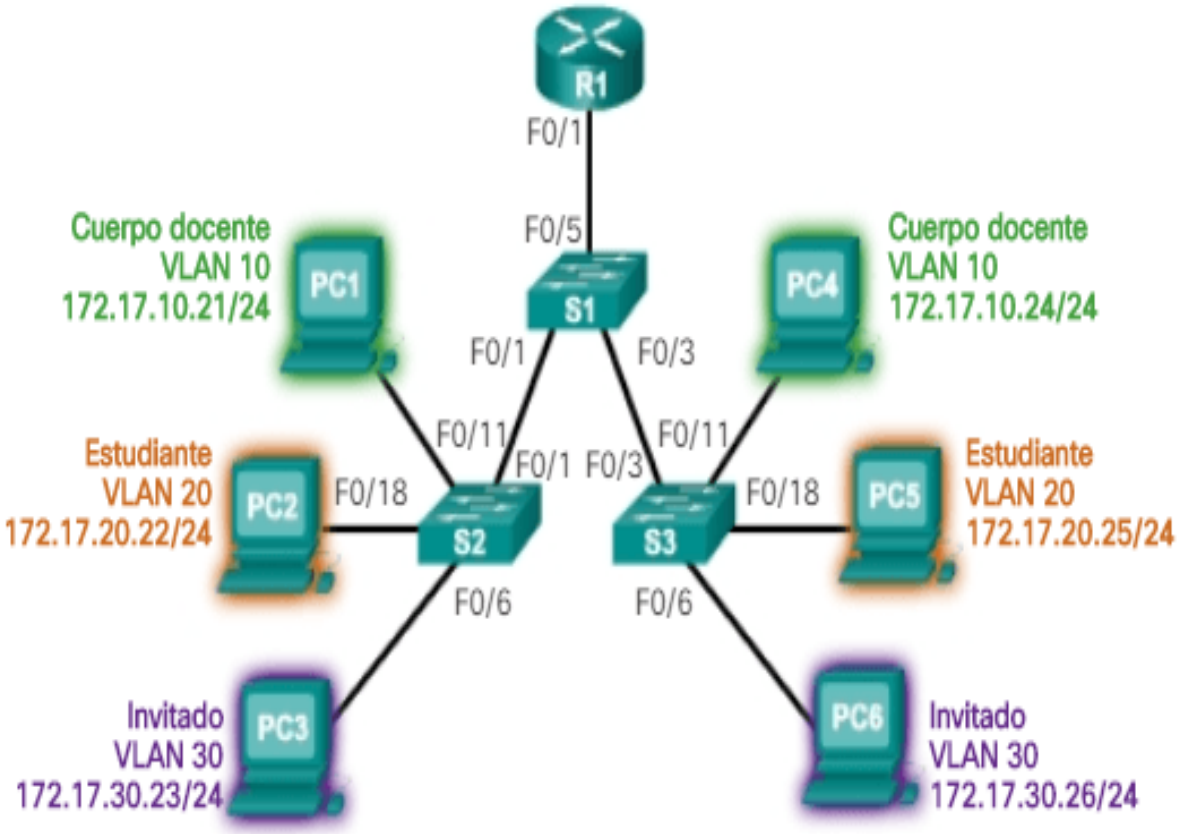
Nota. Estos campos tienen números binarios que examina el proceso de capa 3.

1.5.3. Redes de Área Local Virtuales (VLANs)

Una VLAN es una subred lógica que agrupa dispositivos basado en criterios funcionales o departamentales, aunque o estén conectados al mismo switch físico. El tráfico entre diferentes VLANs requiere ser enrutado (routing). Las ACLs son cruciales para aplicar políticas de seguridad en los puntos de enrutamiento entre VLANs, controlando qué tráfico puede pasar de una VLAN a otra. (Lammle, 2016)

Figura 2

Esquema de segmentación con VLANs y punto de aplicación de ACLs en el router.



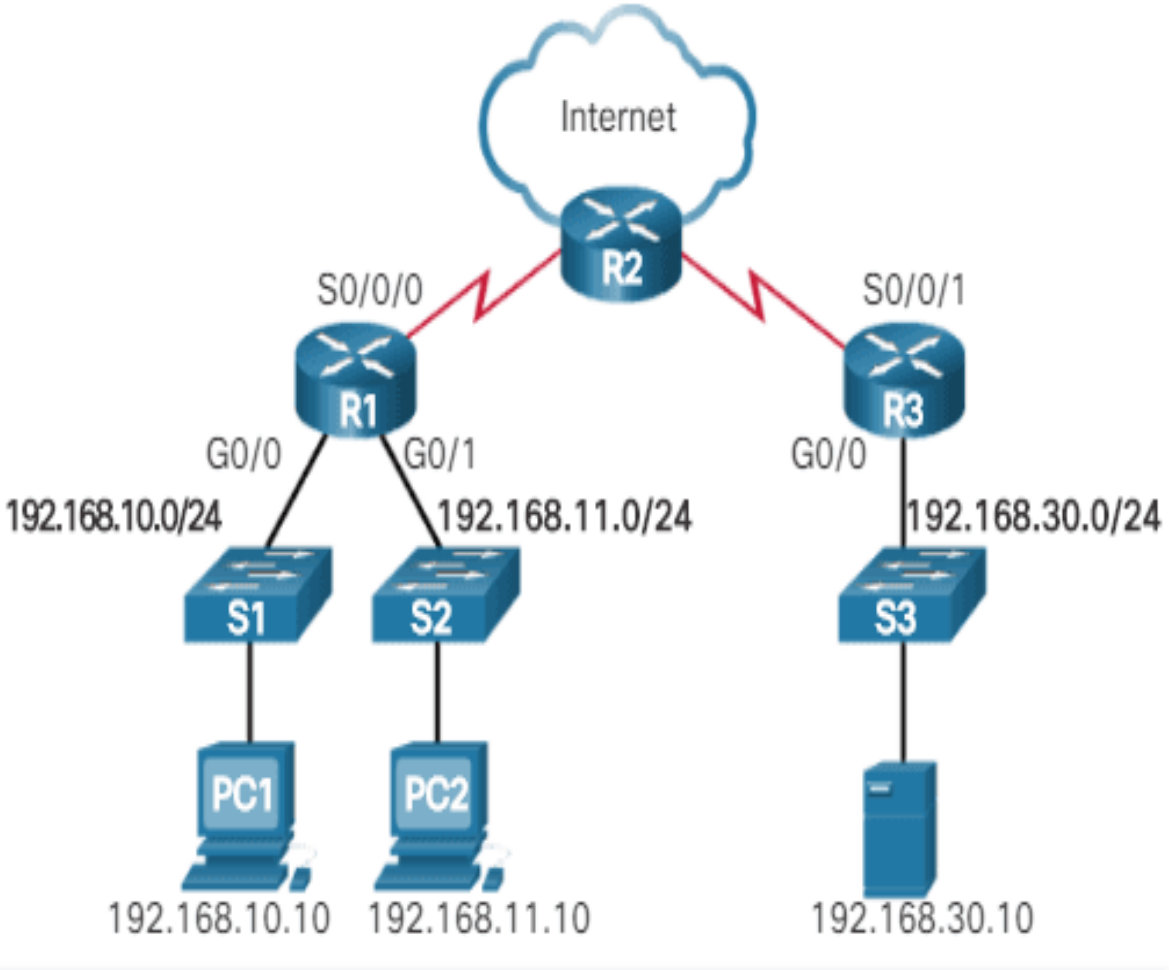
Notas. Las redes VLAN facilitan el diseño de una red para dar soporte a los objetivos de una organización.

1.5.4. Entornos de Red Cisco

Cisco Systems es un líder global en networking. Su sistema operativo Cisco IOS (Internetwork Operating System) es utilizado en la mayoría de sus routers y switches. La sintaxis para configurar ACLs en IOS es específica y robusta, siendo un estándar de aprendizaje y operación en la industria. (Odom, 2016)

Figura 3

configuración d ACL extendida en Cisco ios.



Nota. Ejemplo: de configuración d ACL extendida en Cisco.

2. ASPECTOS ADMINISTRATIVOS

2.1.Recursos humanos

- Jonathan Stalin Naranjo Brito
- Andrés José Caiza Barragán
- Gabriela María Bohórquez Pérez (Tutor)

2.2.Recursos técnicos y materiales

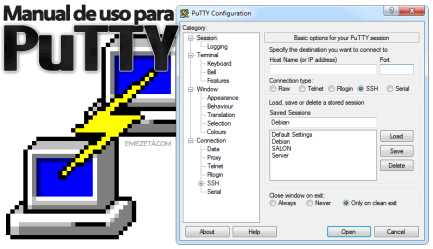
- Tabla de materiales

Table 1

Materiales

EQUIPO	MARCA	GRAFICO
SWITCH	CISCO Catalyst 2960	
ROUTER	CISCO ISR 4321	

COMPUTADORAS	INS	
CABLE CONSOLA	Linoya AWM 2835	
CABLE UTP	Panduit CAT6A	
CONECTORES	RJ45 CAT6	

RACK	BEAUCOUP 4	
PDU	Regleta Multitoma	
PuTTY	0.83 for Windows	

Nota. La implementación física de la propuesta tecnológica se llevó a cabo utilizando equipos que ya se encontraban disponibles en el instituto, debido a que los dispositivos recientemente adquiridos aún no habían llegado. Estos equipos estaban previamente montados en un rack pequeño de tipo movible, lo que facilitó tanto la organización como la movilidad del conjunto durante las fases de configuración y pruebas. Asimismo, el rack contaba con una PDU integrada, que permitió la conexión directa, ordenada y segura de los dispositivos de red empleados, garantizando un suministro eléctrico estable y reduciendo riesgos asociados a sobrecargas o conexiones improvisadas. Esta disposición aseguró que el trabajo realizado fuera plenamente funcional y práctico, a la vez que sirvió como base para validar en condiciones reales.

Table 2

Recursos técnicos.

RECURSOS	TIEMPO
PCs	6 días
Cable utp cat6	6 días
Router	6 días
Switch	6 días

Nota. El tiempo que se usó los equipos del ISUCT.

2.3.Viabilidad

2.3.1. Financiera

El proyecto es altamente viable financieramente. La inversión requerida es mínima $600 para cables de conexión, router y switch, ya que se utilizará la infraestructura de hardware y software ya disponible en el laboratorio de la carrera. Esto requiere la adquisición de equipos costosos, software adicional. Los costos son asumibles por los estudiantes y no representan una barrera para la ejecución del proyecto.

Table 3

Equipos y costos estimados.

N.º	Equipo / Material	Cantidad	Costo Und. (USD)	Costo Total (USD)	Uso principal
1	Router Cisco ISR 4321	1	1,500.00	1,500.00	Implementación de ACLs extendidas y enrutamiento IPv4.
2	Switch Cisco Catalyst 2960	1	600.00	600.00	Segmentación de VLANs y configuración de políticas de acceso.
3	Computadora portátil / PC de gestión	1	0.00	0.00	Configuración, monitoreo y administración de los dispositivos.
4	Cableado Ethernet categoría 6 (patch)	5	0.00	0.00	Conexión de equipos para pruebas y tráfico de red.
5	Conectores RJ-45	20	0.00	0.00	Ensamblaje de cables de red.
6	Software de simulación (Cisco Packet Tracer)	1	0.00	0.00	Simulación previa y validación de configuraciones.
	Total estimado	—	—	**2,100.00**	—

Nota. Tabla de costos de los equipos utilizados para la práctica de la tesis.

2.3.2. Operativa

El proyecto es operativamente viable, dado que se cuenta con los recursos humanos, técnicos y logísticos necesarios para su ejecución. Los estudiantes involucrados poseen conocimientos previos en redes Cisco adquiridos durante su formación académica, lo que facilita el manejo adecuado de dispositivos de red como el router Cisco ISR 4321 y el switch Cisco Catalyst 2960. Además, el laboratorio académico dispone de horarios establecidos para el desarrollo de proyectos de titulación, asegurando el acceso al equipamiento sin interferir con las actividades regulares.

El tutor asignado posee experiencia en la configuración, gestión y administración de redes Cisco, lo cual garantiza un acompañamiento técnico especializado durante todo el proceso. Las actividades de configuración, aplicación de listas de control de acceso (ACLs) extendidas y pruebas de segmentación de VLANs se planificarán en horarios extracurriculares, respetando la programación de clases. Asimismo, se implementarán procedimientos estandarizados para restablecer la configuración original de los dispositivos tras cada sesión de pruebas, preservando así la integridad del entorno de red para otros usuarios.

A continuación, se detallan los aspectos metodológicos que conforman la operatividad del proyecto:

La viabilidad operativa se observa a través del desarrollo de las actividades planificadas dentro del laboratorio de redes, la utilización efectiva de los dispositivos Cisco (router ISR 4321 y switch Catalyst 2960), la correcta implementación de ACLs extendidas en entornos IPv4 y la segmentación exitosa de VLANs.

Además, se constata mediante la participación de los estudiantes en las configuraciones, las pruebas de conectividad y el monitoreo del tráfico de red. La medición se realiza a través de la ejecución de tareas específicas que evidencien el cumplimiento de los objetivos operativos.

Entre estas se incluyen la cantidad de sesiones de configuración realizadas, el porcentaje de éxito en las pruebas de conectividad, el número de políticas de acceso implementadas correctamente y la verificación del aislamiento entre VLANs. Estos resultados se compararán con los objetivos planteados en el proyecto para determinar el grado de efectividad operativa.

Table 4

Indicadores o dimensiones.

Dimensión	**Indicador**	**Descripción**
Planificación operativa	Cumplimiento del cronograma	Porcentaje de actividades ejecutadas en los tiempos establecidos
Implementación técnica	Configuración de ACLs extendidas	Número de políticas de control de tráfico configuradas y aplicadas correctamente
Eficiencia del entorno de pruebas	Conectividad y segmentación	Porcentaje de pruebas exitosas que validan la segmentación entre VLANs
Mantenimiento del entorno	Restauración de configuraciones	Frecuencia con la que se devuelve el equipo a su estado inicial sin errores

Nota. La tabla presenta las dimensiones, indicadores y descripciones empleadas para evaluar la operatividad del proyecto. Cada indicador permite medir el grado de cumplimiento de las actividades planificadas, la correcta implementación de listas de control de acceso (ACLs) extendidas, el nivel de segmentación del tráfico entre VLANs y la efectividad en la restauración del entorno de red, garantizando así el adecuado desarrollo del proyecto en entornos Cisco.

Para la recolección de datos, se emplearán listas de verificación (checklists) y registros de observación directa elaborados específicamente para documentar cada fase del proyecto. Estos instrumentos permitirán registrar las actividades de configuración realizadas, el cumplimiento de objetivos operativos, los resultados de las pruebas de conectividad y la correcta aplicación de las ACLs extendidas. Adicionalmente, se elaborarán practicas al finalizar cada sesión de laboratorio, los cuales servirán como evidencia del progreso y efectividad del proyecto.

Con esta metodología operativa, se asegura que el proyecto sea ejecutado de manera ordenada, eficiente y dentro de las condiciones necesarias para garantizar resultados válidos, replicables y alineados con los objetivos de investigación.

2.3.3. Técnico

El proyecto es técnicamente viable. La tecnología de ACLs extendidas es madura, estable y está ampliamente documentada tanto en la literatura especializada como en los recursos oficiales de Cisco. Los equipos adquiridos para realizar el proyecto de tesis (routers serie ISR 4321 y switches Catalyst 2960 24) tienen plena capacidad y las características de software (Cisco IOS con IP Base o superior) necesarias para soportar las funcionalidades requeridas de ACLs extendidas y enrutamiento inter-VLAN. Para la tesis se tiene acceso al software de simulación Cisco Packet Tracer necesario para la simulación y prueba preliminar de las configuraciones, lo que minimiza riesgos durante la implementación en equipos físicos. La naturaleza del proyecto permite una implementación por fases, facilitando la detección y corrección de errores.

2.3.4. Recursos técnicos disponibles

El proyecto contará con recursos tecnológicos adecuados para su desarrollo. Entre los equipos físicos se dispone de routers Cisco ISR 4321 y switches Catalyst 2960 de 24 puertos, los cuales cumplen con los requerimientos técnicos para la implementación de Listas de Control de Acceso (ACLs) extendidas y el enrutamiento inter-VLAN. Además, se utilizará el software de simulación Cisco Packet Tracer, herramienta fundamental para realizar pruebas preliminares y validar configuraciones antes de su aplicación en los equipos físicos. Las prácticas y configuraciones se realizarán en los laboratorios de redes de la universidad, los cuales cuentan con infraestructura adecuada y conectividad interna estable.

2.3.5. Capacitación del equipo investigador

El equipo investigador cuenta con formación académica en el área de Electrónica y Redes de Computadoras, con conocimientos sólidos en configuración de dispositivos Cisco, segmentación de redes mediante VLANs y aplicación de políticas de seguridad mediante ACLs. Se posee experiencia previa en simulación de entornos de red con Cisco Packet Tracer y en la aplicación de metodologías de prueba y verificación de conectividad, lo cual garantiza un manejo técnico competente de las herramientas utilizadas.

2.3.6. Metodología y herramientas técnicas

La metodología técnica estará basada en la configuración, simulación y validación de políticas de seguridad de red mediante ACLs extendidas. Se emplearán técnicas experimentales y de simulación, iniciando con la creación de un entorno virtual en Packet Tracer que permita verificar la lógica de las configuraciones antes de su implementación real.

2.3.7. Acceso a fuentes de información

El proyecto dispone de acceso a fuentes académicas y técnicas actualizadas, entre ellas las bases de datos institucionales, bibliografía especializada en redes y seguridad informática, y los recursos oficiales de Cisco Networking Academy.

2.3.8. Viabilidad técnica

El proyecto es técnicamente viable, dado que las tecnologías involucradas —ACLs extendidas, enrutamiento inter-VLAN y simulación de redes— son maduras, estables y ampliamente documentadas. Los equipos y el software disponibles cumplen con los requerimientos necesarios, y la estructura modular del proyecto permite una implementación por fases que facilita la detección y corrección de errores durante el proceso. Esto asegura que el desarrollo y la ejecución se realicen dentro de los recursos y capacidades técnicas existentes

CRONOGRAMA

Figura 4

Cronograma de actividades de proyecto de tesis.

Nota. Cronograma de actividades.

BIBLIOGRAFÍA

9.1.2.1 Tipos de ACL de IPv4 de Cisco. (n.d.). Sapalomera.Cat. Retrieved September 30, 2025, from https://www.sapalomera.cat/moodlecf/RS/2/course/module9/9.1.2.1/9.1.2.1.html

Catalyst 3750-X and 3560-X switch software configuration guide, release 12.2(55)SE. (2018, September 11). Cisco. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swipv6.html

Configuración de ACLs con packet tracer. (n.d.). Scribd. Retrieved September 30, 2025, from https://es.scribd.com/document/713452284/Configuracion-de-ACLs-con-Packet-Tracer-Google-Docs

Configuración de direcciones IP y subredes únicas para nuevos usuarios. (2025, January 24). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

Configuración de la lista de control de acceso (ACL) basada en IPv4 y la entrada de control de acceso (ACE) en un switch. (2025, April 30). Cisco. https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb3025-configure-ipv4-based-access-control-list-acl-and-access-cont.html

Configure and filter IP access lists. (2024, February 12). Cisco. https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html?dtid=osscdc000283&linkclickid=srch

Configure IP addresses and unique subnets for new users. (2025, January 24). Cisco. https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

Configure standard access control list step by step guide. (2020, January 12). ComputerNetworkingNotes. https://www.computernetworkingnotes.com/ccna-study-guide/configure-standard-access-control-list-step-by-step-guide.html

De direccionamiento, T. T. (n.d.). *Packet Tracer: configuración de interfaces IPv4 e IPv6*. Sapalomera.Cat. Retrieved September 30, 2025, from https://www.sapalomera.cat/moodlecf/RS/2/course/files/4.1.3.5%20Packet%20Tracer%20-%20Configuring%20IPv4%20and%20IPv6%20Interfaces%20Instructions.pdf

de Ingeniería, E. (n.d.). *ESCUELA POLITÉCNICA NACIONAL*. Edu.Ec. Retrieved September 30, 2025, from https://bibdigital.epn.edu.ec/bitstream/15000/5378/1/T2397.pdf

Molenaar, R. (2016, November 10). *IPv4 address configuration on Cisco IOS catalyst switch*. Networklessons.com. https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ipv4-address-configuration-on-cisco-ios-catalyst-switch

PacketTracerNetwork. (n.d.). *Packet Tracer 8.2 tutorial - ACL configuration*. Packet Tracer Network. Retrieved September 30, 2025, from https://www.packettracernetwork.com/tutorials/packet-tracer-acls.html

CARRERA: ELECTRÓNICA

FECHA DE PRESENTACIÓN:	25 DÍA	06 MES	2025 AÑO
APELLIDOS Y NOMBRES DEL EGRESADO: ANDRES CAIZA & JONATHAN NARANJO			
TITULO DEL PROYECTO: IMPLEMENTACIÓN DE LISTAS DE CONTROL DE ACCESO (ACLS) EXTENDIDAS PARA LA GESTIÓN DE TRÁFICO IPV4 .			

PLANTEAMIENTO DEL PROBLEMA:	CUMPLE	NO CUMPLE
• OBSERVACIÓN Y DESCRIPCIÓN	X	
• ANÁLISIS	X	
• DELIMITACIÓN.	X	
• FORMULACIÓN DEL PROBLEMA CIENTÍFICO	X	
• FORMULACIÓN PREGUNTAS/AFIRMACIÓN DE INVESTIGACIÓN	X	

PLANTEAMIENTO DE OBJETIVOS:

GENERALES:

REFLEJA LOS CAMBIOS QUE SE ESPERA LOGRAR CON LA INTERVENCIÓN DEL PROYECTO

SI	NO
X	

ESPECÍFICOS:

GUARDA RELACIÓN CON EL OBJETIVO GENERAL PLANTEADO

SI	NO
X	

JUSTIFICACIÓN:	CUMPLE	NO CUMPLE
IMPORTANCIA Y ACTUALIDAD	X	
BENEFICIARIOS	X	
FACTIBILIDAD	X	

ALCANCE:	CUMPLE	NO CUMPLE
ESTA DEFINIDO	X	

MARCO TEÓRICO:

FUNDAMENTACIÓN TEÓRICA	SI	NO
DESCRIBE EL PROYECTO A REALIZAR	X	

TEMARIO TENTATIVO:	CUMPLE	NO CUMPLE
ANTECEDENTES, FUNDAMENTACIÓN TEÓRICA	X	
ANÁLISIS Y SOLUCIONES PARA EL PROYECTO	X	
APLICACIÓN DE SOLUCIONES	X	
EVALUACIÓN DE LAS SOLUCIONES	X	

TIPO DE INVESTIGACIÓN PLANTEADA

OBSERVACIONES: La investigación es aplicada y cuantitativa. Se enfoca en resolver un problema concreto mediante la implementación para la gestión de tráfico ipv4 y la segmentación segura entre vlans en entornos de red cisco.

MÉTODOS DE INVESTIGACIÓN UTILIZADOS:
OBSERVACIONES:

- **Método experimental**: Se probará el funcionamiento del sistema de seguridad mediante el listado de control de listas ACLs.

- **Método analítico**: Se analizarán los requerimientos técnicos y de seguridad antes, durante y después de la implementación.

- **Método descriptivo**: Se documentará detalladamente el proceso de instalación, configuración y operación del sistema.

- **Método inductivo-deductivo**: Se partirá de observaciones específicas sobre problemas de control de acceso, para luego proponer soluciones generales y evaluarlas.

CRONOGRAMA:

OBSERVACIONES:
El cronograma incluye las siguientes fases:

- **Recolección de información y diagnóstico** (Mes 1)
- **Diseño del sistema de control de accesos** (Mes 2)
- **Adquisición e integración de componentes** (Mes 3)
- **Instalación y pruebas del sistema** (Mes 4)
- **Análisis de resultados y redacción del informe final** (Mes 5)

FUENTES DE INFORMACIÓN:

Configure IP addresses and unique subnets for new users. (2025, January 24). Cisco. https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

RECURSOS:	CUMPLE	NO CUMPLE
HUMANOS	X	
ECONÓMICOS	X	
MATERIALES	X	

PERFIL DE PROYECTO DE GRADO

Aceptado [X]

Negado [ ] el diseño de investigación por las siguientes razones:

a) ----------

---

b) ----------

---

c) ----------

ESTUDIO REALIZADO POR EL ASESOR:

NOMBRE Y FIRMA DEL ASESOR: BOHÓRQUEZ PÉREZ MARÍA GABRIELA

04 09 2025
DÍA MES AÑO
FECHA DE ENTREGA DE INFORME