UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

EXTENSIÓN EL CARMEN

CARRERA DE INGENIERÍA EN SISTEMA

PROYECTO INTEGRADOR

TEMA:

Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional "Juan Pablo II"

AUTOR:

Rodríguez Utrera Erick Silvino

TUTOR:

Mg. Bladimir Mora. Mg

EL CARMEN – 2024

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EL CARMEN

APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueben el Trabajo de Titulación con modalidad Proyecto Integrador, titulado **"Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional "Juan Pablo II""**, cuyo autor es **Erick Silvino Rodríguez Utrera de la Carrera de Ingeniería en Sistemas** y como Tutor de Trabajo de Titulación el **Ing. Alex Bladimir Mora Marcillo, Mg.**

El Carmen, agosto de 2024

A.S. Wladimir Minaya, Mg.

Presidente del tribunal de titulación

Ing. Danilo Arévalo, Mg.

Miembro del tribunal de titulación

Ing. Carlos López, Mg.

Miembro del tribunal de titulación

CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de investigación, bajo la autoría del estudiante Rodríguez Utrera Erick Silvino, legalmente matriculado en la carrera de Ingeniería en Sistemas, período académico 2023-2024, cumpliendo el total de 400 horas, bajo la opción de titulación de Proyecto Integrador, cuyo tema del proyecto es "Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional Juan Pablo II".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

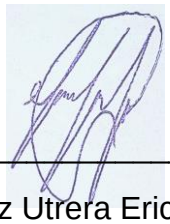
El Carmen, 31 de julio de 2024.

Lo certifico,

Ing. Alex Bladimir Mora Marcillo, Mg.
Docente Tutor
Área: Ingeniería en Sistemas

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: **Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional "Juan Pablo II**" corresponde exclusivamente al estudiante: Rodríguez Utrera Erick Silvino con cédula de ciudadanía número: 172574809-7 los derechos patrimoniales de la misma corresponden a la Universidad Laica “Eloy Alfaro” de Manabí.



Rodríguez Utrera Erick Silvino
C.C. 172574809-7

DEDICATORIA

Queridos padres y familiares:

Quiero expresarles mi más profundo y sincero agradecimiento por todo el apoyo, amor y dedicación que me han brindado a lo largo de mi vida.

A mis padres, gracias por ser mi guía y mi sostén en todo momento. Su esfuerzo, sacrificio y amor incondicional me han dado la fuerza y la motivación necesarias para superar cada desafío y alcanzar mis metas. Su ejemplo de trabajo arduo y perseverancia ha sido una inspiración constante.

A mis familiares, gracias por estar siempre presentes, por sus palabras de aliento y por creer en mí. Cada uno de ustedes ha contribuido de manera significativa a mi crecimiento personal y me ha enseñado lecciones valiosas que atesoro profundamente.

Su apoyo incondicional y sus muestras de cariño han sido fundamentales en mi vida. Estoy agradecido por cada momento compartido, por cada consejo y por cada gesto de amor.

Con gratitud y cariño,

Erick

AGRADECIMIENTO

Queridos padres, familiares, amigos y profesores:

Quiero expresar mi más profundo agradecimiento a todos ustedes por el apoyo, la guía y el amor incondicional que me han brindado a lo largo de este camino.

A mis padres, gracias por ser mi pilar fundamental, por enseñarme con su ejemplo el valor del esfuerzo y la perseverancia. Su dedicación y sacrificio han sido la base sobre la cual he construido mis sueños. Su amor incondicional me ha dado la fuerza para seguir adelante en los momentos más difíciles.

A mis familiares, gracias por estar siempre presentes, por sus palabras de aliento y por creer en mí. Cada uno de ustedes ha contribuido de manera significativa a mi crecimiento personal y académico. Sus consejos y apoyo han sido invaluables.

A mis amigos, gracias por compartir conmigo tantos momentos de alegría, por ser mi red de apoyo en las buenas y en las malas. Su amistad ha sido un refugio y una fuente de energía que me ha impulsado a seguir adelante.

A mis profesores, gracias por su paciencia, dedicación y por compartir su conocimiento conmigo. Han sido una fuente constante de inspiración y motivación. Sus enseñanzas van más allá de lo académico y han dejado una huella imborrable en mi vida.

A todos ustedes, mi más sincero agradecimiento por ser parte de este viaje. Cada uno de ustedes ha jugado un papel crucial en mi desarrollo y en la consecución de mis metas. Les estoy eternamente agradecido.

Con gratitud y cariño,

Erick

RESUMEN

La presente investigación tuvo como objetivo diseñar una “Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional "Juan Pablo II"”, el paradigma de la investigación fue cualitativo, se empleó una investigación documental y de campo, los métodos utilizados fueron el analítico-sintético y deductivo-inductivo, se utilizó una población de 30 docentes de la unidad educativa. Se aplicó un muestreo intencional donde se seleccionó a 5 docentes que forman parte del área administrativa y tienen conocimientos de informática básica. Las técnicas utilizadas fueron la entrevista, y la observación de campo, como resultado se obtuvo diseño de la red LAN con portal cautivo para la transmisión de información, como conclusión, la implementación de una red LAN con portal cautivo ayuda a la gestión administrativa y docencia de la Unidad Educativa Fiscomisional “Juan Pablo II”.

ABSTRACT

The objective of this research was to implement a "LAN Network with a captive portal for the transmission of information in the Fiscomisional Educational Unit "Juan Pablo II"", the paradigm of the research was qualitative, documentary and field research was used, the methods used were analytical-synthetic and deductive-inductive, a population of xxx teachers of the educational unit was used. An intentional sampling was applied where xxx teachers who are part of the administrative area and have basic computer skills were selected. The techniques used were the interview, and field observation, as a result the implementation of the LAN Network with a captive portal for the transmission of information was obtained, as a conclusion, the Implementation of the LAN Network with a captive portal helps the administrative management of the "Juan Pablo II" Fiscal Educational Unit.

INTRODUCCIÓN

Las empresas a nivel mundial utilizan redes LAN con portal cautivo para mejorar la seguridad y el control de acceso, autenticar usuarios, gestionar políticas de uso y monitorear la actividad de la red. Esto asegura que solo usuarios autorizados accedan, protege información sensible y optimiza el uso de recursos. Además, facilita el cumplimiento de normativas y proporciona una experiencia de usuario mejorada con información y comunicaciones personalizadas.

En América Latina, las empresas usan redes LAN con portal cautivo para asegurar la autenticación de usuarios, controlar el acceso y proteger información sensible. También permite gestionar políticas de uso, monitorear la actividad de la red y cumplir con normativas, mejorando así la seguridad y optimizando la experiencia del usuario.

Siendo las cosas así, en Ecuador las empresas como instituciones educativas no se pueden quedar atrás, y necesitan implementar este tipo de seguridades en la red LAN. Este es el caso de la “Unidad Educativa Fiscomisional “Juan Pablo II””, de la provincia de Manabí, cantón El Carmen-Bramadora, que ha diseñado una red LAN con portal cautivo para la transmisión de información.

La presente investigación tuvo como objetivo general “diseñar una red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional “Juan Pablo II””, y se basó en cumplir los objetivos específicos:

Definir los requerimientos iniciales y preparar el entorno para el diseño de la red de la Unidad Educativa Fiscomisional “Juan Pablo II””. Desarrollar un plan detallado para el diseño y la implementación de la red de la Unidad Educativa Fiscomisional “Juan Pablo II””. Crear un diseño detallado y específico de la red LAN de la Unidad Educativa Fiscomisional “Juan Pablo II””.

La estructura de la investigación fue la siguiente: CAPITULO I.- Se realizó una investigación documental sobre red LAN, portal cautivo y transmisión de información. En el CAPITULO II.- Se aplicó una entrevista a 5 docentes de la Unidad Educativa Fiscomisional “Juan Pablo II””, para ver las necesidades y estado actual del servicio de internet e infraestructura tecnológica, así mismo en este orden de ideas se realizó una observación de campo a la Unidad Educativa Fiscomisional “Juan Pablo II”” para ver los materiales existentes de redes y condiciones de las instalaciones. En el CAPITULO III, se aplicó la metodología PPDIOO de Cisco, donde se efectuó cada una de las etapas, dando como resultado final el diseño de la red LAN con portal cautivo en la Unidad Educativa Fiscomisional “Juan Pablo II””, como conclusión final se puede señalar que el diseño de una red LAN con portal cautivo ayuda en la transmisión de información en la Unidad Educativa Fiscomisional “Juan Pablo II””.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

ANEXOS

CAPITULO I

MARCO TEÓRICO

1. REDES LAN.

1.1. Definición de LAN.

Para Hernández (2023), una red LAN (Local Area Network) permite la conectividad y comunicación entre dispositivos periféricos, compartiendo información entre usuarios en la misma ubicación (casa u oficina). Utiliza dispositivos como computadoras, switches, routers y access points, con alcance limitado por medios físicos.

Una red LAN (Local Area Network) conecta dispositivos en una misma ubicación para compartir información y recursos mediante computadoras, switches, routers y otros periféricos, con alcance limitado físicamente.

1.2. Componentes de una LAN.

Los componentes de una red LAN incluyen computadoras, concentrador, conmutador de paquetes (switch), router, punto de acceso (access point), módem y repetidores, los cuales permiten la conectividad y comunicación entre dispositivos periféricos compartiendo información en una misma ubicación (Hernández, 2023).

En este contexto se manifiesta que, los componentes básicos de una red LAN permiten la conectividad y comunicación entre dispositivos periféricos, compartiendo información en una misma ubicación.

1.3. Topología de LAN.

Las topologías de una red LAN definen la disposición de los dispositivos y cables. Las más comunes son la topología de bus, anillo, estrella, jerárquica, malla y árbol, cada una con diferentes estructuras para la interconexión de equipos y transmisión de datos.

Esto se respalda con lo manifestado por Hernández (2023) donde señala que las topologías de las redes LAN son: bus, anillo, estrella, árbol e hibridas.

1.4. Protocolos en una LAN.

Según Delgado (2021), los protocolos LAN incluyen varios tipos de protocolos de señalización como H.323, SIP, MGCP (H.248) y SCCP. H.323 se utiliza para transmitir audio, video y datos a través de IP. SIP, basado en el modelo cliente-servidor, se usa en la señalización de VoIP. MGCP es estándar para la gestión centralizada de pasarelas y soluciones de telefonía de banda ancha. SCCP es un protocolo propietario de Cisco para señalización mediante TCP y UDP.

En este orden de ideas los protocolos de una red LAN incluyen: Ethernet para la transmisión de datos en redes locales. TCP/IP para la comunicación entre dispositivos, ARP para la resolución de direcciones IP a direcciones físicas, DNS para la resolución de nombres de dominio a direcciones IP, DHCP para la asignación dinámica de direcciones IP. Estos protocolos permiten a los dispositivos de una red LAN comunicarse de manera efectiva.

1.5. Direccionamiento de una LAN

El direccionamiento de una red LAN asigna direcciones IP únicas a cada dispositivo conectado, facilitando la identificación y comunicación dentro de la red. Utiliza esquemas como IPv4 e IPv6 para asegurar la correcta transmisión de datos entre dispositivos en una LAN.

El direccionamiento de una red LAN consiste en asignar direcciones IP a los dispositivos conectados a la red. Esto permite identificarlos y facilitar la comunicación entre ellos, asegurando que los datos se envíen y reciban correctamente dentro de la red local (Delgado, 2021).

1.6. Seguridad en una LAN.

Para Leyva et al. (2021), la seguridad en una red LAN se basa en el control de acceso, confidencialidad y conexiones externas. Estos aspectos incluyen la implementación de tecnologías para cumplir con políticas de seguridad,

garantizar la privacidad a través de redes privadas virtuales, y manejar conexiones remotas que pueden afectar el rendimiento y la integridad de los datos.

Con lo expuesto anteriormente, la seguridad en una red LAN implica proteger la integridad, confidencialidad y disponibilidad de los datos mediante controles de acceso, autenticación de usuarios, cifrado de comunicaciones, detección de intrusos y actualizaciones regulares de software y hardware.

1.7. Rendimiento de una LAN.

Solsol (2024), manifiesta que el rendimiento de una LAN está influenciado por factores como la velocidad de transferencia de datos, latencia, ancho de banda, y el uso de firewalls de última generación, que mejoran la seguridad y eficiencia de la red. La implementación de tecnologías avanzadas es crucial para optimizar el desempeño y asegurar una comunicación eficiente.

En este contexto se puede indicar que el rendimiento de una red LAN se evalúa por su velocidad de transmisión, latencia, congestionamiento, y calidad de servicio. La velocidad de transmisión se mide en Mbps, la latencia en milisegundos, y la congestión se puede detectar mediante la pérdida de paquetes y la variación en la velocidad (Solsol, 2024).

1.8. Administración de una LAN.

Para Rosado (2024), la administración de una red LAN implica la gestión eficiente de los equipos informáticos para garantizar alta disponibilidad, seguridad, y una distribución óptima del ancho de banda. Esto incluye el monitoreo constante para prevenir ataques, el uso eficiente de recursos y la implementación de soluciones avanzadas como redes definidas por software (SDN) para mejorar la estabilidad y el rendimiento general.

En otras palabras, la administración de una red LAN consiste en la organización, control y supervisión de la red para mantener su funcionamiento eficiente, mediante el uso de herramientas, aplicaciones y dispositivos. Esto incluye tareas como detección y aislamiento de fallas, evaluación del tráfico, mantenimiento de configuraciones y establecimiento de políticas de seguridad.

1.9. Escalabilidad de una LAN.

Vásquez (2024), señala que la escalabilidad de una red LAN se refiere a la capacidad de la red para adaptarse y crecer a medida que aumentan las demandas de usuarios y aplicaciones sin comprometer su rendimiento. Una red LAN escalable puede manejar un mayor número de dispositivos, tráfico y servicios sin necesidad de reemplazar la infraestructura existente.

Siendo las cosas así, la escalabilidad de una red LAN se refiere a su capacidad para expandirse y adaptarse al aumento de dispositivos y tráfico sin

afectar el rendimiento. Esto implica una planificación y arquitectura adecuadas para asegurar que la red pueda crecer y mantener una operación eficiente y estable (Vásquez, 2024).

1.10. Usos de una LAN.

Una red LAN (Local Area Network) se utiliza principalmente para conectar dispositivos dentro de un área limitada, como una oficina, una casa o una escuela. Facilita compartir recursos como impresoras y archivos, permite comunicaciones rápidas y seguras entre dispositivos, posibilita el acceso a internet compartido, y es fundamental para aplicaciones como videoconferencias y juegos en red (Pita, 2023).

Con la manifestado, una red LAN permite: Compartir recursos, facilita el trabajo colaborativo y el intercambio de información, mejorar la eficiencia, centraliza la administración y el mantenimiento de los sistemas, optimiza el uso de recursos y reduce costos, aumentar la seguridad, controla el acceso a la red y protege la información, facilita la implementación de políticas de seguridad, facilitar la comunicación.

2. PORTAL CAUTIVO.

2.1. Definición.

Para Ayala (2024), un portal cautivo es un mecanismo de seguridad de red que requiere que los usuarios se autentiquen o acepten términos y condiciones antes de obtener acceso completo a la red. Se utiliza para asegurar la red, proporcionar información a los usuarios y controlar el tráfico de la red inalámbrica.

Con estas consideraciones se puede señalar que un portal cautivo es una página web que se muestra antes de otorgar acceso a una red. Se usa en redes Wi-Fi públicas para autenticar usuarios, recolectar datos o mostrar términos de uso, asegurando así un acceso controlado.

2.2. Funcionalidad.

Un portal cautivo es un mecanismo de seguridad de red que requiere que los usuarios se autentiquen o acepten términos y condiciones antes de obtener acceso completo a la red. Su función es asegurar la red, proporcionar información a los usuarios y controlar el tráfico de la red inalámbrica (Ayala, 2024).

2.2.1. Autenticación.

Ruiz y Rodríguez (2024), al referirse a autenticación de un portal cautivo señalan: la autenticación de un portal cautivo es un mecanismo de seguridad

que requiere que los usuarios se identifiquen y autentiquen antes de poder acceder a una red inalámbrica. Esto permite controlar y monitorear el acceso a la red, brindando mayor seguridad y gestión del tráfico de datos.

Ahora bien, la autenticación en un portal cautivo es el proceso mediante el cual se verifica la identidad de un usuario antes de permitirle acceso a la red. Los usuarios deben ingresar credenciales, como nombre de usuario y contraseña, o aceptar términos de uso. Esto asegura que solo usuarios autorizados puedan acceder a la red.

2.2.2. Aceptación de términos.

La aceptación de términos en un portal cautivo es el proceso en el que los usuarios aceptan las condiciones de uso de una red inalámbrica, incluyendo políticas de privacidad y seguridad, antes de poder acceder a la red. Esto asegura que los usuarios entiendan y acepten las reglas del servicio, mejorando la seguridad y la gestión del tráfico de datos (Ruiz y Rodríguez, 2024).

2.3. Usos.

Zamora et al., (2020), manifiestan que un portal cautivo es una herramienta efectiva para controlar el acceso a una red LAN. Permite autenticar usuarios, aplicar políticas de seguridad y recopilar datos de uso. Algunos usos comunes incluyen: a) Restringir el acceso a usuarios no autorizados, b) Redirigir

a los usuarios a una página web específica al conectarse, c) Solicitar credenciales de usuario para autenticar el acceso, d) Aplicar políticas de ancho de banda y uso según el perfil del usuario, e) Recopilar datos de uso y estadísticas de los usuarios conectados.

2.4. Implementación.

Como lo manifiesta León (2021), la implementación de un portal cautivo consiste en configurar un sistema que gestione y controle el acceso a una red inalámbrica. Al conectarse a la red, los usuarios son redirigidos automáticamente a una página de inicio de sesión, donde deben introducir credenciales específicas, como un nombre de usuario y una contraseña, o simplemente aceptar términos de uso.

Este sistema permite administrar el ancho de banda disponible, el tiempo de conexión y asegurar que solo usuarios autorizados accedan a la red. Es especialmente útil en entornos como hoteles, universidades y otros lugares públicos donde se necesita controlar y monitorear el acceso a Internet.

El portal cautivo funciona interceptando la primera solicitud web de un usuario y redirigiéndola a una página de autenticación. Una vez que el usuario ingresa las credenciales necesarias, el sistema las verifica con una base de datos y, si son correctas, permite el acceso a la red.

Esto no solo mejora la seguridad de la red al restringir el acceso, sino que también permite recopilar datos de los usuarios y gestionar el uso del servicio de Internet. Este método es compatible con la mayoría de los dispositivos y sistemas operativos, y no requiere la instalación de software adicional por parte del usuario (León, 2021).

2.5. Beneficios.

Para Romo (2022), un portal cautivo permite controlar el acceso de usuarios a la red inalámbrica, brindando seguridad y evitando el uso no autorizado. Además, el portal cautivo permite recopilar datos de los usuarios que acceden, lo cual facilita el análisis de tráfico y comportamiento en la red.

Siendo las cosas así, un portal cautivo en una red LAN ofrece varios beneficios: mejora la seguridad al controlar el acceso de usuarios, permite la autenticación y autorización personalizada, facilita el monitoreo y la gestión del tráfico de la red, y puede ofrecer oportunidades de marketing al mostrar anuncios o información relevante a los usuarios que se conectan (Romo, 2022).

2.6. Consideraciones legales.

Según Lanchipa (2021), al implementar un portal cautivo en una red LAN, es esencial considerar la privacidad de los datos, cumplir con las leyes de protección de datos locales, obtener el consentimiento explícito de los usuarios,

y proporcionar términos de uso claros. Además, se debe garantizar la seguridad de la información recopilada.

En otras palabras, al implementar un portal cautivo en una red LAN, se debe garantizar el cumplimiento de leyes de privacidad y protección de datos. Es crucial obtener el consentimiento informado de los usuarios, ofrecer términos de uso detallados, y asegurar la seguridad de la información recopilada para evitar vulneraciones legales (Lanchipa, 2021).

2.7. Ejemplos de uso.

Esquivel (2020), un portal cautivo es un sistema que controla y administra el acceso a una red inalámbrica. Algunos ejemplos de uso incluyen: control de acceso a redes Wi-Fi públicas en hoteles, aeropuertos o cafeterías, autenticación de usuarios en redes universitarias o empresariales, monitoreo y registro del uso de la red para fines de seguridad o facturación.

Siendo las cosas así, los portales cautivos se utilizan en entornos como cafeterías, aeropuertos y hoteles para proporcionar acceso a internet. También son comunes en universidades para autenticar estudiantes y en empresas para controlar el acceso de empleados y visitantes, garantizando así la seguridad de la red y ofreciendo contenido personalizado.

3. TRANSMISION DE INFORMACIÓN.

Para Delgado (2021), la transmisión de información en una red LAN (Red de Área Local) permite a los dispositivos conectados compartir datos y recursos. Utilizar protocolos de comunicación como Ethernet y estándares como IEEE 802.11 para asegurar la integridad y seguridad de la información.

En este contexto se manifiesta que la transmisión de información en una red LAN (Red de Área Local) implica el intercambio de datos entre dispositivos conectados dentro de un área geográfica limitada, utilizando cables Ethernet o conexiones inalámbricas, para facilitar la comunicación y el acceso compartido a recursos y servicios.

3.1. Medios de Transmisión

3.1.1. Cables Ethernet

Para Peña (2021), los cables Ethernet son un tipo de cableado utilizado para conectar dispositivos, como computadoras y routers, a través de una red local (LAN). Estos cables permiten la transmisión de datos a velocidades relativamente altas y son esenciales para la comunicación en redes de computadoras.

En este mixto contexto, los cables Ethernet son conductores utilizados para conectar dispositivos en redes de área local (LAN). Facilitan la transmisión

de datos a alta velocidad y fiabilidad, empleando pares trenzados de cobre o fibra óptica, esenciales para la comunicación y acceso a redes.

3.1.2. Wi-Fi

WiFi es una tecnología que permite la conexión inalámbrica de dispositivos a una red local (LAN) y a Internet, utilizando ondas de radio. Facilita la transmisión de datos sin necesidad de cables, proporcionando movilidad y acceso compartido a recursos en diversos entornos (Peña, 2021).

Ahora bien, Salinas (2021), señala que WiFi (Wireless Fidelity) es un sistema de comunicación inalámbrica que permite a los dispositivos electrónicos (como computadoras, teléfonos móviles, mesas, etc.) conectar a Internet o a una red local sin cables.

3.2. Protocolos de Comunicación

3.2.1. Ethernet

Según Murillo y Rey (2020), el protocolo Ethernet es un estándar fundamental para la comunicación en redes de área local (LAN). Ethernet define cómo los dispositivos en una red deben formatear y transmitir datos para garantizar que las comunicaciones sean eficientes y sin errores. Utiliza un esquema de direccionamiento único conocido como dirección MAC (Media

Access Control) para identificar cada dispositivo en la red, lo que facilita el enrutamiento preciso de la información.

Además, el protocolo Ethernet especifica varios métodos de acceso al medio, siendo el más común el CSMA/CD (Carrier Sense Multiple Access with Collision Detection), que permite a los dispositivos detectar si el canal de comunicación está libre antes de enviar datos y manejar colisiones si ocurren. Ethernet soporta diferentes velocidades de transmisión, desde 10 Mbps (Ethernet clásica) hasta 100 Gbps y más (Ethernet de alta velocidad), utilizando tanto cables de cobre (pares trenzados) como fibra óptica (Murillo y Rey, 2020).

3.2.1. Wi-Fi (802.11)

Para Szott et al. (2022), El protocolo WiFi 802.11 es un estándar de comunicación inalámbrica para redes locales, desarrollado por IEEE. Permite la conexión de dispositivos sin cables, utilizando ondas de radio. Sus diversas versiones mejoran la velocidad, cobertura y seguridad de las transmisiones.

WiFi 802.11 opera en bandas de 2.4 GHz y 5 GHz, ofreciendo flexibilidad en la conexión. Las versiones más recientes, como 802.11ac y 802.11ax, aumentan la eficiencia y capacidad de la red, soportando más dispositivos simultáneamente y mayores velocidades (Szott et al., 2022).

3.3. Topologías de Red

Leone (2020), señala: la topología de una red se refiere a la disposición física o lógica de los nodos y conexiones en una red de computadoras. Define cómo se conectan los dispositivos entre sí y cómo se comunican, afectando el rendimiento y la eficiencia de la red .

3.3.1. Estrella

Para Leone (2020), la topología estrella conecta todos los nodos de una red a un dispositivo central, como un switch o un hub. Cada dispositivo tiene un enlace directo al nodo central, lo que facilita la gestión y el aislamiento de fallos en la red.

En la topología estrella, si una conexión individual falla, no afecta a los demás dispositivos de la red. Esta configuración es común en redes LAN debido a su simplicidad y eficiencia en la administración del tráfico de datos, aunque depende de la fiabilidad del nodo central (Leone, 2020).

3.3.2. Bus

Señalando a Leone (2020), la topología bus conecta todos los dispositivos de la red a un solo cable central, conocido como "bus". Los datos se transmiten

en ambas direcciones a lo largo del bus y cada dispositivo escucha el tráfico, capturando los datos dirigidos a él y descartando el resto.

En esta configuración, si el cable central falla, toda la red se desconecta. La topología bus es fácil de implementar y económica, pero su eficiencia disminuye a medida que aumenta el número de dispositivos, ya que todos comparten el mismo canal de comunicación, lo que puede provocar colisiones de datos (Leone, 2020).

3.3.3. Anillo

Para Atoche (2021), la topología de red en anillo conecta cada dispositivo con dos dispositivos vecinos, formando un circuito cerrado. Esta estructura asegura que los datos circulen en una dirección, evitando colisiones. Si un enlace falla, los datos pueden redirigirse en sentido contrario, mejorando la resiliencia de la red.

En una red de topología en anillo, cada dispositivo actúa como repetidor, amplificando la señal antes de pasarla al siguiente dispositivo. Esto permite mantener una alta calidad de transmisión en largas distancias. Sin embargo, la configuración y el mantenimiento pueden ser complejos y costosos (Atoche, 2021).

3.3.4. Malla

Según Leone (2020), en una red de topología en malla, cada nodo se conecta directamente a varios otros nodos, formando una red interconectada. Esta configuración permite múltiples rutas para los datos, mejorando la redundancia y la resistencia a fallos. Si una conexión falla, los datos pueden redirigirse por otro camino.

La topología en malla es ideal para redes que requieren alta disponibilidad y confiabilidad, como las redes de telecomunicaciones y las redes militares. Sin embargo, puede ser costosa y compleja de implementar debido al gran número de conexiones necesarias para asegurar la interconexión completa (Atoche, 2021).

3.4. Direccionamiento

3.4.1. Direcciones MAC

Las direcciones MAC (Media Access Control) son identificadores únicos asignados a las tarjetas de interfaz de red (NIC) de cada dispositivo en una red. Estas direcciones, codificadas en la capa de enlace de datos del modelo OSI, permiten la correcta transmisión de datos entre dispositivos, asegurando que la información llegue al destino correcto sin errores (Obando, 2022).

Las direcciones MAC son identificadores únicos asignados a dispositivos de red, permitiendo la correcta comunicación entre ellos al asegurar que los datos lleguen al destinatario sin errores en la transmisión.

3.4.2. Direcciones IP

Para Obando (2022), las direcciones IP (Protocolo de Internet) son identificadores únicos asignados a cada dispositivo en una red para permitir su identificación y localización. Estas direcciones son esenciales para la comunicación entre dispositivos en una red, facilitando el enrutamiento de datos y permitiendo que los dispositivos se conecten y se comuniquen correctamente.

En otras palabras, una dirección IP es un número único asignado a cada dispositivo en una red, permitiendo su identificación y localización para asegurar la correcta entrega de datos entre dispositivos.

Las direcciones IP se dividen en dos versiones principales: IPv4 e IPv6.

Ejemplos de direcciones IPv4:

192.168.1.1

10.0.0.1

172.16.254.1

Ejemplos de direcciones IPv6:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

fe80:0000:0000:0000:0202:b3ff:fe1e:8329

2001:0db8:0000:0042:0000:8a2e:0370:7334

Las direcciones IPv4 tienen un formato de cuatro octetos separados por puntos, mientras que las direcciones IPv6 utilizan un formato hexadecimal separado por dos puntos (Obando, 2022).

3.5. Transmisión de Datos

3.5.1. Paquetes

Para Garcia (2023), un paquete de datos es una unidad de información que se envía a través de una red. Cada paquete contiene datos y metadatos que indican su origen, destino y otros aspectos necesarios para la correcta transmisión y recepción.

Por otra parte, considerando a Obando (2022), un paquete de datos es una unidad de información transmitida en una red. Está compuesto por un encabezado y una carga útil. El encabezado contiene información de control, como direcciones de origen y destino, mientras que la carga útil contiene los datos reales. Los paquetes permiten la fragmentación y reensamblaje de datos, facilitando una transmisión eficiente y segura.

3.5.2. Switches y Routers

Según Salsabila y Sutabri (2024), un switch es un dispositivo de red que conecta múltiples dispositivos dentro de una red local (LAN). Opera en la capa 2

del modelo OSI, utilizando direcciones MAC para dirigir el tráfico de datos de manera eficiente y evitar colisiones, mejorando así el rendimiento y la velocidad de la red.

Se puede considerar también, que un switch es un equipo de red que enlaza varios dispositivos en una red local (LAN). Funciona en la segunda capa del modelo OSI, usando direcciones MAC para gestionar el tráfico de datos, encaminándolos de manera precisa y evitando interferencias, lo que optimiza la velocidad y eficiencia de la red (Salsabila y Sutabri, 2024).

3.5.3. Fragmentación y Reensamblaje

Considerando a Bonilla y Jairo (2023), fragmentación y reensamblaje son conceptos fundamentales en la transmisión de datos en redes. La fragmentación se refiere al proceso de dividir un paquete de datos en partes más pequeñas para facilitar su envío a través de una red, especialmente cuando el tamaño del paquete excede el límite permitido por el protocolo de red.

Por otra parte, el reensamblaje es el proceso inverso, donde estas partes se vuelven a unir en el destino para reconstruir el paquete original. Este mecanismo es esencial para garantizar la integridad y la eficiencia en la comunicación de datos en entornos de red complejos.

3.6. Velocidad de Transmisión

3.6.1. Ancho de Banda

Para Flores y Guzmán (2023), el ancho de banda se refiere a la cantidad de datos que se pueden transmitir a través de una red en un período específico. Es un factor crucial en la eficiencia de las comunicaciones digitales, ya que determina la velocidad y capacidad de transmisión de información.

Siguiendo este orden de ideas, un mayor ancho de banda permite transferencias más rápidas y simultáneas de datos, mejorando la experiencia del usuario en aplicaciones como streaming, videoconferencias y descargas. Optimizar el uso del ancho de banda es esencial para garantizar la confiabilidad y eficiencia de las redes (Flores y Guzmán, 2023).

3.6.2. Latencia

Para Castillo (2023), la latencia en la transmisión de datos se refiere al tiempo de retraso que se produce al enviar información desde un punto hasta otro en una red. Este retardo puede deberse a factores como la demora en las líneas de transmisión, el procesamiento de datos y el buffering de paquetes en las colas de tráfico .

Con las consideraciones antes mencionadas, la latencia en la transmisión de datos es el retraso temporal que ocurre cuando se envía información a través

de una red, influenciado por la distancia y el procesamiento en cada nodo (Castillo, 2023).

3.6.3. Jitter

Según Castillo (2023), un jitter es “el fenómeno causado por un retardo o latencia que varía entre los paquetes en una comunicación. Esta variabilidad provoca que los paquetes lleguen de manera desordenada, creando lagunas en la secuencia de tramas de la conversación” (p.17).

Ahora bien, el jitter en la transmisión de datos es la fluctuación en los intervalos de llegada de paquetes de datos. Esta variabilidad puede causar problemas en aplicaciones sensibles al tiempo, como la voz y el video en tiempo real, ya que los datos pueden llegar desordenados o con retrasos, afectando la calidad del servicio.

3.7. Seguridad

3.7.1. Firewalls

Viteri y Ávila (2023) manifiestan que “los firewalls actúan como una primera línea de defensa, filtrando el tráfico no autorizado y protegiendo la infraestructura de red contra intrusiones” (p.17).

Por otra parte, Viteri y Ávila (2023), señalan que los firewalls “establecen barreras de protección, controlan el tráfico y bloquean accesos no autorizados” (p.20). Los firewalls son sistemas de seguridad que controlan y filtran el tráfico de red, protegiendo contra accesos no autorizados y ciberataques.

3.7.2. Encriptación

La encriptación de datos en la transmisión de información es el proceso de codificar datos para protegerlos de accesos no autorizados durante su transferencia. Esto se corrobora con lo manifestado por Santillán (2023), al decir:

> “los protocolos WPA y WPA2 utilizan encriptación para proteger la confidencialidad de los datos transmitidos en redes inalámbricas. Se exploran los algoritmos de encriptación, como AES (Advanced Encryption Standard), y se analizan los posibles ataques criptográficos que podrían afectar la seguridad de los dispositivos móviles” (p. 12).

En otras palabras, la encriptación de datos es el proceso de convertir información legible en un código complicado. Esto asegura que solo las partes autorizadas puedan descifrar y acceder a los datos protegidos durante su almacenamiento o transmisión.

3.7.3. Autenticación

Para Insaurralde et al. (2023), la autenticación es un proceso que verifica la identidad de un usuario, máquina o servicio. Utiliza herramientas como

Kerberos, que emplea un sistema de tickets para validar usuarios en redes inseguras, asegurando que las contraseñas no se envíen ni almacenen localmente, y emplea criptografía de clave simétrica para mayor seguridad.

Así mismo, Insaurralde et al. (2023), señalan: que la autenticación de datos en una red verifica la identidad de usuarios, máquinas o servicios antes de permitir el acceso. Utiliza protocolos como Kerberos, que emplea tickets para validar usuarios, asegurando que las contraseñas no se envíen ni almacenen localmente.

3.8. Control de Acceso

3.8.1. Listas de Control de Acceso (ACLs)

Para García y Moreno (2021). “Las listas de control de acceso (ACL) son un tipo de control que ayuda a definir permisos o accesos según las políticas de seguridad establecidas por la organización y gestionadas por el administrador de la red de comunicaciones” (p. 12).

En otras palabras, las listas de control son herramientas utilizadas para mejorar la seguridad y eficiencia en diversos contextos, permitiendo verificar, organizar y priorizar tareas, procesos o elementos según criterios específicos y establecidos previamente (García y Moreno, 2021).

3.8.2. VLANs

Las VLAN (Redes de Área Local Virtual) permiten segmentar una red física en redes lógicas distintas, mejorando la seguridad, eficiencia y gestión del tráfico. Facilitan el aislamiento de segmentos de red, reduciendo colisiones y permitiendo una administración flexible sin cambios físicos en la infraestructura (Garcia y Moreno, 2021).

Esto se corrobora por lo manifestado por Almalki (2020), al decir, las VLAN (Virtual Local Area Network) permiten segmentar una red física en varias redes lógicas, mejorando la seguridad y la eficiencia. Facilitan la gestión y el control del tráfico de datos sin necesidad de cambios físicos en la infraestructura de red.

3.9. QoS (Quality of Service)

3.9.1. Priorización de Tráfico

Para Mejía et al. (2022), la priorización de tráfico es una técnica utilizada para gestionar el flujo de datos en una red. Permite identificar y clasificar los paquetes según criterios como la tasa de transferencia, el retraso (delay), la variación del retraso (jitter) y la pérdida de paquetes. Esto asegura que los servicios críticos, como VoIP y videoconferencias, tengan una mayor calidad y estabilidad en la red.

Esta gestión se logra mediante diferentes mecanismos, como el balanceo de carga y la asignación de ancho de banda prioritario a ciertos tipos de tráfico o usuarios específicos. Implementar estas técnicas optimiza el uso de los recursos de red, mejorando la eficiencia y reduciendo los costos asociados a la contratación de planes de mayor ancho de banda (Mejía et al., 2022).

3.9.2. Gestión del Ancho de Banda

Según Mejía et al.,(2022), la gestión del ancho de banda es una técnica utilizada para controlar y optimizar el uso de la capacidad de una red. Consiste en monitorear y administrar la cantidad de datos que pueden transmitirse a través de una red en un tiempo determinado, generalmente medido en bits por segundo (bps).

Este control es crucial para evitar la congestión y garantizar que los servicios críticos tengan suficiente ancho de banda para operar de manera eficiente. A través de la gestión del ancho de banda, se puede asignar prioridades a diferentes tipos de tráfico, asegurando que las aplicaciones esenciales, como videoconferencias o VoIP, reciban un tratamiento preferente en la red (Mejía et al., 2022).

3.10. Monitoreo y Administración

3.10.1. SNMP (Simple Network Management Protocol)

Según Gobantes (2023), SNMP (Simple Network Management Protocol) es un protocolo de gestión de red que permite a los administradores monitorizar y controlar remotamente dispositivos de red. Utiliza una arquitectura de gestión que incluye agentes SNMP en los dispositivos gestionados y gestores SNMP que recopilan información de los agentes.

Los agentes exponen datos de gestión a través de objetos definidos en bases de información de gestión (MIB). SNMP proporciona un marco estandarizado para la gestión de redes heterogéneas (Gobantes, 2023).

3.10.2. Herramientas de Monitoreo

Gobantes (2023), señala que las herramientas de monitoreo son fundamentales para la gestión eficiente de redes. Permiten a los administradores obtener información esencial para medir, mantener y mejorar los sistemas y procesos distribuidos que conforman las redes.

Proporcionan una visión integral de los aspectos relevantes, creando una base sólida para la toma de decisiones informadas y la optimización continua de las redes. Su uso estratégico garantiza un funcionamiento óptimo y mayor eficiencia en la gestión de redes (Gobantes, 2023).

CAPITULO II

ESTUDIO DE CAMPO

1. **PARADIGMA DE LA INVESTIGACIÓN CUALITATIVO.**

Para Centeno y Acuña (2023), el paradigma cualitativo se enfoca en comprender fenómenos sociales y educativos desde la perspectiva de los participantes. Utiliza métodos como entrevistas y grupos de discusión para recolectar datos ricos en detalle y contexto. En este enfoque, se busca interpretar y analizar los significados y experiencias de las personas, proporcionando una comprensión profunda y holística de la realidad estudiada.

En la presente investigación se empleó el paradigma cualitativo, al aplicar entrevistas a profesionales con bastos conocimientos en aplicaciones informáticas, que están vinculadas a una red LAN con portal cautivo, que sirven para la transmisión de datos.

2. TIPO DE INVESTIGACIÓN

2.1. Investigación documental

Según Reyes y Carmona (2020), al referirse a investigación documental señalan:

> “La investigación documental es una de las técnicas de la investigación cualitativa que se encarga de recolectar, recopilar y seleccionar información de las lecturas de documentos, revistas,

> libros, grabaciones, filmaciones, periódicos, artículos resultados de investigaciones, memorias de eventos, entre otros” (p.1).

En la presente investigación se utilizó la investigación documental para revisar, analizar y describir cada una de las partes, componentes y software que se utiliza en una red LAN con portal cautivo para la transmisión de información.

Por otra parte, Reyes y Carmona (2020) manifiestan que “con la investigación documental, también es posible hacer una reflexión de todos aquellos aspectos que hacen alusión a instrumentos para evaluar las categorías de análisis que se estén trabajando” (p. 1).

2.2. Investigación de campo

Para Sandoval (2022), la investigación de campo es una fase crucial en la investigación social, que implica una interacción directa con los actores sociales en sus entornos naturales. Permite al investigador recopilar información primaria, comprender las realidades sociales, económicas, culturales y políticas, y analizar percepciones y dinámicas. Este proceso fomenta la empatía y la confianza con las comunidades, y puede ser complementado con el uso de herramientas tecnológicas para organizar y analizar los datos recolectados.

En la presente investigación, se acudió directamente a la Unidad Educativa Fiscomisional "Juan Pablo II" para dialogar con las autoridades y docentes que conocen la realidad sobre la infraestructura tecnológica existente,

y sobre cada uno de los aspectos que encierran la transmisión de información. Esto permitió recopilar datos para el desarrollo de la presente investigación.

3. MÉTODOS DE INVESTIGACIÓN

3.1. Método analítico – sintético

Tomando el criterio de Falcón y Serpa (2021), el “método analítico-sintético procesa y valora los diversos puntos de vista que sobre la variedad de métodos de investigación existen, así como para establecer las coincidencias, aspectos cuestionables o rescatables en cada caso” (p.23).

Por otra parte, Falcón y Serpa señalan: “el método analítico-sintético parte de entender el análisis como el procedimiento mental que descompone lo complejo en sus partes y cualidades, permitiendo la división mental del todo en sus múltiples relaciones” (p. 24).

Siendo las cosas así, en la presente investigación el método analítico-sintético implicó descomponer el sistema en componentes básicos de la red LAN (análisis), como dispositivos y conexiones, para luego integrar estos elementos (síntesis) en una red funcional y eficiente, optimizando su rendimiento y seguridad.

3.2. Método deductivo – inductivo

Según lo manifestado por Almeida (2022), el método inductivo-deductivo es una estrategia de razonamiento que combina la inducción y la deducción. La inducción parte de casos particulares para llegar a una conclusión general, mientras que la deducción aplica principios generales a casos específicos. Este método permite analizar un fenómeno desde diferentes perspectivas, formulando hipótesis y verificándolas para obtener conocimiento científico.

Ahora bien, en la presente investigación se aplicó el método inductivo-deductivo para el diseño de una red LAN con portal cautivo, recopilando datos sobre redes existentes (inductivo) para identificar patrones de uso y necesidades específicas. Luego, se formuló una hipótesis sobre la configuración óptima de la red. Finalmente, se diseñó la red y se evaluó su rendimiento, ajustando según los resultados obtenidos (deductivo).

4. TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

4.1. Técnicas de investigación

Las técnicas de investigación son métodos sistemáticos utilizados para recolectar, analizar e interpretar datos. Incluyen encuestas, entrevistas, observación, estudios de caso, experimentos y análisis documental. Cada técnica se elige según los objetivos del estudio y el tipo de información que se necesita, permitiendo obtener resultados válidos y fiables (Tajero, 2021).

4.1.1. Entrevista

Se destaca lo manifestado por Lopezosa (2020), al referirse a lo que es una entrevista:

> La entrevista es un instrumento de gran eficacia para desarrollar investigaciones cualitativas y tiene como función principal recabar datos que después podremos aplicar a nuestros estudios. Se trata de una técnica que se caracteriza por tratarse de una conversación más o menos dirigida (dependiente del tipo de entrevista) entre el investigador (emisor) y el sujeto de estudio (receptor) con un fin siempre bien determinado y enfocado a la resolución de los objetivos y preguntas de investigación de trabajos (p. 89).

Siguiendo este orden de ideas, una entrevista en una investigación es un método cualitativo que consiste en una conversación estructurada o semiestructurada entre el investigador y el participante. Su objetivo es obtener información profunda sobre experiencias, opiniones y percepciones, enriqueciendo así el análisis del tema estudiado (Lopezosa, 2020).

En la presente investigación, se usó la entrevista para obtener información de los docentes, que tienen cargo administrativo y bastos conocimientos en infraestructura tecnológica.

4.1.2. Observación de campo

Según Vega et al. (2021), uno de los métodos más usados en la investigación en las ciencias sociales es la observación, sin embargo, se la usa en otras áreas del conocimiento, “el cual pareciera ser muy simple; sin embargo,

su exigencia es basta, pues requiere de habilidades y destrezas exigentes para el observador, toda vez que de ellas dependen resultados fidedignos y precisos” (p. 71).

La observación de campo sirvió para verificar la existencia y el estado de la infraestructura tecnológica de la Unidad Educativa Fiscomisional "Juan Pablo II". Siendo de mucha ayuda para el desarrollo de la presente investigación.

4.2. Instrumentos de investigación

4.2.1. Guía de entrevista

En relación con el término guía de entrevista, Ávila et al. (2020), lo consideran como:

> “el instrumento metodológico que permite la aplicación del método en la práctica. Es frecuente obviar el hecho de que, lo que se aplica en la práctica directamente, no es el método, como abstracción teórica, sino su guía, por su carácter metodológico” (p. 69).

Cabe considerar, que la guía de la entrevista es un documento que contiene las preguntas o temas a abordar durante la entrevista de investigación. Sirve como una estructura flexible que permite al entrevistador cubrir los puntos clave, adaptándose a las respuestas del participante y profundizando en aspectos relevantes que surjan durante la conversación.

En la presente investigación la guía de la entrevista sirvió para obtener datos de los entrevistados con relación del diseño de la red LAN con portal cautivo para la Unidad Educativa Fiscomisional “Juan Pablo II”.

4.2.2. Ficha de observación

Al hablar de la ficha de observación Román et al. (2021), manifiestan: la ficha de observación en una investigación es un instrumento que permite recoger datos de forma sistemática y estructurada sobre un fenómeno específico. Su diseño incluye categorías y variables relevantes que guían la observación, facilitando la recolección de información cualitativa y cuantitativa. Este recurso es esencial para analizar el contexto y las dinámicas observadas, contribuyendo a la validez y confiabilidad de los hallazgos en estudios educativos y sociales.

La guía de la observación se empleó en la presente investigación para colectar datos de las instalaciones, laboratorio, áreas de recreación, áreas administrativas, entre otros lugares, para la implementación de la red LAN con portal cautivo, para la transmisión de información en la Unidad Educativa Fiscomisional “Juan Pablo II”.

5. POBLACIÓN Y MUESTRA

5.1. Población

Mucha et al. (2021) al referirse a la población en una investigación señalan:

> La determinación de la población y la muestra, parte del tipo de investigación que se aplica para enfrentarse a la realidad problemática, por ello es importante dar una mirada al enfoque de los tipos de investigación, según la naturaleza de las variables (p. 51).

Por otra parte, Mucha et al. (2021), manifiestan que el investigador debe considerar que la población sea relativamente homogénea respecto de las variables de su interés.

En la presente investigación se utilizó una población de 30 docentes, que trabajan en la Unidad Educativa Fiscomisional “Juan Pablo II”, y tienen conocimientos del uso de infraestructura tecnológica.

5.2. Muestra

Sodeify y Habibpour (2021), en una investigación cualitativa, el número mínimo de entrevistados puede variar dependiendo del enfoque y los objetivos del estudio. Sin embargo, generalmente se recomienda entrevistar al menos a 5 a 10 personas para obtener una variedad suficiente de perspectivas. Algunos estudios pueden necesitar más participantes para alcanzar la saturación de datos, donde la información adicional ya no aporta nuevos insights significativos. Es crucial que la muestra sea lo suficientemente diversa para cubrir los diferentes aspectos del fenómeno investigado.

En este contexto, el muestreo intencional es una técnica de selección de participantes basada en criterios específicos y el juicio del investigador para obtener datos relevantes y significativos para el estudio (Sodeify y Habibpour, 2021).

Tomando en cuenta estas consideraciones, en la presente investigación se aplicó un muestreo intencional, donde se seleccionó a 5 docentes de la

Unidad Educativa Fiscomisional “Juan Pablo II”, que tiene bastos conocimientos en el uso de herramientas informáticas y conocen sobre infraestructura tecnológica orientada a redes LAN y portales cautivos.

6. ANÁLISIS DE RESULTADOS

6.1. Entrevista

Entrevista realizada a los 5 docentes de la Unidad Educativa Fiscomisional “Juan Pablo II”, que tiene bastos conocimientos en el uso de herramientas informáticas y conocen sobre infraestructura tecnológica orientada a redes LAN y portales cautivos.

Tabla 1: Análisis de la entrevista realizada.

No.	Pregunta	Respuestas	Análisis
1	¿Qué es un portal cautivo?	Página web de autenticación. Control de acceso a la red. Seguridad adicional para usuarios. Herramienta para gestionar conexiones. Portal para verificar identidades	Las respuestas destacan la función principal del portal cautivo: autenticar y controlar el acceso, proporcionando seguridad y gestión eficiente.

2	¿Beneficios de una red LAN en la escuela?	Mejor comunicación interna. Acceso rápido a recursos. Internet más eficiente. Apoyo en actividades educativas. Reducción de costos operativos.	Las respuestas enfatizan la eficiencia, el apoyo educativo y la reducción de costos, destacando la importancia de la red LAN en un entorno escolar.
3	¿Cómo garantiza seguridad el portal cautivo?	Filtra accesos no autorizados. Monitorea el uso de internet. Registra actividades online. Autentica usuarios. Protege contra amenazas externas.	Las respuestas subrayan la capacidad del portal cautivo para asegurar la red mediante filtrado, monitoreo y autenticación, protegiendo la integridad del sistema.
4	¿Qué equipos son necesarios para una red LAN?	Routers y switches. Puntos de acceso inalámbricos. Servidor central. Cables de red. Dispositivos finales.	Las respuestas identifican el hardware esencial para una red LAN, subrayando la infraestructura básica necesaria para su implementación y funcionamiento.

5	¿Ventajas del portal cautivo en educación?	Controla el uso de internet. Acceso supervisado a la red. Mejora la ciberseguridad. Facilita la gestión de usuarios. Optimiza el rendimiento de la red.	Las respuestas muestran cómo el portal cautivo mejora la seguridad y eficiencia de la red, facilitando la gestión y el control en un entorno educativo.
6	¿Cómo afecta el portal cautivo al rendimiento?	Gestiona el ancho de banda. Prioriza el tráfico educativo. Reduce accesos no autorizados. Controla el tiempo de conexión. Asegura una red eficiente.	Las respuestas destacan cómo el portal cautivo optimiza el uso de recursos y asegura una conexión eficiente, priorizando actividades educativas.
7	¿Pasos para implementar una red LAN?	Evaluar necesidades de red. Adquirir el hardware adecuado. Configurar equipos y software. Instalar el portal cautivo. Probar y ajustar la red.	Las respuestas detallan un proceso estructurado para la implementación de la red LAN, subrayando la importancia de una planificación y configuración adecuadas.

8	¿Retos en la implementación del portal cautivo?	Configuración inicial compleja. Necesidad de mantenimiento continuo. Problemas de compatibilidad. Capacitación del personal. Resistencia al cambio.	Las respuestas identifican desafíos técnicos y humanos, resaltando la importancia de la preparación y la adaptación para una implementación exitosa.
9	¿Cómo facilita la transmisión de información?	Asegura conectividad estable. Gestiona el acceso a recursos. Centraliza administración de red. Proporciona acceso seguro. Optimiza el ancho de banda.	Las respuestas destacan la centralización y seguridad proporcionadas por el portal cautivo, mejorando la eficiencia en la transmisión de información.
10	¿Medidas para mantener la red segura?	Actualizar software regularmente. Monitorear el tráfico de red. Establecer políticas de acceso. Implementar cortafuegos.	Las respuestas enfatizan la importancia de medidas proactivas y continuas para mantener la seguridad de la red, subrayando la

		Realizar auditorías de seguridad.	necesidad de un enfoque integral.

6.2. Observación

Observación realizada en la Unidad Educativa Fiscomisional “Juan Pablo II”, para conocer el estado de su infraestructura tecnológica.

Tabla 2: Análisis de la observación de campo realizada.

No	Pregunta	Respuesta	Análisis
1	¿Qué tipo de conexión a internet tiene la escuela?	La escuela utiliza una conexión de fibra óptica de 100 Mbps	La conexión de fibra óptica de 100 Mbps es adecuada para soportar una red LAN con portal cautivo, permitiendo una transmisión de información rápida y estable.
2	¿Cuántos routers están actualmente instalados?	Actualmente, hay dos routers instalados en la escuela.	Dos routers pueden ser suficientes para una red básica, pero puede necesitar más para cubrir todas las

			áreas con una señal fuerte y estable.
3	¿Existen puntos de acceso inalámbricos en todas las áreas clave?	Solo hay puntos de acceso inalámbricos en las áreas administrativas.	La falta de puntos de acceso en áreas clave puede limitar la conectividad y la efectividad de la red LAN en toda la escuela.
4	¿Qué tipo de switches se utilizan en la red actual?	Se utilizan switches no gestionados de 24 puertos.	Los switches no gestionados pueden ser limitantes para la configuración y el control avanzados necesarios en una red LAN con portal cautivo.
5	¿Hay un servidor central dedicado para la red?	No, actualmente no hay un servidor central dedicado.	La falta de un servidor central puede dificultar la gestión centralizada y la implementación del portal cautivo, reduciendo la

			eficiencia y seguridad de la red.
6	¿Cuántos dispositivos finales (computadoras, tabletas) se conectan a la red?	Aproximadamente 50 dispositivos se conectan a la red.	Con 50 dispositivos conectados, la red debe ser robusta y bien gestionada para evitar saturaciones y asegurar un rendimiento óptimo.
7	¿Se realiza algún tipo de monitoreo de tráfico de red?	No se realiza monitoreo de tráfico de red actualmente.	La ausencia de monitoreo de tráfico limita la capacidad de detectar y solucionar problemas, así como de optimizar el rendimiento y la seguridad de la red.
8	¿Qué medidas de seguridad están implementadas en la red actual?	Solo se utilizan contraseñas básicas para el acceso.	Las contraseñas básicas son insuficientes para asegurar una red educativa, especialmente con un portal cautivo,

			exponiendo la red a posibles amenazas.
9	¿Existe un plan de mantenimiento regular para los equipos de red?	No, no hay un plan de mantenimiento regular.	La falta de un plan de mantenimiento puede resultar en un deterioro del rendimiento de la red y fallos inesperados que afectan la transmisión de información.
10	¿La infraestructura actual soporta la expansión a una red LAN completa con portal cautivo?	La infraestructura actual es insuficiente para una expansión completa.	Se necesita una actualización significativa de la infraestructura para soportar eficazmente una red LAN con portal cautivo, asegurando un rendimiento y seguridad adecuados.

6.3. Análisis de resultados

La observación de campo en la Unidad Educativa Fiscomisional "Juan Pablo II" revela una infraestructura tecnológica limitada para la implementación de una red LAN con portal cautivo. La conexión a internet es adecuada, pero la cobertura de puntos de acceso es insuficiente y falta un servidor central. Los switches no gestionados y la ausencia de monitoreo de tráfico y mantenimiento regular son puntos críticos. La seguridad es básica, lo que pone en riesgo la red. Para una expansión efectiva, se requiere una actualización significativa en equipos y prácticas de gestión para asegurar una red robusta y segura.

Con respecto a la entrevista realizada, la implementación de una red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II" ofrece múltiples beneficios y presenta ciertos desafíos. Los análisis individuales de cada pregunta y respuesta proporcionan una visión clara y detallada de los aspectos más relevantes de este proceso.

Función del Portal Cautivo: Las respuestas destacan que la principal función del portal cautivo es autenticar y controlar el acceso a la red, proporcionando una capa adicional de seguridad y una gestión eficiente de las conexiones. Esto es fundamental en un entorno educativo donde es crucial proteger la integridad de la red y garantizar que solo usuarios autorizados accedan a los recursos.

Beneficios de la red LAN: La red LAN mejora la comunicación interna, facilita el acceso rápido a recursos, optimiza el uso de internet, apoya las actividades educativas y reduce los costos operativos. Estos beneficios son esenciales para mejorar la eficiencia operativa y la calidad educativa en la institución.

Seguridad Proporcionada por el Portal Cautivo: El portal cautivo garantiza la seguridad de la red filtrando accesos no autorizados, monitoreando el uso de internet, registrando actividades online, autenticando usuarios y protegiendo contra amenazas externas. Esto asegura que la red se mantenga segura y confiable.

Equipos Necesarios para la red LAN: Los equipos esenciales incluyen routers, switches, puntos de acceso inalámbricos, un servidor central, cables de red y dispositivos finales. Estos componentes son cruciales para la infraestructura básica de la red y su funcionamiento adecuado.

Ventajas en el Contexto Educativo: El portal cautivo controla el uso de internet, proporciona acceso supervisado, mejora la ciberseguridad, facilita la gestión de usuarios y optimiza el rendimiento de la red. Estas ventajas son particularmente importantes en un entorno educativo donde es necesario asegurar un uso adecuado y seguro de los recursos digitales.

Impacto en el Rendimiento de la red: El portal cautivo gestiona el ancho de banda, prioriza el tráfico educativo, reduce accesos no autorizados, controla

el tiempo de conexión y asegura una red eficiente. Esto garantiza que los recursos de la red se utilicen de manera óptima para apoyar las actividades educativas.

Proceso de Implementación: Los pasos para implementar la red LAN incluyen evaluar las necesidades de la red, adquirir el hardware adecuado, configurar equipos y software, instalar el portal cautivo y probar y ajustar la red. Este proceso estructurado es esencial para asegurar una implementación exitosa y funcional.

Retos en la Implementación: Los desafíos incluyen la configuración inicial compleja, la necesidad de mantenimiento continuo, problemas de compatibilidad, capacitación del personal y resistencia al cambio. Reconocer estos retos permite planificar estrategias efectivas para superarlos.

Facilitación de la Transmisión de Información: El portal cautivo asegura una conectividad estable, gestiona el acceso a recursos, centraliza la administración de la red, proporciona acceso seguro y optimiza el ancho de banda. Estos factores son cruciales para una transmisión eficiente de información.

Medidas de Seguridad: Mantener la red segura requiere actualizar el software regularmente, monitorear el tráfico de red, establecer políticas de acceso, implementar cortafuegos y realizar auditorías de seguridad. Estas

medidas proactivas son fundamentales para garantizar la seguridad continua de la red.

En resumen, la implementación de una red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II" ofrece importantes beneficios en términos de eficiencia, seguridad y gestión de recursos, aunque también presenta desafíos que deben ser abordados con planificación y estrategias adecuadas.

CAPITULO III

Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional "Juan Pablo II"

1. ANTECEDENTES

Con acuerdo No. 184 el 20 de septiembre de 1994, se crea el Colegio Juan Pablo II de Fe y Alegría. Con Acuerdo No. 569, se autoriza el funcionamiento del sexto curso de bachillerato Técnico en Contabilidad y Administración. Con resolución No. 217 – DIECH del 18 de febrero del 2011, se autoriza el cambio de denominación del Bachillerato Técnico en Comercio y Administración especialidad Contabilidad y Administración por Bachiller Técnico Contador Bachiller en Ciencias de Comercio y Administración. Unidad Educativa Fiscomisional “Juan Pablo II” (UEFJII, 2024).

La Comuna Unión y Progreso - La Bramadora en los últimos años ha abierto sus puertas a una gran cantidad de personas que habitan en el mismo lugar, ofreciendo un mejor porvenir para sus familias, la mayor parte de su población es propia de la región, súmese a esta población los grupos emigrantes de otros lugares del país, personas provenientes de Esmeraldas, Loja, Manabí, Los Ríos y Guayas, entre otros (UEFJII, 2024).

Actualmente, la Unidad Educativa Fiscomisional “Juan Pablo II” ofrece básica superior, bachillerato técnico polivalente con especialidad en comercio y

administración, bachillerato con la modalidad en contabilidad y administración. Cuenta con más de 200 estudiantes y 30 profesionales, que cumplen las funciones: administrativas, docencia, psicólogo, pastorista, secretaria, colectora y un conserje (UEFJII, 2024).

La infraestructura de la Unidad Educativa Fiscomisional “Juan Pablo II” está conformada por 10 aulas de clases, laboratorio de química, informática, oficinas administrativas, áreas verdes, canchas deportivas, bar, entre otras áreas (UEFJII, 2024).

El laboratorio de informática tiene 24 computadoras operativas, con servicio de internet. En las oficinas administrativas se cuenta con computadoras, impresoras, internet, entre otros equipos informáticos, se tiene wifi para la conectividad de los estudiantes, personal administrativo y docentes (UEFJII, 2024).

Figura 1: Fachada principal de la Unidad Educativa “Juan Pablo II”

Fuente: Erick Rodríguez (2024)

Figura 2: Patio principal de la Unidad Educativa “Juan Pablo II”

Fuente: Erick Rodríguez (2024)

Figura 3: Área de recreación de la Unidad Educativa “Juan Pablo II”

Fuente: Erick Rodríguez (2024)

2. INTRODUCCIÓN

Una red LAN en una unidad educativa es esencial para mejorar la conectividad, facilitar el acceso a recursos digitales, y optimizar la comunicación interna. Esta infraestructura tecnológica apoya las actividades educativas, promueve la colaboración y asegura un entorno de aprendizaje moderno y eficiente, beneficiando a estudiantes y docentes (Acán et al. 2023).

Para Morales y Zambrano (2023), implementar un portal cautivo en una red LAN es crucial para controlar el acceso a la red, asegurar la autenticación de usuarios y proteger contra amenazas. Mejora la gestión de recursos, facilita el monitoreo del tráfico y garantiza un uso adecuado de internet, optimizando la seguridad y eficiencia de la red.

En este contexto, un portal cautivo mejora la transmisión de información al asegurar que solo usuarios autorizados accedan a la red, optimizando el uso del ancho de banda. Esto reduce la congestión y mejora la velocidad y estabilidad de la conexión, asegurando una comunicación más eficiente y segura dentro de la red (Ruiz y Rodríguez, 2024).

Con los antecedentes antes expuestos, la Unidad Educativa Fiscomisional “Juan Pablo II”, requiere implementar una red LAN con portal cautivo para la transmisión de información. De esta manera mejora el servicio de internet que utiliza toda la comunidad educativa.

3. METODOLOGÍA

3.1. Metodología de desarrollo PPDIOO de Cisco

Para Criollo (2022), la metodología PPDIOO de Cisco consiste en un ciclo de vida continuo para el diseño y la implementación de redes. Sus fases son: Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. Cada fase aborda aspectos específicos desde la definición de requisitos hasta la gestión proactiva de la red, con el objetivo de mejorar la disponibilidad, fiabilidad y escalabilidad de la infraestructura de red.

Ahora bien, basada en la metodología PPDIOO de Cisco, se detalla a continuación cada una de las etapas con su análisis para crear la red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional “Juan Pablo II”, basado en (Criollo, 2022).

3.1.1. Etapa preparar

Objetivo: Definir los requerimientos iniciales y preparar el entorno para el diseño de la red.

Evaluación de necesidades:

- Identificar los requerimientos de la Unidad Educativa en términos de conectividad y seguridad.
- Determinar el número de usuarios, dispositivos y áreas a cubrir con la red LAN.

- Especificar los requerimientos del portal cautivo para la transmisión de información.

Análisis del entorno actual:

- Revisar la infraestructura existente, como el estado del cableado, la disponibilidad de espacio para equipos y la infraestructura eléctrica.
- Evaluar la cobertura de red y las zonas muertas.

Recolección de información:

- Recolectar datos sobre el tráfico esperado, tipos de aplicaciones y servicios que se utilizarán en la red.
- Considerar los requisitos de ancho de banda y calidad de servicio (QoS).

3.1.2. Etapa Planear

Objetivo: Desarrollar un plan detallado para el diseño y la implementación de la red.

Diseño de alto nivel:

- Definir la topología de la red LAN, incluyendo la distribución de puntos de acceso y switches.
- Decidir la ubicación del portal cautivo y la distribución de SSID.

Especificación de hardware y software:

- Seleccionar los dispositivos de red adecuados (switches, routers, puntos de acceso, servidores) y el software necesario para el portal cautivo.

- Planificar la adquisición de licencias y componentes adicionales.

Plan de seguridad:

- Desarrollar políticas de seguridad para el acceso a la red y el uso del portal cautivo.
- Incluir medidas de autenticación, autorización y auditoría.

Plan de implementación:

- Elaborar un cronograma detallado para la instalación y configuración de la red.
- Establecer puntos de control y fases del proyecto.

3.1.3. Etapa Diseñar

Objetivo: Crear un diseño detallado y específico de la red.

Diagramas de red:

- Crear diagramas detallados de la red, mostrando la ubicación exacta de todos los dispositivos y conexiones.
- Incluir diagramas de flujo para el portal cautivo.

Configuraciones de dispositivos:

- Documentar las configuraciones de todos los dispositivos de red, incluyendo direcciones IP, VLANs, configuraciones de SSID y parámetros del portal cautivo.
- Especificar las configuraciones de QoS y políticas de seguridad.

Pruebas de diseño:

- Planificar y documentar las pruebas que se realizarán para asegurar que el diseño cumple con los requisitos.
- Incluir pruebas de rendimiento y seguridad.

3.1.4. Etapa Implementar

Objetivo: Instalar y configurar la red según el diseño especificado.

Despliegue de hardware:

- Instalar los switches, routers y puntos de acceso según el plan.
- Realizar el cableado necesario y asegurar todos los dispositivos en sus ubicaciones.

Configuración inicial:

- Configurar los dispositivos de red según la documentación de diseño.
- Configurar el portal cautivo, incluyendo las páginas de inicio de sesión y los parámetros de control de acceso.

Pruebas iniciales:

- Realizar pruebas para verificar la conectividad básica y el funcionamiento del portal cautivo.
- Asegurarse de que todas las políticas de seguridad y QoS estén funcionando correctamente.

3.1.5. Etapa Operar

Objetivo: Mantener y monitorizar la red para asegurar su funcionamiento continuo.

Monitoreo:

- Implementar herramientas de monitoreo para supervisar el rendimiento de la red y el portal cautivo.
- Configurar alertas para detectar y responder a problemas de red.

Mantenimiento:

- Programar tareas de mantenimiento regular para los dispositivos de red.
- Aplicar actualizaciones de software y firmware según sea necesario.

Soporte y documentación:

- Establecer procedimientos de soporte para los usuarios de la red.
- Mantener la documentación actualizada de todas las configuraciones y cambios en la red.

3.1.6. Etapa Optimizar

Objetivo: Mejorar continuamente la red basándose en el monitoreo y la retroalimentación.

Evaluación del rendimiento:

- Revisar periódicamente el rendimiento de la red y el portal cautivo.

- Identificar áreas de mejora en términos de velocidad, cobertura y seguridad.

Implementación de mejoras:

- Realizar ajustes en la configuración y la topología de la red según los resultados del monitoreo.
- Actualizar o reemplazar hardware y software para mejorar el rendimiento.

Capacitación continua:

- Proveer capacitación continua al personal de TI sobre las mejores prácticas y nuevas tecnologías.
- Mantener a los usuarios informados sobre las políticas de uso y seguridad de la red.

Este análisis se basa en la metodología PPDIOO de Cisco, adaptada para las necesidades específicas de la Unidad Educativa Fiscomisional "Juan Pablo II". Cabe recalcar que en la presente investigación solo cubre hasta la etapa 3 del diseño. Quedando la investigación disponible para que nuevos investigadores la puedan implementar.

4. OBJETIVOS

4.1. General

Diseñar una red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional "Juan Pablo II"

4.2. Específicos

- Definir los requerimientos iniciales y preparar el entorno para el diseño de la red de la Unidad Educativa Fiscomisional “Juan Pablo II””.
- Desarrollar un plan detallado para el diseño y la implementación de la red de la Unidad Educativa Fiscomisional “Juan Pablo II””.
- Crear un diseño detallado y específico de la red LAN de la Unidad Educativa Fiscomisional “Juan Pablo II””.

5. REQUERIMIENTOS INICIALES Y ENTORNO PARA EL DISEÑO DE LA RED DE LA UNIDAD EDUCATIVA FISCOMISIONAL “JUAN PABLO II”

5.1. Evaluación de necesidades.

5.1.1. Requerimientos de la Unidad Educativa

Para la implementación de una red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II", los requerimientos en términos de conectividad y seguridad son cruciales. A continuación, se detallan los requerimientos:

Tabla 3: Requerimientos de la Unidad Educativa

Nombre	**Descripción**
Requerimientos de Conectividad	1. Cobertura Total: 2. Capacidad y Ancho de Banda: 3. Redundancia y Fiabilidad: 4. Velocidad de Conexión:
Requerimientos de Seguridad	1. Autenticación y Control de Acceso: 2. Segmentación de la Red: 3. Encriptación de Datos: 4. Monitoreo y Detección de Intrusiones: 5. Políticas de Seguridad: 6. Copia de Seguridad y Recuperación: 7. Actualización y Mantenimiento:

Fuente: Erick Rodríguez (2024)

5.1.2. Determinar el número de usuarios, dispositivos y áreas a cubrir con la red LAN

Tabla 4: Usuarios, dispositivos y áreas a cubrir

Nombre	**Descripción**
Usuarios:	Profesionales: 30 Estudiantes: 200 Comunidad educativa: 100
Dispositivos:	2 switch gestionables 5 routers 1 servidor
Áreas para cubrir	2 oficinas centrales 10 salones de clases 1 laboratorio de computación 1 laboratorio de química 3 áreas de recreación

Fuente: Erick Rodríguez (2024)

5.1.3. Especificar los requerimientos del portal cautivo para la transmisión de información

Tabla 5: Requerimientos del portal cautivo

Nombre	**Descripción**
Requerimientos Funcionales	1. Página de Inicio de Sesión 2. Autenticación de Usuarios: 3. Control de Acceso: 4. Redirección Post-Autenticación: 5. Integración con el Sistema de Gestión de Identidades: 6. Registro y Monitoreo:
Requerimientos de Seguridad	1. Encriptación de Datos: 2. Protección contra Ataques: 3. Control de Sesiones: 4. Cumplimiento de Normativas: **5.** Auditoría y Reporting:
Requerimientos de Usabilidad	1. Diseño Adaptable: 2. Soporte y Documentación: **3.** Experiencia de Usuario:

Fuente: Erick Rodríguez (2024)

5.2. Análisis del entorno actual

Tabla 6: Análisis del entorno actual

Nombre	Descripción
Infraestructura existente	Se debe aumentar recursos en la infraestructura tecnológica.
Estado del Cableado	Se debe reemplazar el 50% del cableado existente.
Disponibilidad de espacios para equipos	Existe suficiente espacio para la implementación de nuevos equipos.
Infraestructura eléctrica	Se debe aumentar determinados puntos de electricidad, para la instalación de nuevos equipos.
Cobertura de red	Se debe implementar nuevos puntos de red, para cubrir todas las áreas.
Zonas muertas	No existe la posibilidad de zonas muertas, hay espacio adecuado para la instalación de nuevos equipos.

Fuente: Erick Rodríguez (2024)

5.3. Recolección de información

Tabla 7: Recolección de información

Nombre	Descripción
Tráfico esperado	Alto debido a autenticación y acceso continuo de usuarios.
Tipos de aplicaciones	Las aplicaciones típicas incluyen: navegación web, correos electrónicos, aplicaciones de mensajería instantánea y redes sociales. Se priorizan servicios básicos sobre protocolos específicos para gestionar el acceso y el ancho de banda eficientemente.
Servicios que se utilizarán en la red	Se utilizan servicios como autenticación de usuarios, gestión de accesos, control de ancho de banda, monitoreo de tráfico, y filtrado de contenido web para asegurar un uso adecuado y eficiente de la red.
Requisitos de ancho de banda	Los requisitos de ancho de banda dependen del número de usuarios y sus actividades. Se debe garantizar suficiente capacidad para navegación web, streaming de medios y actualizaciones, asegurando una experiencia fluida sin congestiones.
Calidad de servicios (QoS)	Se espera una QoS que garantice la autenticación eficiente de usuarios, acceso

	seguro, ancho de banda controlado, baja latencia, alta disponibilidad y gestión de tráfico priorizado para servicios críticos.

Fuente: Erick Rodríguez (2024)

6. PLAN DETALLADO PARA EL DISEÑO Y LA IMPLEMENTACIÓN DE LA RED DE LA UNIDAD EDUCATIVA FISCOMISIONAL “JUAN PABLO II”.

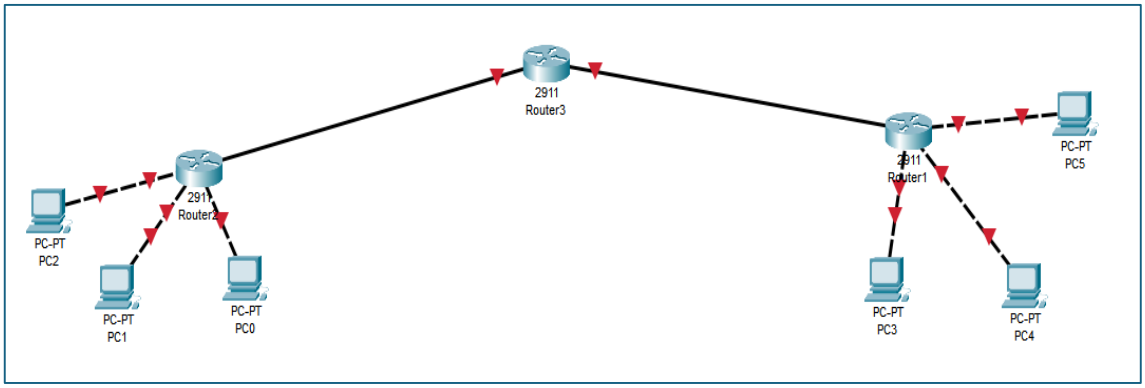
6.1. Diseño de alto nivel

6.1.1. Topología de red LAN

Para Peña (2021), en las redes de topología estrella “cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción” (p. 191).

Tomando como antecedente lo manifestado por Peña (2021), en el diseño de la red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional “Juan Pablo II”, se empleará la topología de red tipo estrella. A continuación, se presenta una gráfica de la topología.

Figura 4. Topología estrella extendida.



Fuente: Erick Rodríguez (2024)

6.1.2. Ubicación del portal cautivo y la distribución del SSID

Para la implementación de la red LAN con portal cautivo en la Unidad Educativa Fiscomisional “Juan Pablo II”, se tomará en cuenta la siguiente distribución.

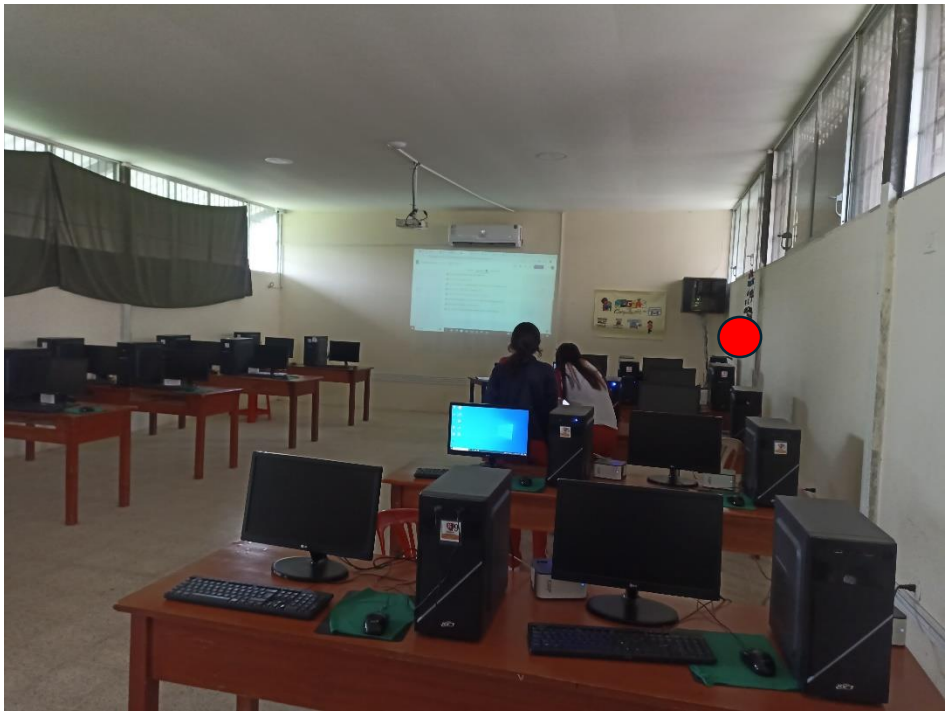
Figura 5. Distribución del SSID - 1

Fuente: Erick Rodríguez (2024)

Figura 6. Distribución del SSID - 2

Fuente: Erick Rodríguez (2024)

Figura 7. Servidor Principal



Fuente: Erick Rodríguez (2024)

Ubicar dos SSID en la red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II" permite separar el tráfico de estudiantes y personal, garantizando seguridad, gestión de ancho de banda, y priorización de recursos. Además, facilita la administración y mejora la calidad de servicio para diferentes necesidades.

6.2. Especificaciones de hardware y software

Tabla 8: Servidor Principal

Servidor	Dell PowerEdge R740
Características	Procesador: Dual Intel Xeon Silver 4214 (2.2GHz, 12 núcleos) Memoria RAM: 64GB DDR4 Almacenamiento: 2TB SSD en RAID 1 para redundancia Red: Tarjeta de red de 10GbE Sistema Operativo: Linux (CentOS/Ubuntu) o Windows Server Software de Portal Cautivo: pfSense, UniFi Controller, o similar Seguridad: Cortafuegos integrado y soporte para VPN Gestión: Interfaz de administración web, monitoreo en tiempo real
Cantidad	1
Precio	Servidor: $4,000 - $5,000 USD Licencias de Software (si aplica): $500 - $1,000 USD Instalación y Configuración: $1,000 - $2,000 USD Mantenimiento Anual: $500 - $1,000 USD
Total Aproximado	$6,000 - $9,000 USD

Fuente: Erick Rodríguez (2024)

Tabla 9: SSID para Estudiantes: "JP2-Estudiantes"

Router y Access Points:	Ubiquiti UniFi o Cisco Meraki
Servidor:	Dell PowerEdge R740
Software de Portal Cautivo:	pfSense, UniFi Controller, o similar
Router	$500 - $1,000 USD
Access Points	(5 unidades): $150 - $300 USD cada uno (700 - $1,500 USD en total)
Dell PowerEdge R740:	$4,000 - $5,000 USD
Licencias (si aplica):	$500 - $1,000 USD
Profesional de TI:	$1,000 - $2,000 USD
Mantenimiento Anual:	$500 - $1,000 USD
Total Aproximado	$8,000 - $11,000 USD

Fuente: Erick Rodríguez (2024)

Tabla 10: SSID para Personal: "JP2-Personal"

Router y Access Points:	Ubiquiti UniFi o Cisco Meraki
Servidor:	Dell PowerEdge R740
Software de Portal Cautivo:	pfSense, UniFi Controller, o similar
Router	$500 - $1,000 USD
Access Points	(5 unidades): $150 - $300 USD cada uno (700 - $1,500 USD en total)
Dell PowerEdge R740:	$4,000 - $5,000 USD
Licencias (si aplica):	$500 - $1,000 USD
Profesional de TI:	$1,000 - $2,000 USD
Mantenimiento Anual:	$500 - $1,000 USD
Total Aproximado	$8,000 - $11,000 USD

Fuente: Erick Rodríguez (2024)

6.3. Plan de seguridad

Tabla 11: Plan de seguridad

Autenticación y Acceso	• Portal Cautivo: Utilizar un portal cautivo que requiera autenticación para acceder a la red. • Credenciales Únicas: Asignar credenciales únicas para estudiantes y personal. • Multi-Factor Authentication (MFA): Implementar MFA para el personal administrativo y TI.

Encriptación	• WPA3: Utilizar WPA3 para encriptación de las conexiones Wi-Fi. • SSL/TLS: Asegurar que el portal cautivo use HTTPS para cifrar las comunicaciones entre usuarios y el servidor.
Segmentación de Red	• VLANs: Crear VLANs separadas para estudiantes, personal y dispositivos administrativos. • Firewall: Configurar reglas de firewall para controlar el tráfico entre las VLANs y proteger recursos sensibles.
Monitoreo y Detección	• Sistema de Detección de Intrusos (IDS): Implementar un IDS para monitorear y alertar sobre actividades sospechosas. • Registro de Actividades: Mantener registros detallados de acceso y actividades en la red.
Gestión de Ancho de Banda y QoS	• Control de Ancho de Banda: Limitar el ancho de banda para aplicaciones no críticas y priorizar tráfico esencial. • QoS: Implementar Quality of Service para asegurar la disponibilidad de recursos críticos.
Actualización y Mantenimiento	• Parches y Actualizaciones: Mantener todos los dispositivos y software actualizados con los últimos parches de seguridad. • Revisión de Configuración: Realizar auditorías periódicas de configuración de red y ajustes de seguridad.
Educación y Concienciación	• Capacitación de Usuarios: Educar a estudiantes y personal sobre buenas prácticas de seguridad informática. • Políticas de Seguridad: Establecer y comunicar políticas claras de uso aceptable y seguridad.
Respuesta a Incidentes	• Plan de Respuesta a Incidentes: Desarrollar un plan detallado para responder a incidentes de seguridad, incluyendo procedimientos de aislamiento y recuperación. • Equipo de Respuesta a Incidentes: Designar un equipo responsable de manejar incidentes y realizar investigaciones.
Copias de Seguridad	• Backups Regulares: Realizar copias de seguridad regulares de datos críticos y configuraciones de red. • Almacenamiento Seguro: Almacenar copias de seguridad en ubicaciones

	seguras, preferiblemente fuera del sitio principal.
Costos Aproximados	• Portal Cautivo y Software de Seguridad: $500 - $1,000 USD • Dispositivos de Red y Seguridad (firewall, IDS, etc.): $3,000 - $5,000 USD • Servicios de Capacitación y Consultoría: $1,000 - $2,000 USD • Licencias y Mantenimiento: $500 - $1,000 USD anuales
Total Aproximado	$5,000 - $9,000 USD (con costos recurrentes anuales adicionales para mantenimiento y licencias).

Fuente: Erick Rodríguez (2024)

Este plan ofrece un enfoque integral para proteger la red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II", abarcando desde la autenticación hasta la respuesta a incidentes y la educación de los usuarios.

6.4. Plan de implementación

6.4.1. Cronograma detallado

Tabla 12: Cronograma detallado

Semana	Actividad	Dias
Semana 1	Evaluación Inicial	1-5
Semana 2	Diseño de la Red	1-5
Semana 3-4	Adquisición de Equipos y Software	1-10
Semana 5	Configuración y Pruebas de Laboratorio	1-5
Semana 6-7	Despliegue en Sitio	1-10
Semana 8	Implementación del Portal Cautivo	1-5
Semana 9	Capacitación y Documentación	1-5
Semana 10	Monitoreo y Mantenimiento Continuo	1-5

Fuente: Erick Rodríguez (2024)

Semana 1: Evaluación Inicial

Días 1-2: Reunión Inicial

- Reunión con el equipo de TI y administración para definir objetivos y requerimientos.
- Auditoría de la infraestructura existente.

Días 3-5: Análisis de Requisitos

- Determinar el número de usuarios, tipos de dispositivos y servicios críticos.
- Identificar necesidades específicas de seguridad y segmentación de red.

Semana 2: Diseño de la Red

Días 1-3: Diseño de Arquitectura

- Diseñar la arquitectura de la red, incluyendo segmentación de VLANs y topología.

Días 4-5: Selección de Hardware y Software

- Seleccionar routers, switches, access points, servidores y software de portal cautivo.

Semana 3-4: Adquisición de Equipos y Software

Días 1-10: Proceso de Compra

- Solicitar cotizaciones y realizar compras de equipos y licencias de software.
- Coordinar la entrega de los equipos y software.

Semana 5: Configuración y Pruebas de Laboratorio

Días 1-3: Montaje y Configuración Inicial

- Montar y configurar todos los equipos en un entorno controlado.
- Configurar VLANs, SSIDs, portal cautivo, QoS y reglas de firewall.

Días 4-5: Pruebas de Funcionamiento

- Realizar pruebas de conectividad, rendimiento y seguridad.

Semana 6-7: Despliegue en Sitio

Días 1-3: Instalación Física

- Montar y conectar físicamente los equipos en la institución educativa.

Días 4-5: Configuración Final

- Aplicar la configuración final y realizar ajustes según las necesidades del entorno.

Días 6-10: Pruebas en Sitio

- Probar la red en el entorno real para asegurar que todo funciona correctamente.

Semana 8: Implementación del Portal Cautivo

Días 1-3: Configuración del Portal

- Configurar el portal cautivo con las políticas de acceso y autenticación definidas.

Días 4-5: Integración y Pruebas

- Integrar el portal cautivo con la red y realizar pruebas de acceso para estudiantes y personal.

Semana 9: Capacitación y Documentación

Días 1-2: Capacitación del Personal de TI

- Capacitar al personal de TI en la gestión y mantenimiento de la red.

Días 3-4: Educación a Usuarios

- Informar a estudiantes y personal sobre el uso correcto de la red y las políticas de seguridad.

Días 5: Documentación

- Crear documentación detallada de la configuración, procedimientos de mantenimiento y planes de contingencia.

Semana 10: Monitoreo y Mantenimiento Continuo

Días 1-2: Implementación de Herramientas de Monitoreo

- Implementar herramientas de monitoreo para supervisar el rendimiento y la seguridad de la red.

Días 3-5: Mantenimiento Regular

- Establecer un cronograma de mantenimiento regular y auditorías de seguridad.

6.4.2. Puntos de control y fases del proyecto

Tabla 13: Puntos de control y fases del proyecto

Fase	Puntos de control
Fase 1: Evaluación Inicial	Reunión inicial, auditoría, documentación de requerimientos
Fase 2: Diseño de la Red	Finalización del diseño, selección de hardware/software, aprobación del diseño
Fase 3: Adquisición de Equipos y Software	Recepción de cotizaciones, confirmación de entrega, verificación de equipos/software
Fase 4: Configuración y Pruebas de Laboratorio	Configuración inicial, pruebas de conectividad/rendimiento/seguridad, validación de pruebas
Fase 5: Despliegue en Sitio	Instalación física, configuración final, pruebas en entorno real
Fase 6: Implementación del Portal Cautivo	Configuración del portal, integración con la red, pruebas de acceso
Fase 7: Capacitación y Documentación	Capacitación del personal de TI, educación a usuarios, finalización de documentación
Fase 8: Monitoreo y Mantenimiento Continuo	Implementación de monitoreo, cronograma de mantenimiento, auditorías periódicas

Fuente: Erick Rodríguez (2024)

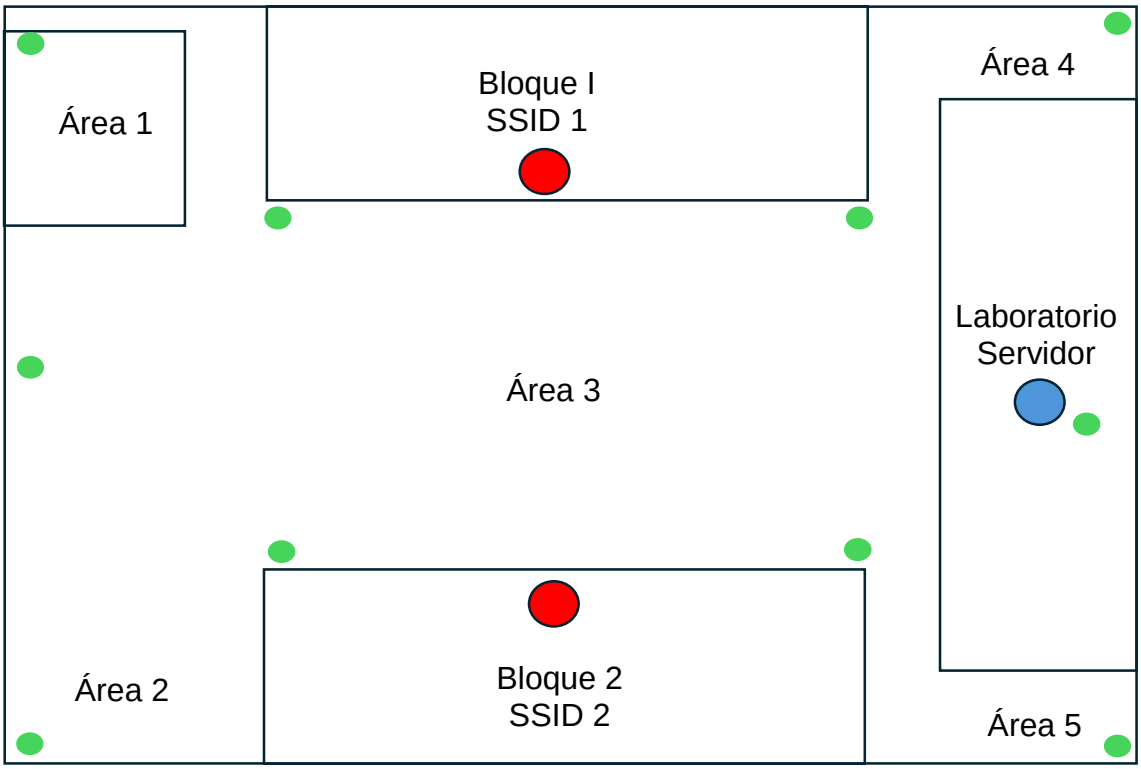
Este esquema asegura un control detallado en cada fase del proyecto, permitiendo una implementación ordenada y eficiente de la red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II".

7. DISEÑO DETALLADO Y ESPECÍFICO DE LA RED LAN DE LA UNIDAD EDUCATIVA FISCOMISIONAL “JUAN PABLO II”.

7.1. Diagrama de red

7.1.1. Ubicación de los dispositivos y conexiones.

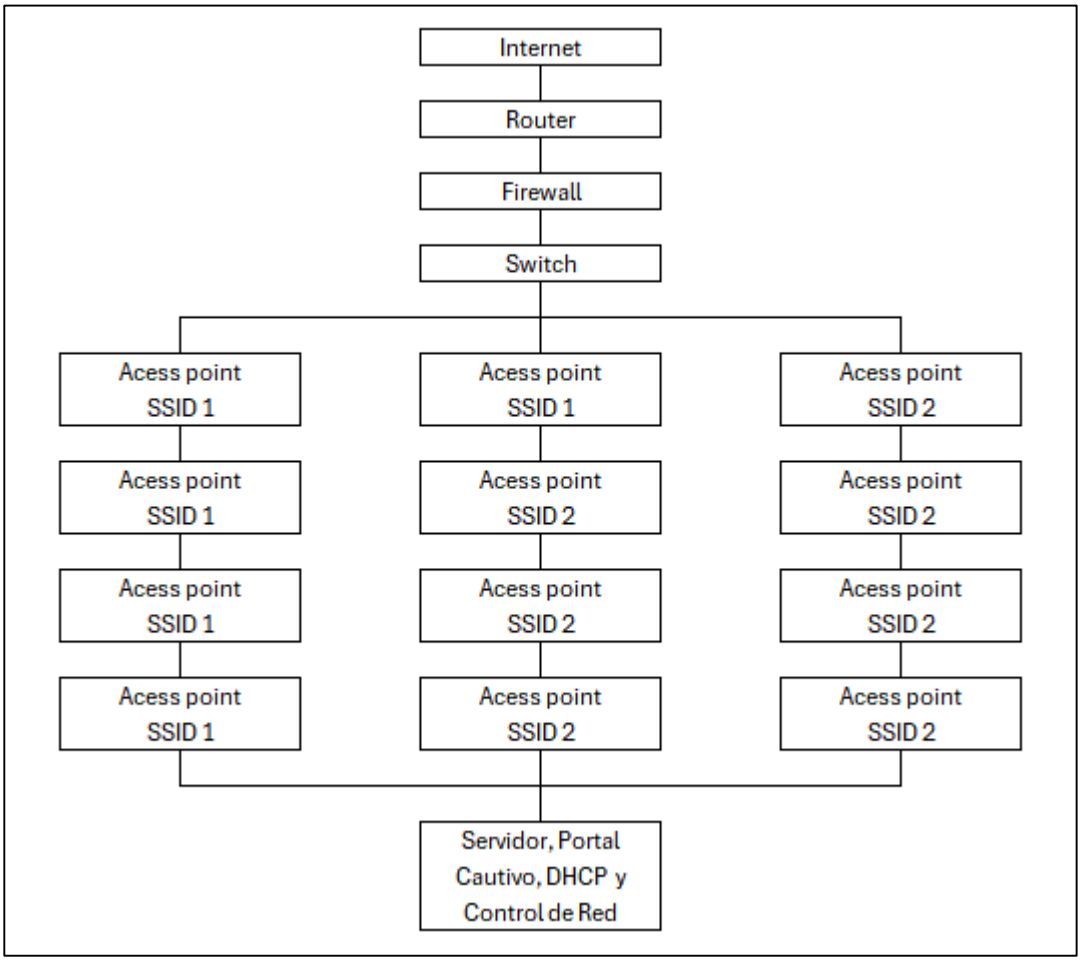
Figura 8. Servidor Principal



Fuente: Erick Rodríguez (2024)

7.1.2. Diagramas de flujo del portal cautivo

Figura 9. Diagrama de Flujo



Fuente: Erick Rodríguez (2024)

Descripción del Diagrama de Flujo

- Internet: El punto de entrada a la red global.
- Router: El router conecta la red interna con Internet y gestiona el tráfico entre ellos.
- Firewall: Protege la red interna de accesos no autorizados y ataques externos.

- Switch: Distribuye la conexión a los diferentes dispositivos en la red interna.
- Access Points: Distribuidos por la institución, emiten dos SSID diferentes (SSID 1 para estudiantes y SSID 2 para personal).
- Servidor: Maneja el portal cautivo, DHCP y el control de la red, autenticando a los usuarios y asignando IPs.

Explicación del Funcionamiento

Conexión Inicial:

Los usuarios se conectan a la red mediante uno de los Access Points, eligiendo entre SSID 1 o SSID 2 según su rol (estudiantes o personal).

Portal Cautivo:

- Una vez conectados, los usuarios son redirigidos al portal cautivo alojado en el servidor.
- El portal cautivo autentica a los usuarios utilizando sus credenciales.

Acceso a la Red:

- Tras la autenticación, el servidor asigna una dirección IP a los dispositivos mediante DHCP y permite el acceso a la red y a Internet.
- El tráfico de la red es gestionado y supervisado para asegurar un uso eficiente y seguro.

Este diagrama y descripción proveen una visión clara de la estructura y funcionamiento de la red LAN con portal cautivo en la Unidad Educativa Fiscomisional "Juan Pablo II".

7.2. Configuraciones de dispositivos

7.2.1. Configuraciones básicas de cada dispositivo de red.

Direcciones IP

Tabla 14: Direcciones IP de los dispositivos

Dispositivo	IP Address	Notas
Router	192.168.1.1	Gateway para toda la red
Firewall	192.168.1.2	Conectado a zona LAN
Switch	192.168.1.3	IP de gestión
Servidor	192.168.1.4	Portal cautivo, DHCP, control
AP1	192.168.1.10	IP de gestión
AP2	192.168.1.11	IP de gestión
AP3	192.168.1.12	IP de gestión
AP4	192.168.1.13	IP de gestión
AP5	192.168.1.14	IP de gestión
AP6	192.168.1.15	IP de gestión
AP7	192.168.1.16	IP de gestión
AP8	192.168.1.17	IP de gestión
AP9	192.168.1.18	IP de gestión
AP10	192.168.1.19	IP de gestión
Estudiantes	192.168.10.0/24	Rango DHCP: 192.168.10.100-200
Personal	192.168.20.0/24	Rango DHCP: 192.168.20.100-200
Servidor	192.168.1.4	Portal cautivo, DHCP, control

Fuente: Erick Rodríguez (2024)

Este esquema de direcciones IP proporciona una estructura clara y organizada para la red LAN con portal cautivo, permitiendo una gestión eficiente y segura de los dispositivos y usuarios en la Unidad Educativa Fiscomisional "Juan Pablo II".

VLANs

Configurar VLANs (Virtual Local Area Networks) para una red LAN con portal cautivo permite segmentar el tráfico de red para diferentes tipos de usuarios, como estudiantes y personal. A continuación, se describe una configuración básica de VLANs en una red LAN con portal cautivo.

Paso 1: Planificación de VLANs

VLAN 10: Estudiantes

- ID de VLAN: 10
- Rango de IP: 192.168.10.0/24

VLAN 20: Personal

- ID de VLAN: 20
- Rango de IP: 192.168.20.0/24

Paso 2: Configuración del Switch

Asumiendo que el switch soporta VLANs y tiene una interfaz de administración web o CLI (Command Line Interface), sigue estos pasos:

1. Configuración de VLANs en el Switch

Acceso a la Interfaz de Administración

- Accede a la interfaz de administración del switch a través de su dirección IP (e.g., 192.168.1.3).

Creación de VLANs

```
# Acceder al modo de configuración global
configure terminal

# Crear VLAN 10 para Estudiantes
vlan 10
 name Estudiantes

# Crear VLAN 20 para Personal
vlan 20
 name Personal
```

Asignación de Puertos a VLANs

```
# Asignar puertos específicos a VLAN 10 (Estudiantes)
interface range fastethernet 0/1-5
 switchport mode access
 switchport access vlan 10

# Asignar puertos específicos a VLAN 20 (Personal)
interface range fastethernet 0/6-10
 switchport mode access
 switchport access vlan 20
```

Configurar el Puerto Trunk para Access Points y el Router

```
# Configurar el puerto trunk que conecta el switch al router y access points
interface gigabitethernet 0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
```

Paso 3: Configuración del Router o Firewall

El router o firewall debe manejar el tráfico de las VLANs y proporcionar servicios como DHCP y el portal cautivo.

Configuración Básica de VLANs en el Router (ejemplo con un router Cisco)

```
# Acceder al modo de configuración global
configure terminal

# Crear subinterfaces para cada VLAN
interface gigabitethernet 0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0

interface gigabitethernet 0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
```

Paso 4: Configuración del Servidor (Portal Cautivo y DHCP)

Configuración de DHCP

El servidor debe estar configurado para proporcionar direcciones IP a los dispositivos en las VLANs.

Configuración de DHCP para VLAN 10 (Estudiantes)

```
subnet 192.168.10.0 netmask 255.255.255.0 {
  range 192.168.10.100 192.168.10.200;
  option routers 192.168.10.1;
  option domain-name-servers 192.168.1.4;
}
```

Configuración de DHCP para VLAN 20 (Personal)

```
subnet 192.168.20.0 netmask 255.255.255.0 {
  range 192.168.20.100 192.168.20.200;
  option routers 192.168.20.1;
  option domain-name-servers 192.168.1.4;
}
```

Paso 5: Configuración de Access Points

Los access points deben ser configurados para emitir los SSIDs correspondientes y etiquetar el tráfico con las VLANs adecuadas.

Ejemplo de Configuración de Access Points (ejemplo con un AP de Cisco)

```
# Configuración del SSID para Estudiantes en VLAN 10
dot11 ssid Estudiantes
  vlan 10
  authentication open
  guest-mode

# Configuración del SSID para Personal en VLAN 20
dot11 ssid Personal
  vlan 20
  authentication open
  guest-mode

# Asignación de SSID a las radios del AP
interface Dot11Radio 0
  ssid Estudiantes
  ssid Personal
```

7.2.2. Configuraciones de QoS y políticas de seguridad

7.2.2.1. Configuraciones de QoS

Según Viteri y Ávila (2023), para optimizar el rendimiento y la seguridad en una red LAN con portal cautivo, es crucial implementar configuraciones adecuadas de Calidad de Servicio (QoS) y políticas de seguridad. QoS se configura para priorizar el tráfico esencial y garantizar un rendimiento eficiente.

En un switch y router, se pueden crear políticas que asignen alta prioridad al tráfico de aplicaciones críticas como VoIP y video, mientras que se limita el ancho de banda para el tráfico menos crítico. Los access points también deben configurarse para aplicar estas políticas, asegurando que el tráfico de los SSIDs importantes reciba el tratamiento adecuado. Esto se logra mediante la creación de clases de tráfico y políticas de QoS que se aplican a las interfaces relevantes,

garantizando que el portal cautivo y las aplicaciones educativas reciban el ancho de banda necesario para un rendimiento óptimo (Viteri y Ávila, 2023).

7.2.2.1. Políticas de seguridad

Para Ruiz (2023), en cuanto a las políticas de seguridad, es esencial proteger la red contra accesos no autorizados y amenazas. En el firewall, se configuran reglas para permitir solo el tráfico necesario y bloquear accesos no deseados. En los switches, se implementan medidas como la seguridad de puertos y el filtrado de VLANs para evitar ataques y controlar el acceso a la red.

Los access points deben utilizar autenticación robusta, como WPA2-Enterprise, y cifrado para proteger la comunicación inalámbrica. Además, el servidor de portal cautivo debe estar configurado con reglas estrictas para la autenticación de usuarios y el monitoreo de tráfico, garantizando así la seguridad de la red y la protección de la información transmitida (Ruiz, 2023).

7.3. Pruebas de diseño

7.3.1. Planificación para asegurar que el diseño cumple con requisitos

La planificación para asegurar que el diseño de una red LAN con portal cautivo cumpla con los requisitos implica una serie de pasos clave que aseguran la adecuación del diseño a las necesidades específicas y la correcta implementación de todos los elementos de la red.

Tabla 15: Planificación para asegurar que el diseño cumple con requisitos

Nombre	Descripción	Detalle
Definición de Requisitos	Requisitos Funcionales y No Funcionales:	Requisitos Funcionales: Determinar el propósito del portal cautivo, como autenticación de usuarios, gestión de ancho de banda, y acceso a recursos específicos. Identificar los requisitos de los SSIDs (por ejemplo, uno para estudiantes y otro para personal) y el tipo de tráfico que se priorizará. Requisitos No Funcionales: Establecer criterios de rendimiento como la capacidad de la red, la calidad del servicio (QoS), y la seguridad necesaria. Esto incluye la disponibilidad, escalabilidad y la capacidad de manejo de usuarios concurrentes.
	Análisis de Necesidades de Usuario:	Estudiantes: Requisitos de acceso a recursos educativos, ancho de banda para streaming y navegación. Personal: Necesidades de acceso a sistemas administrativos, aplicaciones críticas y seguridad adicional.
Diseño de la Red	Topología y Segmentación	Topología de Red: Definir la estructura de la red LAN, incluyendo la disposición de switches, routers, firewalls, y access points. Segmentación con VLANs: Crear VLANs para separar el tráfico de estudiantes y personal, garantizando que cada segmento cumpla con los requisitos específicos y facilite la gestión del tráfico.
	Configuración de QoS	Políticas de QoS: Establecer reglas para priorizar el tráfico esencial, como la autenticación del portal cautivo y aplicaciones críticas, y garantizar la asignación adecuada de ancho de banda para evitar la congestión.
	Políticas de Seguridad	Acceso y Autenticación: Implementar políticas de acceso a la red, configuración de firewalls, seguridad de puertos en switches y autenticación segura en los access points. Protección del Portal Cautivo: Asegurar que el servidor de portal cautivo esté configurado para manejar

		la autenticación de usuarios y la gestión de acceso de manera segura.
Validación y Pruebas	Verificación del Diseño	Revisión de Diseño: Revisar el diseño de la red con las partes interesadas para confirmar que todos los requisitos están cubiertos. Documentación: Crear documentación detallada del diseño y las configuraciones planificadas, incluyendo diagramas de red, direcciones IP, y políticas de QoS y seguridad.
	Pruebas de Implementación	Pruebas de Conectividad: Verificar que todos los dispositivos están correctamente conectados y comunicándose según lo esperado. Pruebas de Rendimiento: Evaluar la capacidad de la red para manejar el tráfico de usuarios y aplicaciones, asegurando que las políticas de QoS se apliquen correctamente y que el rendimiento sea adecuado. Pruebas de Seguridad: Realizar auditorías de seguridad y pruebas de penetración para identificar vulnerabilidades y asegurar que las políticas de seguridad están efectivas.
Implementación y Monitoreo	Implementación Gradual	Despliegue por Fases: Implementar la red en fases, comenzando con una prueba piloto y luego extendiendo la implementación a toda la red para asegurar que los problemas se identifiquen y resuelvan en etapas tempranas.
	Monitoreo y Mantenimiento	Monitoreo Continuo: Utilizar herramientas de monitoreo para supervisar el rendimiento de la red, el tráfico y la seguridad, ajustando las configuraciones según sea necesario para mantener la eficiencia y seguridad de la red. Mantenimiento Regular: Realizar mantenimientos periódicos para actualizar configuraciones, aplicar parches de seguridad y optimizar el rendimiento.

Fuente: Erick Rodríguez (2024)

Esta planificación asegura que el diseño de la red LAN con portal cautivo cumpla con los requisitos establecidos y que se mantenga operativa, segura y eficiente a lo largo del tiempo.

7.3.2. Pruebas de rendimiento y seguridad

Para Ayala (2023), las pruebas de rendimiento en una red LAN con portal cautivo evalúan la capacidad de la red para manejar el tráfico esperado, incluyendo la velocidad, latencia y ancho de banda, asegurando que el portal y aplicaciones críticas funcionen correctamente bajo carga. Las pruebas de seguridad detectan vulnerabilidades y evalúan la efectividad de las políticas de seguridad, garantizando protección contra accesos no autorizados y ataques.

7.3.4. Pruebas de login del portal cautivo y servidor

Un login en un portal cautivo debe incluir una interfaz amigable y segura para que los usuarios introduzcan sus credenciales (nombre de usuario y contraseña). Debe tener medidas de seguridad como CAPTCHA para prevenir accesos no autorizados, y cifrado SSL para proteger la información transmitida. Además, debería ofrecer opciones de recuperación de contraseña y soporte para autenticación multifactor, asegurando tanto la facilidad de uso como la seguridad de los datos del usuario (Ruiz y Rodríguez, 2024).

7.3.4.1. Login en el servidor

Un login en un servidor de portal cautivo debe incluir credenciales seguras (usuario y contraseña), cifrado SSL, CAPTCHA, autenticación multifactor y opciones de recuperación de contraseña, asegurando tanto la seguridad de los datos como la facilidad de acceso para el usuario.

Figura 10. Login Servidor Principal

Fuente: Erick Rodríguez (2024)

7.3.4.2. Login en los usuarios

Un login en un portal cautivo para usuarios debe tener campos para usuario y contraseña, cifrado SSL, CAPTCHA, autenticación multifactor, y recuperación de contraseña, garantizando seguridad en el acceso y protección de datos.

Figura 11. Login en los usuarios del portal cautivo

Fuente: Erick Rodríguez (2024)

8. CONCLUSIONES

- Definir los requerimientos iniciales y evaluar el entorno actual son cruciales para establecer una base sólida para el diseño de la red LAN con portal cautivo.
- Desarrollar un plan detallado, especificando hardware, software y medidas de seguridad, asegura una implementación estructurada y eficiente de la red.
- Crear un diseño detallado con diagramas y configuraciones específicas garantiza que todos los aspectos de la red estén bien documentados y preparados para la implementación.
- Instalar y configurar los dispositivos siguiendo el diseño planificado permite una puesta en marcha eficiente y asegura que la red funcione según lo esperado.
- Monitorear y mantener la red regularmente asegura su funcionamiento continuo, previene problemas y optimiza el rendimiento del portal cautivo.
- Evaluar y mejorar continuamente la red basada en el monitoreo y la retroalimentación garantiza una infraestructura robusta y eficiente a largo plazo.

9. RECOMENDACIONES

- Se recomienda a las autoridades de la Unidad Educativa Fiscomisional "Juan Pablo II" supervisar el uso de la red LAN, garantizar el cumplimiento de las políticas de seguridad y proporcionar capacitaciones periódicas. Inviertan en mantenimiento y actualizaciones regulares para asegurar un rendimiento óptimo y proteger la integridad de la información transmitida a través del portal cautivo.

- Se recomienda a los docentes de la Unidad Educativa Fiscomisional "Juan Pablo II" usar la red LAN de manera responsable, siguiendo las políticas de uso y seguridad establecidas. Eviten compartir credenciales y aseguren dispositivos contra accesos no autorizados. Reporten problemas técnicos al personal de TI y fomenten el uso adecuado de la red entre los estudiantes para garantizar una experiencia segura y eficiente.

- Se recomienda a los estudiantes de la Unidad Educativa Fiscomisional "Juan Pablo II" utilizar la red LAN de manera responsable y segura. Sigan las políticas de uso, no compartan sus credenciales y eviten descargar contenido no autorizado. Informen cualquier problema al personal de TI. Un uso adecuado y respetuoso de la red garantiza un entorno digital seguro y eficiente para todos.

10. REFERENCIAS BIBLIOGRAFICAS

Acán, S. A. G., López, R. C. O., & Mejía, S. B. A. (2023). Estudio de la infraestructura de redes LAN de las instituciones educativas de la ciudad de Riobamba en el año 2021. Dominio de las Ciencias, 9(1), 508-527.

Almalki, F. A. (2020). Implementación de edificios inteligentes basados en IoT 5G utilizando la configuración de VLAN a través de Cisco Packet Tracer. Revista Internacional de Comunicación Electrónica e Ingeniería Informática, 11(4), 56-67.

Almeida Aguacunchi, M. P. (2022). Aplicación del método científico en Ciencias Naturales para el desarrollo del razonamiento práctico.

Anzola Anzola, J. P., Simanca Herrera, F. A., & García-Díaz, V. (2023). Impacto del Jitter en un control de formación multiagente. Revista Iberoamericana de Automática e Informática Industrial, 21(1), 17-28.

Atoche Yupanqui, N. N. (2021). Propuesta de implementación de un anillo backbone IP-MPLS y capacidad para brindar conectividad de red y escalabilidad a ISP's en la ciudad de Lima-2021.

Ayala Bendezu, C. (2023). Portal cautivo para administrar la seguridad de datos de la red inalambrica del IESTP San Pedro.

Avila, H. F., González, M. M., & Licea, S. M. (2020). La entrevista y la encuesta:¿ métodos o técnicas de indagación empírica?. Didasc@ lia: didáctica y educación, 11(3), 62-79.

Bonilla Castro, J. F., & Jairo Oliver, E. S. (2023). Diseño de un dispositivo de enseñanza inalámbrico utilizando IOT y RASPBERRY PI (Bachelor's thesis).

Castillo Ramos, M. R. (2023). Modelo tecnológico de infraestructura de redes para la comunicación de datos en la Dirección Regional de Salud (DIRESA), 2023.

Centeno Caamal, R., & Acuña Gamboa, L. A. (2023). Competencias digitales docentes y formación continua: una propuesta desde el paradigma cualitativo.

Criollo Rimaycuna, G. (2022). Lan de Cámaras IP de Monitoreo para los Protocolos de Bioseguridad Mediante la Metodología de Diseño de Red PPDIOO–Cisco en la IE José Carlos Mariátegui–La Oroya.

Delgado Aquino, L. V. (2021). Red lan de voz y datos con acceso inalámbrico para la transmisión de información del colegio Zenon de Elea.

Delgado, S. M. C. (2021). Revisión sistemática de Comunicaciones Unificadas de VoIP en redes CAN. Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 5(1), 17-34.

Esquivel Cuy, K. E. (2020). Implementación de portal cautivo para control y administración de la infraestructura de red de los laboratorios de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala (Doctoral dissertation, Universidad de San Carlos de Guatemala).

Falcón, A. L., & Serpa, G. R. (2021). Acerca de los métodos teóricos y empíricos de investigación: significación para la investigación educativa. Revista Conrado, 17(S3), 22-31.

Flores, R. R., & Guzmán, P. V. (2023). Instalación y configuración de equipos de red de capa 2 y capa 3 administrables para optimizar los recursos de ancho de banda brindando confiabilidad escalabilidad disponibilidad y eficiencia a la red de datos de la Radio Latacunga. In Universidad de las Fuerzas Armadas ESPE.

García Vega, L. G. (2023). Propuesta de mejora de la programación didáctica “Instalación y mantenimiento de redes para transmisión de datos.

García-Martínez, B. A., & Moreno-Duarte, H. A. (2021). Análisis de la implementación de listas de control de acceso (ACL), para mejorar la seguridad de la información en la empresa Crawford Colombia Ltda.

Gobantes Martínez, F. (2023). Laboratorio Docente Virtual basado en el simulador GNS3 para la Gestión y Operación de Redes mediante el protocolo SNMP.

Hernández, E. M. (2023). Redes locales. Con-Ciencia Serrana Boletín Científico de la Escuela Preparatoria Ixtlahuaco, 5(10), 14-15.

Insaurralde, N. D., Ríos, A. F., & Zalazar, R. E. (2023). Autenticación mediante FreeIPA en Linux Centos. In Concurso de Trabajos Estudiantiles (EST 2023)-JAIIO 52 (Universidad Nacional de Tres de Febrero, 4 al 8 de septiembre de 2023).

Lanchipa Valencia, E. F. (2021). Implementación de una web app para facilitar la administración y gestión de una red LAN en una PYMES utilizando un servidor Mikrotik OS.

Leone, M. (2020). Breve historia topológica del mundo: del muro a la red. DeSignis, (33), 0219-230.

León López, d. E. (2021). Estudio de factibilidad para la implementación de un portal cautivo para mejorar la seguridad de transmisión de datos en la Universidad Estatal del Sur de Manabí (Bachelor's thesis, Jipijapa. UNESUM).

Leyva, N. V. L., Ayabaca, D. M. G., Flores, C. R. B., & Gómez, V. J. G. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje. Sociedad & Tecnología, 4(2), 205-222.

Lopezosa, C. (2020). Entrevistas semiestructuradas con NVivo: pasos para un análisis cualitativo eficaz. Lopezosa C, Díaz-Noci J, Codina L, editores Methodos Anuario de Métodos de Investigación en Comunicación Social, 1. Barcelona: Universitat Pompeu Fabra; 2020. p. 88-97.

Mejía, M. J. O., Ortiz, C. A. A., Ramos, W. E. V., & Moscoso, L. E. P. (2022). Gestión del tráfico de red en la calidad de servicio “QoS” WAN en Tambopata-Perú 2021. Revista de ciencias sociales, 28(2), 300-318.

Morales Freire, S. G., & Zambrano Pilatasig, K. M. (2023). Diseño e implementación de un portal cautivo para el edificio matriz del Instituto Superior Tecnológico Sudamericano Quito (Doctoral dissertation, Villasis Chiriboga Fabrizio Vicente).

Mucha-Hospinal, L. F., Chamorro-Mejía, R., Oseda-Lazo, M. E., & Alania-Contreras, R. D. (2021). Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado. Desafíos, 12(1), 50-57.

Murillo Ospina, J. M., & Rey Beltran, J. D. (2020). Diseño de un plan de mejora de la red LAN del fondo financiero de salud para solucionar problemas de Broadcast por medio de protocolos de comunicación en segmentación.

Obando, C. (2022). Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI). InGente Americana, 2(2), 71-78.

Pita Tomala, R. A. (2023). Implementación de una infraestructura de red mediante redes LAN y WLAN, empleando equipos de redes, para la optimización de la red de la Institución Educativa Ancón (Bachelor's thesis, La Libertad: Universidad Estatal Península de Santa Elena, 2023).

Peña, D. M. (2021). Diseño e implementación de red LAN para tecnoimport: diseño e implementación de red LAN para tecnoimport. UNESUM-Ciencias. Revista Científica Multidisciplinaria, 5(4), 185-196.

Reyes-Ruiz, L. & Carmona Alvarado, F. A. (2020). La investigación documental para la comprensión ontológica del objeto de estudio.

Román, J., Peñafiel, M., Alvear, L., Chavez, R., & Vinueza, M. (2021). Modelos pedagógicos aplicados en educación inicial. Espacios, 42(01), 97-106.

Romo Manosalvas, N. F. (2022). Diseño de un sistema de publicidad multimedia manejado por una aplicación android y controlado el acceso de usuarios mediante un portal cautivo para el centro comercial Laguna Mall (Bachelor's thesis).

Rosado Baldarrago, L. A. (2024). Implementación de una SDN-LAN (Red Definida por Software–Red de área Local) para mejorar la administración de Redes en el CIP CDA.

Ruiz Córdova, C. A., & Rodríguez Andy, J. A. (2024). Portal cautivo y servicio aaa (authentication, authorization, and accounting) para el instituto superior Tecnológico Tena.

Ruiz García, S. (2023). Validación de los conceptos y niveles de seguridad en el portal cautivo de la Universidad Cooperativa de Colombia-Sede Bogotá (Bloque principal).

Salinas Valencia, F. A. (2021). Análisis de vulnerabilidad de la red wifi, del Departamento de TICS del GAD Municipal del cantón Baba (Bachelor's thesis, BABAHOYO: UTB, 2021).

Salsabila, A., & Sutabri, T. (2024). Analisis Pembelajaran Teknologi Jaringan untuk Mengetahui Simulasi Jaringan dengan Menggunakan Switch dan Router di Aplikasi Cisco Packet Tracer. IJM: Revista Indonesia de Multidisciplinaria, 2(3), 91-97.

Sandoval Forero, E. A. (2022). El trabajo de campo en la investigación social en tiempos de pandemia. Espacio Abierto. Cuaderno Venezolano de Sociología, 31(3), 10-22.

Santillán Vera, A. A. (2023). Análisis de los protocolos wpa y wpa2 en dispositivos móviles: aspectos de autenticación y encriptación de datos (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).

Sodeify, R., & Habibpour, Z. (2021). Percepciones de las enfermeras sobre el apoyo de los compañeros de trabajo en el lugar de trabajo: investigación cualitativa. Enfermería clínica, 31(6), 355-362.

Szott, S., Kosek-Szott, K., Gawłowicz, P., Gómez, J. T., Bellalta, B., Zubow, A., & Dressler, F. (2022). Wi-Fi se une a ML: una encuesta sobre cómo mejorar el rendimiento de IEEE 802.11 con el aprendizaje automático. IEEE Communications Surveys & Tutorials, 24(3), 1843-1893.

Solsol Isminio, J. E. (2024). Rendimiento de una red de área local con firewalls open source de siguiente generación, 2023.

Tejero González, J. M. (2021). Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario.

Vega, A. M. D. C. G., Arellano, L. E. V., & García, J. M. R. (2021). La Observación en el Estudio de las Organizaciones. A prática na Investigação Qualitativa: Experiências de Grupos de Investigação//La práctica en, 19(4), 71-82.

Vasquez Malca, J. (2024). Percepción del modelamiento de Red Lan en la transferencia de información de datos en equipos de Cómputo del Senati sede Yurimaguas, Perú, 2022.

Viteri Hernández, C., & Avila Pesantez, D. (2023). Exploración integral de la seguridad en redes de proveedores de servicios de internet: una revisión sistemática de literatura.

Vera Forero, Y. A. (2022). Análisis de ACL Complejas (reflexivas y basadas en el tiempo) para Configuración de QoS a través de GNS3.

Zamora Salazar, J. E., Espinal, S., & Albert, I. (2020). Diseño e implementación de una infraestructura inalámbrica basada en Alepo Meraki y Portal Cautivo para el control de acceso de empleados, proveedores y clientes en una entidad financiera (Master's thesis, ESPOL. FIEC).

11. ANEXOS

11.1. Guía de entrevista realizada

Entrevista realizada a los 5 docentes de la Unidad Educativa Fiscomisional “Juan Pablo II”, que tiene bastos conocimientos en el uso de herramientas informáticas y conocen sobre infraestructura tecnológica orientada a redes LAN y portales cautivos.

Anexo 1: Preguntas de la entrevista realizada.

No.	Pregunta
1	¿Qué es un portal cautivo?
2	¿Beneficios de una red LAN en la escuela?
3	¿Cómo garantiza seguridad el portal cautivo?
4	¿Qué equipos son necesarios para una red LAN?
5	¿Ventajas del portal cautivo en educación?
6	¿Cómo afecta el portal cautivo al rendimiento?
7	¿Pasos para implementar una red LAN?
8	¿Retos en la implementación del portal cautivo?
9	¿Cómo facilita la transmisión de información?
10	¿Medidas para mantener la red segura?

11.2. Ficha de observación

Observación realizada en la Unidad Educativa Fiscomisional “Juan Pablo II”, para conocer el estado de su infraestructura tecnológica.

Anexo 2: Preguntas de la observación de campo realizada.

No	Pregunta
1	¿Qué tipo de conexión a internet tiene la escuela?
2	¿Cuántos routers están actualmente instalados?
3	¿Existen puntos de acceso inalámbricos en todas las áreas clave?
4	¿Qué tipo de switches se utilizan en la red actual?
5	¿Hay un servidor central dedicado para la red?
6	¿Cuántos dispositivos finales (computadoras, tabletas) se conectan a la red?
7	¿Se realiza algún tipo de monitoreo de tráfico de red?
8	¿Qué medidas de seguridad están implementadas en la red actual?
9	¿Existe un plan de mantenimiento regular para los equipos de red?
10	¿La infraestructura actual soporta la expansión a una red LAN completa con portal cautivo?

CERTIFICADO DE ANÁLISIS
magister

Red LAN con portal cautivo para la transmisión de información en la Unidad Educativa Fiscomisional Juan Pablo II

4% Textos sospechosos

3% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas

1% Idiomas no reconocidos

Nombre del documento: Tesis Erick Rodriguez 31_07 R.docx
ID del documento: f4fabdaf2fea41d40ffbf6a83bb193383d36a156
Tamaño del documento original: 1,94 MB
Autor: Erick Rodriguez Utrera

Depositante: Erick Rodriguez Utrera
Fecha de depósito: 8/8/2024
Tipo de carga: url_submission
fecha de fin de análisis: 8/8/2024

Número de palabras: 15.709
Número de caracteres: 104.936

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.carloslopezosa.com | Entrevistas semiestructuradas con NVivo [Reseña] https://www.carloslopezosa.com/entrevistas-semiestructuradas-nvivo/	< 1%		Palabras idénticas: < 1% (77 palabras)
2	www.academia.edu | (PDF) La investigación documental para la comprensión onto... https://www.academia.edu/44288695/La_investigación_documental_para_la_comprensión_ontológic... 7 fuentes similares	< 1%		Palabras idénticas: < 1% (65 palabras)
3	revistas.udh.edu.pe http://revistas.udh.edu.pe/index.php/udh/article/download/253e/23	< 1%		Palabras idénticas: < 1% (58 palabras)
4	bibdigital.epn.edu.ec https://bibdigital.epn.edu.ec/bitstream/15000/8496/4/CD-5740.pdf.txt	< 1%		Palabras idénticas: < 1% (57 palabras)
5	academica-e.unavarra.es https://academica-e.unavarra.es/xmlui/bitstream/2454/16764/4/TFG_GonzalezNovilloR.pdf 1 fuente similar	< 1%		Palabras idénticas: < 1% (25 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario #729c20 El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (24 palabras)
2	cdn.www.gob.pe https://cdn.www.gob.pe/uploads/document/file/5448588/43847-oficio-de-minedu-sobre-internet.pdf	< 1%		Palabras idénticas: < 1% (25 palabras)
3	repositorio.utn.edu.ec http://repositorio.utn.edu.ec/bitstream/123456789/4666/9/04 RED 070 TESIS.pdf.txt	< 1%		Palabras idénticas: < 1% (14 palabras)
4	tiposde.net | Tipos De Instrumentos De Investigación - TIPOSDE https://tiposde.net/tipos-de-instrumentos-de-investigacion/	< 1%		Palabras idénticas: < 1% (13 palabras)
5	www.byronvargas.com | Guía completa: Paso a paso para configurar un switch de... https://www.byronvargas.com/web/como-se-pone-un-switch/	< 1%		Palabras idénticas: < 1% (18 palabras)

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
Uleam
COMISIÓN ACADÉMICA
EL CARMEN - MANABÍ