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

INSTRUCTIVO PARA LA ELABORACIÓN DE PERFIL DE PROYECTO DE GRADO

PERFIL DE PROYECTO DE TITULACIÓN

Quito – Ecuador 2025

PERFIL DE PROYECTO DE TITULACIÓN

CARRERA: ELECTRÓNICA

TEMA: Diseño e Implementación de un Sistema de Control de Acceso y Seguridad en Redes Locales Mediante Filtrado por Dirección MAC, Control de Puertos y Segmentación de Tráfico

Elaborado por:

LUIS FRA PADILLA VALLE KEVIN DAVID

ROLDAN PACHECO FRANKLIN SEBASTIAN

Tutor:

Bohórquez Pérez María Gabriela

Fecha: (04/09/2025)

Índice de contenidos

Índice de gráficos

Índice de tablas

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 Formulación y planteamiento del Problema

A pesar de que las redes locales (LAN) son esenciales para la operación de organizaciones, muchas de ellas presentan deficiencias en sus mecanismos de seguridad a nivel de infraestructura, lo que permite el acceso no autorizado de dispositivos, exposición de datos sensibles y propagación de amenazas internas. La ausencia de filtrado por dirección MAC, control de puertos y segmentación lógica del tráfico genera redes vulnerables y difíciles de administrar. Además, la falta de recursos o conocimientos técnicos limita la adopción de soluciones avanzadas como sistemas de autenticación 802.1X o firewalls dedicados. Ante esta problemática, se hace necesario diseñar e implementar un sistema de control de acceso y seguridad de red basado en tecnologías accesibles y configurables, como el filtrado por MAC, la gestión de puertos y la creación de VLANs en switches y routers gestionables, con el fin de restringir el acceso no autorizado, aislar segmentos de red y mejorar la eficiencia y seguridad de las comunicaciones internas.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un sistema de control de acceso y seguridad en redes locales que utilice filtrado por dirección MAC, control de puertos y segmentación mediante VLAN, como mecanismos para gestionar de forma segura el acceso a la red. Esta solución debe ser accesible y estar orientada a prevenir accesos no autorizados, además de mejorar el rendimiento en entornos de redes pequeñas y medianas.

1.2.2 Objetivos específicos

- Analizar los requerimientos técnicos y de seguridad de una red local, identificando vulnerabilidades

asociadas al acceso físico y lógico no autorizado.

- Configurar mecanismos de filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLAN, utilizando switches y routers gestionables, tanto en entornos físicos como simulados.
- Evaluar el funcionamiento del sistema implementado mediante pruebas de conectividad, acceso controlado y segmentación de tráfico, determinando su eficacia para mejorar la seguridad y administración de la red.

1.3 Justificación

En un contexto donde la aplicación práctica cobra mayor relevancia, proteger las redes locales (LAN) se vuelve esencial para asegurar la confidencialidad, integridad y disponibilidad de los recursos informáticos dentro de una organización. Sin embargo, muchas pequeñas y medianas entidades carecen de soluciones efectivas para controlar el acceso a su red interna, ya sea por limitaciones presupuestarias

Implementar un sistema de control de acceso basado en mecanismos como el filtrado por dirección MAC, el control de puertos y la segmentación lógica mediante VLANs representa una alternativa accesible, escalable y eficaz para fortalecer la seguridad en infraestructuras existentes. Estas tecnologías, disponibles en la mayoría de switches y routers gestionables, permiten restringir el acceso a dispositivos no autorizados, aislar segmentos críticos del tráfico y reducir el riesgo de propagación de amenazas internas.

Además, esta propuesta ofrece una solución adaptable a las necesidades de cada organización, sin requerir inversiones elevadas en equipamiento especializado ni en licencias de software costosas. Por tanto, el desarrollo e implementación de este tipo de sistema contribuye significativamente a mejorar la gestión de red, la protección de los activos informáticos y el cumplimiento la buena práctica en seguridad, especialmente en entornos con recursos técnicos y financieros limitados.

1.4 Alcance

El presente proyecto comprende el diseño, implementación y validación de un sistema de control de acceso y seguridad en redes locales, que emplea técnicas de filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLANs, utilizando switches y routers.

La implementación incluye tanto la configuración y prueba en un entorno físico real, comprobados con equipos de Cisco, como la simulación en herramientas especializadas para verificar el correcto funcionamiento y eficacia del sistema.

Se adquirieron y configuraron dispositivos compatibles con las tecnologías requeridas, garantizando su integración con la infraestructura de red existente sin generar interrupciones. Además, se desarrolló una guía de configuración que documenta paso a paso la implementación de los mecanismos de seguridad mencionados, incluyendo la verificación del filtrado, el control de puertos y la segmentación del tráfico.

Este proyecto se enfoca en redes de pequeña y mediana escala, tales como las de instituciones educativas o pequeñas empresas, donde se busca mejorar la seguridad y la administración del tráfico interno, mitigando accesos no autorizados y optimizando el rendimiento de la red. No contempla la integración con sistemas de autenticación avanzados ni soluciones de seguridad a nivel de capa superior, enfocándose en la capa 2 y 3 del modelo OSI.

1.5 Métodos de investigación

Método de Estudio de Casos: El proyecto se enmarca en el método de Estudio de Casos, el cual permite analizar de manera detallada la implementación de un sistema de seguridad en aulas de la carrera de Electrónica, integrando el control de acceso físico y lógico. En primer lugar, se procede al análisis de los requerimientos técnicos y de seguridad de la red local, identificando vulnerabilidades relacionadas con accesos no autorizados. Posteriormente, se configuran mecanismos de protección como filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLAN, empleando switches y routers gestionables en entornos físicos y simulados, con el fin de garantizar un diseño seguro y funcional.

Método de Análisis de Documentos: A partir de este enfoque, se analizan normas, manuales técnicos, artículos académicos y documentación de fabricantes con el fin de identificar los requerimientos técnicos y de seguridad aplicables a la red local, así como posibles vulnerabilidades vinculadas al acceso físico y lógico no autorizado. De igual manera, se estudian guías y protocolos de configuración que permiten definir la implementación de mecanismos de filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLAN en switches y routers gestionables, tanto en entornos físicos como simulados. Finalmente, la revisión documental proporciona los criterios necesarios para establecer indicadores de evaluación del sistema, orientados a medir su funcionamiento mediante pruebas de conectividad, acceso controlado y segmentación de tráfico, determinando así la eficacia de la solución propuesta en la mejora de la seguridad y administración de la red.

Método de Observación: El proyecto aplica el método de Observación, el cual consiste en monitorear directamente el comportamiento de los usuarios del sistema de control de acceso en un entorno real, verificando además las características de seguridad de las cerraduras inteligentes implementadas, como su resistencia a manipulaciones y sus mecanismos de protección. A través de esta técnica, se observan situaciones prácticas en las que los estudiantes y docentes hacen uso del sistema, identificando posibles vulnerabilidades relacionadas con el acceso físico y lógico no autorizado.7

Método de Análisis de Productos: El proyecto emplea el método de Análisis de Productos, el cual permite comparar diferentes modelos de filtrado de red disponibles en el mercado, evaluando aspectos clave como sus funcionalidades, costos, facilidad de

instalación y el soporte técnico ofrecido por los fabricantes. Este análisis sirve de base para seleccionar el dispositivo más adecuado en función de los requerimientos técnicos y de seguridad identificados en la red local, considerando la necesidad de prevenir accesos físicos y lógicos no autorizados.

Método de Análisis de Costos y Beneficios: **:** se aplica para evaluar los gastos asociados al análisis de los requerimientos técnicos y de seguridad de la red local, considerando los recursos necesarios para identificar y mitigar vulnerabilidades relacionadas con accesos físicos y lógicos no autorizados. De igual forma, se contemplan los costos derivados de la configuración de mecanismos de filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLAN en switches y routers gestionables, tanto en entornos físicos como simulados, contrastándolos con las ventajas que aportan en términos de protección y eficiencia en la administración de la red.

1.6 Marco Teórico

La seguridad en redes locales (LAN) representa un componente crítico para garantizar la protección de la información y la continuidad operativa en organizaciones de todo tipo. El aumento en la interconectividad de dispositivos y la proliferación de amenazas tanto internas como externas hacen necesario implementar mecanismos sólidos que regulen el acceso a la red y permitan una segmentación eficiente del tráfico. Este estudio se enfoca en la implementación de tres técnicas fundamentales de seguridad dentro de la infraestructura de red tenemos: filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLAN, empleando equipos gestionables como switches y routers Cisco, tanto en entornos simulados como en implementaciones físicas reales.

1.6.1 Filtrado por Dirección MAC

- El filtrado por dirección MAC (Media Access Control) se fundamenta en la identificación única de cada dispositivo a través de su dirección física, operando en la capa 2 del modelo OSI, esta técnica restringe el acceso a la red solo a los dispositivos cuyo identificador está previamente autorizado.
- Esta medida resulta eficaz para impedir la conexión de dispositivos no autorizados, mitigar ataques de suplantación (MAC Spoofing) y limitar la expansión de amenazas internas. No obstante, debido a que las direcciones MAC pueden ser falsificadas, el filtrado por MAC debe ser complementado con otras medidas de seguridad para garantizar un control efectivo.

1.6.2 Control de Puertos

El control de puertos es una funcionalidad avanzada que regula la conexión física de dispositivos a los puertos de los switches. Cisco implementa esta característica bajo el nombre de Port Security, la cual permite definir parámetros como el número máximo de direcciones MAC permitidas por puerto, las direcciones MAC estáticas autorizadas y las acciones ante violaciones, como el bloqueo del puerto o el envío de alertas al administrador.

1.6.3 Port SecuritY

Contribuye significativamente a prevenir ataques de MAC flotantes, donde un atacante intenta saturar la tabla MAC del switch para provocar un modo de difusión que comprometa la seguridad de la red. Además, limita la inserción no autorizada de dispositivos, fortaleciendo la seguridad en el perímetro físico de la red.

1.6.4 Segmentación del Tráfico mediante VLANs

Las VLANs (Virtual Local Area Networks) permiten la creación de redes lógicas independientes dentro de una misma infraestructura física, dividiendo el dominio de broadcast para mejorar tanto el rendimiento de la seguridad. Al operar en la capa 2, las VLANs facilitan la segregación de usuarios y servicios, minimizando la propagación de tráfico no deseado y reduciendo el riesgo de ataques que se diseminan a través del dominio broadcast.

En dispositivos Cisco, la configuración de VLANs se realiza a nivel de switch, asignando puertos a diferentes VLANs y gestionando las etiquetas VLAN en las tramas Ethernet (802.1Q). Para permitir la comunicación entre VLANs, es necesario el enrutamiento inter-VLAN, que puede ser realizado por routers dedicados o switches multicapa que operan en la capa 3 del modelo OSI.

Esta segmentación lógica es vital para implementar políticas de seguridad diferenciadas, limitar el acceso entre grupos y optimizar el uso del ancho de banda, favoreciendo la escalabilidad y flexibilidad de la red.

1.6.5 Simulación en Cisco Packet Tracer

Cisco Packet Tracer es una herramienta de simulación ampliamente utilizada en el ámbito académico y profesional para diseñar, configurar y probar topologías de red. Esta plataforma ofrece un entorno visual y dinámico que emula el comportamiento real de dispositivos Cisco, permitiendo la configuración mediante comandos CLI idénticos a los empleados en hardware físico.

La simulación en Packet Tracer facilita la experimentación con configuraciones complejas, como la aplicación de filtrado por MAC, Port Security y VLANs, sin la necesidad de

disponer de equipos físicos. Además, permite realizar pruebas de conectividad, validación de tablas de enrutamiento y monitoreo del tráfico, proporcionando un ambiente seguro y controlado para la detección y corrección de errores antes de la implementación física. Esta herramienta contribuye a la reducción de costos y riesgos asociados a pruebas en redes reales, y es fundamental para la capacitación y desarrollo de competencias en administración y seguridad de redes.

1.6.6 Implementación Física con Equipos Cisco

La implementación física con dispositivos Cisco gestionables es esencial para validar en un entorno real las configuraciones y protocolos diseñados en la simulación. Los switches y routers Cisco ofrecen soporte completo para todas las funcionalidades estudiadas, incluyendo filtrado MAC, Port Security y VLANs, además de proporcionar herramientas avanzadas de monitoreo, gestión y diagnóstico.

La configuración se realiza a través de la interfaz de línea de comandos (CLI), permitiendo un control detallado de parámetros y políticas de seguridad. El montaje en racks, la conexión física mediante cables UTP, y la integración con la red existente permiten evaluar el desempeño bajo condiciones reales, como latencias, interferencias electromagnéticas y variaciones en el tráfico.

La implementación física también incluye la documentación por que no existe exhaustiva de configuraciones, procedimientos de prueba y verificación, y el establecimiento de protocolos de mantenimiento y actualización, garantizando la escalabilidad y continuidad del sistema de seguridad.

1.6.7 Tipos de direcciones IP

Las direcciones IP son fundamentales para la comunicación en Internet y en redes locales. A continuación, te explico sobre los diferentes tipos de direcciones IP.

- **Direcciones IP Públicas**

  Las direcciones IP públicas son aquellas que se pueden acceder desde Internet. Estas direcciones son únicas en Internet y se asignan a dispositivos que necesitan ser accesibles desde la red global ejemplo tienes un negocio en línea y quieres que la gente pueda acceder a tu sitio web desde cualquier lugar del mundo. Para eso necesitas una dirección IP pública, que es como una señal única que permite que los dispositivos se conecten a tu servidor desde Internet.

- **Direcciones IP Estáticas**

  Las direcciones IP estáticas son aquellas que se asignan de forma permanente a un dispositivo. Estas direcciones no cambian, aunque se reinicie el dispositivo o se desconecte de la red. Las direcciones IP estáticas se utilizan comúnmente en

servidores y otros dispositivos que requieren una dirección IP fija para funcionar correctamente.

- Direccionamiento Ipv IPv4

  En el ámbito de IPv4, las direcciones se clasifican principalmente en tres tipos: direcciones unicast, broadcast y multicast. Cada una de estas tiene funciones específicas dentro de una red y se utiliza según el tipo de comunicación requerida. Comprender las diferencias entre estos tipos de direcciones es esencial para una correcta planificación y asignación de direcciones IPv4.

1.6.8 Tipos de Direcciones IPv4

- **Las direcciones Unicast**

  Este tipo de dirección identifica de manera única a un solo dispositivo dentro de la red. La comunicación unicast implica que un paquete se envía desde un origen hacia un único destino específico. Es el tipo de dirección más común y se utiliza para la mayoría de las comunicaciones entre dispositivos.

- **Las direcciones Broadcast**

  Una dirección broadcast permite enviar un paquete a todos los dispositivos dentro de una red local. La dirección de broadcast para una red se representa por una dirección IP donde todos los bits de la parte del host están en 1 (por ejemplo, 192.168.1.255 para una red con máscara 255.255.255.0). Este tipo de comunicación es útil cuando se necesita anunciar información a todos los nodos de la red simultáneamente.

- **Las direcciones Multicast**

  Las direcciones multicast se utilizan para enviar datos a un grupo específico de dispositivos que han expresado interés en recibir esa información. A diferencia del broadcast, que llega a todos, el multicast solo alcanza a los dispositivos que forman parte del grupo multicast. Las direcciones multicast en IPv4 pertenecen al rango de 224.0.0.0 a 239.255.255.255.

1.6.9 Rutas estáticas

Las rutas estáticas permiten a los routers anunciar redes no conectadas directamente, especificando el prefijo de red y la dirección IP del siguiente salto. Esto facilita la transmisión de paquetes hacia destinos dentro del rango de red asignado, el proceso es similar al de IPv4, con la particularidad de que el siguiente salto debe ser una dirección link-local.

1.6.10 La evolución de direccionamiento de IPv4

El direccionamiento IPv4 fue diseñado inicialmente con un espacio limitado de 4.3 mil millones de direcciones, usando un sistema por clases (A, B, C). Sin embargo, el crecimiento de internet provocó un rápido agotamiento de estas direcciones. Para optimizar su uso, se implementaron soluciones como CIDR (direccionamiento sin clases) y NAT (traducción de direcciones de red), que permitieron una asignación más eficiente.

1.6.11 El desafío del agotamiento de direcciones IPv4

El protocolo IPv4 utiliza direcciones de 32 bits, lo que permite alrededor de 4.300 millones de direcciones únicas. Pero con tantos dispositivos conectados a Internet, estas direcciones se acabaron rápido. Para solucionar esto, se crearon técnicas como NAT (Traducción de Dirección de Red) que permiten reutilizar direcciones IP y prolongar la vida de IPv4.

1.6.12 Ventajas IPv4:

- Mas Amplio soporte y compatibilidad con la mayoría de los dispositivos, sistemas operativos y redes.
- Infraestructura estable y probada, gracias a años de implementación y optimización.
- Simplicidad en la configuración, especialmente en redes pequeñas.
- ●Soporte para NAT, lo que permite que múltiples dispositivos compartan una sola dirección IP pública.

Simulador Cisco Packet Tracer

1.6.13 Introducción de Packet Tracer

En el campo de las redes y la ciberseguridad, la práctica constante y la experimentación son fundamentales para alcanzar un alto nivel de competencia. Cisco Packet Tracer se destaca como una herramienta de simulación líder, que proporciona un entorno de laboratorio virtual seguro e inmersivo para desarrollar habilidades prácticas en configuración, diseño y solución de problemas de redes. Esta plataforma permite visualizar el flujo de tráfico en la red y realizar simulaciones como pruebas de conectividad (ping y traceroute) desde consolas integradas. Además, es compatible con la mayoría de los comandos del sistema operativo Cisco IOS y como algo adicional ofrece la función de autocompletado de comandos ("tab completion") para agilizar el trabajo. Gracias a estas funcionalidades, Cisco Packet Tracer se consolida como una herramienta esencial para quienes desean

perfeccionar sus habilidades en un entorno de aprendizaje interactivo y sin riesgos.

1.6.14 Características de Cisco Packet Tracer

- Simulación de redes: Permite diseñar, configurar y probar redes virtuales.
- Entorno de laboratorio virtual: Ofrece un entorno seguro y controlado para practicar y experimentar.
- Diseño de redes: Permite diseñar redes complejas con dispositivos de red, como routers, switches y servidores.
- Configuración de dispositivos: Permite configurar dispositivos de red y probar sus configuraciones.
- Visualización del tráfico de red: Permite visualizar el flujo de tráfico de red y analizar su comportamiento.

1.6.15 Routers

Un router es el corazón de cualquier red, ya que actúa como un distribuidor inteligente que conecta múltiples redes informáticas y dirige el tráfico de datos con precisión. Al enrutar paquetes de datos entre redes, un router permite que varios usuarios compartan una conexión a Internet y accedan a recursos en línea de manera eficiente. Además, los routers facilitan la conexión de redes dentro de una organización o entre sucursales remotas, lo que permite una comunicación fluida y segura entre diferentes ubicaciones. Con su capacidad para elegir la mejor ruta para el tráfico de datos, los routers garantizan que la información se transmita de manera rápida y confiable, lo que es fundamental para el funcionamiento eficiente de cualquier red. En resumen, un router es un componente esencial para cualquier red que requiera conectividad, seguridad y eficiencia en la transmisión de datos.

1.6.16 Funciones principales

Una de las funciones prioritarias de esta red es el bloqueo de puertos basado en la dirección MAC asignada a cada equipo. Este mecanismo realiza una verificación constante de conectividad mediante comandos de ping y verificar constantemente su conectividad sin paro, lo que permite identificar si un dispositivo permanece conectado correctamente al puerto asignado. En caso de que el equipo sea desconectado o trasladado a otro puerto —por ejemplo, si se intenta conectar desde otra PC no autorizada— el sistema detecta el cambio y bloquea automáticamente el acceso del nuevo dispositivo.

Esta medida de seguridad se complementa con la segmentación de la red mediante VLANs (Redes de Área Local Virtuales) y la asignación de contraseñas específicas por usuario, lo que refuerza el control de acceso. Además, se ha habilitado la

configuración de un servidor DHCP, que permite asignar dinámicamente direcciones IP dentro del rango permitido para cada segmento de red, facilitando la administración y reduciendo errores de configuración manual.

2. ASPECTOS ADMINISTRATIVOS

2.1. Recursos humanos

- PADILLA VILLA KEVIN DAVID
- ROLDAN PACHECO FRANKLIN SEBASTIAN

2.2. Recursos técnicos y materiales

Tabla de materiales

Tabla 1
Equipos y materiales

EQUIPO	MARCA	Gráficos
SWITCH	CISCO Catalyst 3560 v2series	
ROUTER	CISCO 1921	
COMPUTADORAS	INS	

CABLE CONSOLA	Linoya AWM 2835	
CABLE UTP	Panduit CAT6A	
CONECTORES	RJ45 CAT6	
RACK	BEAUCOUP 4 pies con base móvil	
PDU	Regleta multitoma	

2.3. Viabilidad

Los objetivos planteados para el proyecto son viables tanto en términos técnicos como prácticos. El objetivo general de diseñar un sistema de control de acceso y seguridad en redes locales mediante filtrado por dirección MAC, control de puertos y segmentación mediante VLAN es alcanzable, ya que los recursos necesarios, como switches y routers gestionables, herramientas de simulación (por ejemplo, Cisco Packet Tracer) y cerraduras inteligentes, son accesibles y ampliamente utilizados en entornos académicos y de redes pequeñas y medianas.

Los objetivos específicos también son factibles:

- Análisis de requerimientos técnicos y de seguridad: es viable mediante la revisión de documentación técnica, normas de seguridad y la inspección del entorno físico y lógico de la red. Esto permitirá identificar vulnerabilidades sin requerir infraestructura costosa.

- Configuración de mecanismos de seguridad: la implementación de filtrado por MAC, control de puertos y VLAN puede realizarse tanto en entornos simulados como reales, aprovechando equipos de laboratorio o simuladores de red, lo que facilita la experimentación y validación práctica.

- Evaluación del funcionamiento del sistema: la viabilidad está garantizada mediante pruebas de conectividad, control de acceso y segmentación de tráfico, que permiten medir objetivamente la eficacia del sistema y la mejora en la seguridad y administración de la red.

2.3.1 Financiera

La viabilidad financiera de los objetivos del proyecto es favorable, dado que los recursos requeridos para el diseño e implementación del sistema de control de acceso y seguridad en redes locales son accesibles dentro del marco académico y de laboratorios de redes. La inversión principal está asociada a la adquisición de switches y routers gestionables, así como de cerraduras inteligentes para el control de acceso físico. Para reducir costos, parte de la implementación y pruebas pueden realizarse en entornos simulados como Cisco Packet Tracer, minimizando la necesidad de equipamiento físico completo.

El análisis de requerimientos técnicos y de seguridad no implica gastos significativos, ya que se puede realizar mediante revisión de documentación y auditorías internas de la red.

La configuración de filtrado por dirección MAC, control de puertos y segmentación mediante VLAN puede ejecutarse en equipos de laboratorio existentes, lo que optimiza el presupuesto. Finalmente, las pruebas de conectividad, acceso controlado y segmentación de tráfico no requieren inversiones adicionales relevantes, siendo mayormente operativas y de tiempo de personal.

2.3.2 Operativa

La viabilidad operativa de los objetivos del proyecto es alta, ya que las actividades planificadas se pueden ejecutar con los recursos humanos y tecnológicos disponibles en un entorno académico. El diseño del sistema de control de acceso y seguridad en redes locales se puede realizar utilizando equipos de laboratorio existentes, como switches y routers gestionables, además de cerraduras inteligentes para el control físico de acceso.

El análisis de los requerimientos técnicos y de seguridad es operativamente factible, ya que se puede llevar a cabo mediante inspección del entorno de red, revisión de documentación técnica y auditorías internas, sin necesidad de infraestructura adicional compleja. La configuración de los mecanismos de seguridad, como filtrado por dirección MAC, control de puertos y segmentación mediante VLAN, se puede implementar tanto en entornos simulados (Cisco Packet Tracer u otros simuladores) como en entornos físicos, lo que permite pruebas seguras antes del despliegue real.

2.3.3 Técnico

Para alcanzar los objetivos del proyecto se aplicará una combinación de técnicas que incluyen la revisión documental y auditoría de red para analizar los requerimientos técnicos y de seguridad,

identificando vulnerabilidades asociadas al acceso físico y lógico no autorizado; la implementación práctica en entornos físicos y simulados, mediante la configuración de filtrado por dirección MAC, control de puertos y segmentación de tráfico mediante VLAN en switches y routers gestionables; y las pruebas de conectividad y control de acceso, que permiten evaluar el funcionamiento del sistema en escenarios reales y simulados, verificando la eficacia de la solución en la prevención de accesos no autorizados, la correcta segmentación del tráfico y la mejora en la administración y seguridad de la red local.

2.4 Cronograma

Figura 4 Cronograma de actividades de proyecto de tesis

3. BIBLIOGRAFÍA

Academy, C. N. (s.f.). Cisco Packet Tracer. Obtenido de https://www.netacad.com/es/cisco-packet-tracer

Autmix. (s.f.). ¿Qué es un protocolo de red y para qué sirve? Obtenido de Autmix.: https://autmix.com/blog/que-es-protocolo-red

Cisco. (s.f.). ¿Cómo funciona un router? Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/how-does-a-router-work.html

Cisco. (s.f.). ¿Qué es un switch de red? Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html

Citrix. (s.f.). Internet Protocol version 6 (IPv4). Obtenido de https://docs.netscaler.com/es-es/citrix-adc/current-release/networking/internet-protocol-version-6-ipv6.html

Community, C. (4 de Mayo de 2022). Fundamentos de IPv4. Obtenido de https://community.cisco.com/t5/blogs-general/fundamentos-de-ipv6/ba-p/4725481

Community, C. (8 de Julio de 2022). OSPFv3 para IPv4 en Cisco IOS XE. Obtenido de https://community.cisco.com/t5/blogs-general/ospfv3-para-ipv4-en-cisco-ios-xe/ba-p/4794693

Monografías.com. (s.f.). Principios de redes. Obtenido de https://www.monografias.com/trabajos107/principios-redes/principios-redes

CARRERA: ELECTRÓNICA

FECHA DE PRESENTACIÓN: 08 (DÍA) 03 (MES) 2025 (AÑO)

APELLIDOS Y NOMBRES DEL EGRESADO: KEVIN DAVID PADILLA VALLE
FRANKLIN SEBASTIAN ROLDAN PACHECO

TITULO DEL PROYECTO: Diseñar un sistema de control de acceso y seguridad en redes locales que utilice filtrado por dirección MAC, control de puertos y segmentación mediante VLAN, como mecanismos para gestionar de forma segura el acceso a la red. Esta solución debe ser accesible y estar orientada a prevenir accesos no autorizados, además de mejorar el rendimiento en entornos de redes pequeñas y medianas.

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: El proyecto se enmarca dentro de una investigación aplicada de tipo experimental y descriptiva, ya que su propósito es diseñar, implementar y evaluar un sistema de control de acceso y seguridad en redes locales mediante técnicas concretas como filtrado por dirección MAC, control de puertos y segmentación mediante VLAN. La investigación es aplicada, porque busca generar soluciones prácticas para prevenir accesos no autorizados y mejorar la administración de redes en entornos de tamaño pequeño y mediano. Además, tiene un componente experimental, al configurar y probar los mecanismos de seguridad en entornos físicos y simulados, permitiendo medir la efectividad del sistema mediante pruebas de conectividad, control de acceso y segmentación de tráfico.

MÉTODOS DE INVESTIGACIÓN UTILIZADOS:

OBSERVACIONES:

- **Método experimental**: Se aplica al **configurar y probar el sistema de control de acceso** en entornos físicos y simulados, permitiendo observar los resultados de las configuraciones de filtrado por MAC, control de puertos y segmentación VLAN, y medir la efectividad del sistema.

- **Método analítico**: Sirve para documentar y detallar el funcionamiento del sistema implementado, registrando cómo se comporta la red, cómo los usuarios acceden a los recursos y cómo se segmenta el tráfico.

- **Método descriptivo**: Sirve para documentar y detallar el funcionamiento del sistema implementado, registrando cómo se comporta la red, cómo los usuarios acceden a los recursos y cómo se segmenta el tráfico..

- **Método inductivo-deductivo**: Se emplea para extraer conclusiones a partir de la observación y pruebas, partiendo de casos específicos (resultados de pruebas de conectividad y control de acceso) para formular generalizaciones sobre la eficacia del sistema y validar el diseño propuesto.

CRONOGRAMA:

OBSERVACIONES:
El cronograma incluye las siguientes fases:

- **Recolección de información y diagnóstico** (SEMANA 1)
- **Diseño del sistema de control de accesos** (SEMANA 2)
- **Adquisición e integración de componentes** (SEMANA 4)
- **Instalación y pruebas del sistema** (SEMANA 6)
- **Análisis de resultados y redacción del informe final** (SEMANA 9)

FUENTES DE INFORMACIÓN:

ManageEngine. (s.f.). Protocolos de red: definición, tipos y lista de protocolos. Obtenido de https://www.manageengine.com/es/network-monitoring/network-protocols.html

Oracle. (s.f.). IPv4 Overview. Obtenido de Oracle Help Center: https://docs.oracle.com/cd/E19957-01/820-2981/ipv4-overview-10/index.html

Sistelec. (25 de Febrero de 2021). Redes de datos: ¿qué son, tipos y ventajas? Obtenido de https://sistelec.es/blog/redes-de-datos/

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

Firmado electrónicamente por:
MARIA GABRIELA BOHORQUEZ PEREZ
Validar únicamente con FirmaEC

04 09 2025
DÍA MES AÑO
FECHA DE ENTREGA DE INFORME