UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

"Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo"

Tesis para optar el Título Profesional de Ingeniero(a) en Computación e Informática.

INVESTIGADORES:

- Bach. Carrasco Zeña, Jessica Katherin
- Bach. Valdera Limo, Diego Antonio

ASESOR:

Dra. Jessie Bravo Jaico

Lambayeque – Perú

2021

“Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo”

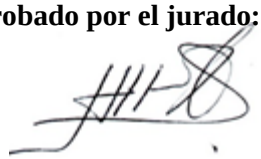
Tesis para optar el Título Profesional de Ingeniero(a) en Computación e Informática,

presentado por

Bach. Carrasco Zeña, Jessica Katherin

Bach. Valdera Limo, Diego Antonio

Aprobado por el jurado:



Dr. Ing. Armando José Moreno Heredia

Presidente

M.Sc. Ing. Nilton César Germán Reyes

Secretario

M.Sc. Ing. Janet del Rosario Aquino Lalupú

Vocal

Dra. Ing. Jessie Bravo Jaico

Asesor

ACTA DE SUSTENTACIÓN

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DECANATO
Ciudad Universitaria - Lambayeque

ACTA DE SUSTENTACIÓN VIRTUAL N°008-2022-D/FACFyM

Siendo las 9:20 am del día 23 de febrero del 2022, se reunieron vía plataforma virtual, https://meet.google.com/xyg-svfm-sgz los miembros del jurado evaluador de la Tesis titulada:

"Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo"

Designados por Resolución N° 642-2019-D/FACFyM de fecha 17 de mayo del 2019

Con la finalidad de evaluar y calificar la sustentación de la tesis antes mencionada, conformada por los siguientes docentes:

Dr. Ing. Armando José Moreno Heredia	Presidente
M.Sc. Ing. Nilton César Germán Reyes	Secretario
M.Sc. Ing. Janet del Rosario Aquino Lalupú	Vocal

La tesis fue asesorada por la Dra Jessie Leila Bravo Jaico, nombrado por Resolución N° 097-2019-D/FACFyM de fecha 25 de enero del 2019

El Acto de Sustentación fue autorizado por Resolución N° 156-2022-VIRTUAL-D/FACFyM de fecha 14 de febrero del 2022

La Tesis fue presentada y sustentada por los Bachilleres: Valdera Limo Diego Antonio y Carrasco Zeña Jessica Katherin y tuvo una duración de 30 minutos.

Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado se procedió a la calificación respectiva, otorgándole el Calificativo de 17 (Diecisiete) en la escala vigesimal, mención Bueno.

Por lo que quedan aptos para obtener el Título Profesional de **Ingeniero en Computación e Informática** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ciencias Físicas y Matemáticas y la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 10:10 am se dio por concluido el presente acto académico, dándose conformidad al presente acto con la firma de los miembros del jurado.

Dr. Ing. Armando José Moreno Heredia
Presidente

M.Sc. Ing. Nilton César Germán Reyes
Secretario

M.Sc. Ing. Janet del Rosario Aquino Lalupú
Vocal

Dra. Ing. Jessie Leila Bravo Jaico
Asesor

CERTIFICO: Que, es copia fiel del original
Fecha: 23 / 03 / 2022
M.Sc. Marco Antonio Martín Peralta Lui
SECRETARIO DOCENTE - FACFyM
VÁLIDO PARA TRÁMITES INTERNOS DE LA UNPRG

CONSTANCIA DE SIMILITUD

N° 35-2022-VIRTUAL-UI-FACFyM

EL DIRECTOR DE LA UNIDAD DE INVESTIGACIÓN DE LA FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO, HACE CONSTAR:

Que, la Bachiller **CARRASCO ZEÑA JESSICA KATHERIN**, de la Escuela Profesional de **INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA**, ha cumplido con presentar la **SIMILITUD DE ORIGINALIDAD DE LA TESIS (TURNITIN), como requisito indispensable para la sustentación de la tesis, según detalle**:

- **TÍTULO DE LA TESIS**: "DISEÑO Y ARQUITECTURA DE GESTIÓN Y SEGURIDAD PARA MEJORAR EL RENDIMIENTO DE LA RED INFORMÁTICA DEL COLEGIO SANTA MARÍA REINA DE CHICLAYO"
- **ÍNDICE DE SIMILITUD: 17 %**
- **ASESORA**: Dra. Ing. Jessie Leila Bravo Jaico.

Se expide la presente, para la tramitación del Título Profesional, dispuesto en **la Directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG.**

Lambayeque, 8 de abril de 2022

Dr. CAMILO QUINTOS CHUQUICAHUA
DIRECTOR UI-FACFyM

CONSTANCIA DE SIMILITUD

N° 36-2022-VIRTUAL-UI-FACFyM

EL DIRECTOR DE LA UNIDAD DE INVESTIGACIÓN DE LA FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO, HACE CONSTAR:

Que, el Bachiller **VALDERA LIMO DIEGO ANTONIO**, de la Escuela Profesional de **INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA**, ha cumplido con presentar la **SIMILITUD DE ORIGINALIDAD DE LA TESIS (TURNITIN), como requisito indispensable para la sustentación de la tesis, según detalle**:

- **TÍTULO DE LA TESIS**: "DISEÑO Y ARQUITECTURA DE GESTIÓN Y SEGURIDAD PARA MEJORAR EL RENDIMIENTO DE LA RED INFORMÁTICA DEL COLEGIO SANTA MARÍA REINA DE CHICLAYO"
- **ÍNDICE DE SIMILITUD: 17 %**
- **ASESORA**: Dra. Ing. Jessie Leila Bravo Jaico.

Se expide la presente, para la tramitación del Título Profesional, dispuesto en **la Directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG.**

Lambayeque, 8 de abril de 2022

Dr. CAMILO QUINTOS CHUQUICAHUA
DIRECTOR UI-FACFyM

DECLARACIÓN JURADA DE ORIGINALIDAD

Nosotros; Carrasco Zeña, Jessica Katherin y Valdera Limo, Diego, investigadores principales, y Dra. Ing. Jessie Bravo Jaico, asesor del trabajo de investigación "Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo", declaramos bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se demostrará lo contrario, asumo responsablemente la anulación de este informe y por ende el proceso administrativo a que hubiera lugar. Que puede conducir a la anulación del título o grado emitido como consecuencia de este informe.

Lambayeque, diciembre de 2021

Bach. Carrasco Zeña, Jessica Katherin

Bach. Valdera Limo, Diego

Dra. Ing. Jessie Bravo Jaico

DEDICATORIA

Dedico esta investigación a mis padres, y a mi hermana por su amor, su apoyo y brindarme sus modelos a seguir, que ha influenciado en mi vida dándome su consejo y guía para seguir satisfactoriamente mi formación profesional.

Y por último a mi asesor de tesis que nos ayudado a poder culminar esta investigación

Jessica Katherin Carrasco Zeña

Con mucho agradecimiento a Dios, por ser mi guía en todo momento y ponerme en el camino personas que han portado grandemente en mi carrera y mi formación como persona. Asimismo, quiero dedicar este proyecto de investigación a mis padres y a mi hermano, porque ellos siempre estuvieron a mi lado brindándome sus apoyo y consejo.

Diego Antonio Valdera Limo

AGRADECIMIENTO

Agradecer a Dios y a mis padres por ser los principales impulsores de mis sueños, y agradecerles por confiar y creer en mí y en mis expectativas todos los días.

.

A nuestra asesora la Dra. Ing. Jessie Bravo Jaico por su paciencia en el proceso de desarrollo del presente trabajo y que compartió generosamente su conocimiento para lograr con éxito este objetivo

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el presente trabajo de investigación se presenta una solución que cubra los requerimientos de una red de computadoras en una institución educativa. Se muestra además una propuesta de arquitectura de red y seguridad que surgió en base a la relevancia de la Tecnología de la Información y Comunicación para poder fortalecer un proceso educativo donde se muestre una infraestructura que ofrezca a sus estudiantes, docentes y administrativos una mejor forma de aprendizaje en el cual permita la comunicación de manera ágil y oportuna en la institución educativa.

Por estas razones surge la idea de poder proponer un Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo, la cual podrá facilitar las actividades académicas, salvaguardar la información en su totalidad, y que usuarios autorizados puedan acceder a ella, de esta forma se podrá aumentar la eficiencia, reducir riesgos e incrementar la calidad y rentabilidad de la institución educativa.

Finalmente esperamos que esta investigación pueda ser de mucho apoyo para otras instituciones educativas en donde se presente un deterioro en su infraestructura tecnológica y puedan introducir la tecnología en sus aulas haciendo cambio de paradigma, en los contenidos programados y en los sistemas de evaluación, ya que será necesario adaptarlos a la nueva realidad.

Palabras clave: tecnología, educación, infraestructura, red, seguridad

ABSTRACT

This research paper presents a solution that meets the requirements of a computer network in an educational institution. It also shows a proposal of network architecture and security that emerged based on the relevance of Information and Communication Technology to strengthen an educational process where an infrastructure is shown that offers its students, teachers and administrators a better way of learning in which it allows communication in an agile and timely manner in the educational institution.

For these reasons arises the idea of being able to propose a design of management and security architecture to improve the performance of the computer network of the School Santa María Reina, of Chiclayo, which will be able to facilitate academic activities, safeguard the information in its entirety, and that authorized users can access it, in this way it will be possible to increase efficiency, reduce risks and increase the quality and profitability of the educational institution.

Finally, we hope that this research can be very supportive for other educational institutions where there is a deterioration in their technological infrastructure and can introduce technology in their classrooms making a paradigm shift, in the programmed contents and in the evaluation systems, since it will be necessary to adapt them to the new reality.

Keywords: technology, education, infrastructure, network, security.

INTRODUCCIÓN

Actualmente en estos tiempos de COVID-19, la tecnología se ha convertido en una herramienta clave para el sector educación la era digital ha revolucionado de manera sorprendente y muchas escuelas han tenido que realizar cambios de sus herramientas de información, procesos y recursos para poder brindar educación a sus estudiantes. En el Perú muchas escuelas tanto del sector privado y público se han visto perjudicadas por la mala infraestructura tecnológica en sus campus escolares afectando a los estudiantes y también a los mismos trabajadores que ahora ya no pueden acceder a la información que trabajaban de manera cotidiana, lo cual se convierte en un problema grave que debe tratarse de manera rápida.

La investigación titulada "Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo" se ha orientado específicamente en poder ofrecerle a la Institución Educativa Santa Maria Reina una arquitectura de red que permita a los estudiantes y trabajadores poder conectarse desde sus hogares y salvaguardar la información que maneja la institución.

Para ello la investigación comprende cuatro capítulos importantes que va desde lo más general hasta el resultado final de la tesis.

El capítulo primero contempla las diferentes investigaciones que nos sirven de referencia para orientarnos sobre nuestra tesis propuesta, ayudando a estabilizar la investigación con argumentos sólidos asimismo, se encuentra la definición de los términos que permitirá esclarecer el objeto de investigación.

En el segundo capitulo se indica el diseño de investigación a utilizar describiendo las diferentes técnicas e instrumentos para la recolección y procesamiento de datos.

En tercer capítulo se contempla los resultados basándose en las fases de la metodología que proponemos la "Metodologia Top Down" lo cual permite obtener ventajas de segmentación de

subredes con las VLAN y explicando de manera detallada la seguridad informática. Asimismo, se explica la tecnología y equipos que darán solución a las necesidades de la institución.

Por último, en el cuarto capitulo se finaliza con la discusión, conclusiones y recomendaciones, explicando los beneficios de la red, logrando la disponibilidad, escalabilidad, rendimiento, performance, adaptabilidad y no menos importante la seguridad de la información.

Nuestra investigación permitirá a la Institución Educativa ofrecer a sus estudiantes, docentes, padres de familia y colaboradores una infraestructura tecnológica competente para la actual situación que viene atravesando el sector educación a nivel mundial.

CAPÍTULO I

1. DISEÑO TEÓRICO

1.1. Antecedentes

1.1.1. Antecedentes internacionales

Yáñez, C. (2017), en su tesis titulada: "Sistema de Gestión de Seguridad de la Información para La Subsecretaria de Economía empresas de Menor Tamaño", presentada en la Universidad de Chile de la Facultad de Ciencias Físicas y Matemáticas del Departamento de Ciencias de la Computación. El objetivo de la investigación es, definir e implementar un conjunto de sistemas basados en software libre para crear un SGSI con la normativa ISO 27001:2013. En la investigación se usó la auditoría interna al control de acceso conformes al estándar ISO/IEC 27001:2013 y la auditoría externa realizada por Neosecure para revelar brechas de seguridad de la información.

Llegando a las siguientes conclusiones:

- El proyecto permitió conocer mediante la observación una actitud de temor frente a los distintos tipos de riesgos de seguridad de la información y desarrollo de aplicativos. El personal al ver lo beneficios que genera un SGSI en cualquier organización moderna fue cambiando de actitud aceptando la existencia de riesgos y buscando la posibilidad de mitigarlos.
- Se logro diseñar 44 políticas y procedimientos de seguridad cumpliendo con la norma ISO 27001:2013 resultando ser practica e inclusiva favoreciendo el aprendizaje y la orientación en la creación de equipos de trabajo sin perder la visión y el objetivo final.
- Al utilizar el software libre alivianó los costos de los proyectos, dedicando más recursos de implementación de políticas llegando a cubrir un área organizacional mucho mayor.

Irastroza, J. (2016), en su tesis titulada: "Arquitectura de Gestión Distribuida para Redes Malladas Inalámbricas: Aplicación en el Entorno de la Red Personal", presentada en la Universidad de Cantabria. España. El objetivo de la investigación es, gestionar entornos de computación y comunicación en redes personales, se describen los componentes y funcionalidades que permitan construir un marco de gestión

adecuado, que colabore en la formación, mantenimiento y actualización de dichos entornos. La investigación tuvo una muestra aleatoria de datos y usó de instrumento el simulador NS-2.

Llegando a las siguientes conclusiones:

- Se requiere del diseño e incorporación de un marco de gestión adaptado al modelo de redes personales de nueva generación, que incluyen conceptos novedosos como la Community Área Network. Pacwoman es una arquitectura de esquema sencillo, centralizado y jerárquico, que es adecuado para su implementación sobre el prototipo de red personal que utiliza el protocolo SNMP como base para su desarrollo.
- La Community Area Network (CAN), incluye aspectos como la federación de redes, compartición de recursos, la seguridad y la gestión de los entornos correspondientes, compuestos por terminales heterogéneos, que acceden a los recursos distribuidos sobre topologías multisalto.

Muñoz, J. (2016), en su tesis titulada: "Diseño de Políticas de Seguridad Informática para la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad de Cuenca", presentada en la Universidad de Cuenca. Ecuador. El objetivo de la investigación es, analizar, diseñar políticas de seguridad informática para la Dirección de Tecnologías de la Información Comunicación, en base a la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009, manual de Políticas de Seguridad Informática – Mejoras Practicas Internacionales. La investigación tuvo como muestra al personal de las tres unidades de la DTIC y se usó de instrumento un test sobre los 11 dominios de seguridad de la norma ISO 27002.

Llegando a las siguientes conclusiones:

- Tras la aplicación de la prueba al personal de las tres unidades de la Dirección de Tecnologías de la Información y Comunicación, se pudo estimar que el primer porcentaje de cumplimiento de los 11 dominios de seguridad de la norma ISO 27002 era del 52%, lo cual es un valor de cumplimiento "bajo" dado que la norma puede ser aplicada a diversos tipos de organizaciones, privada o pública, grande, mediana o pequeña.

- Se ha podido calificar qué controles son los más necesarios para la mejora de porcentajes actuales de ejecución analizando la información brindada por el personal que trabaja en las 3 unidades de la DTI, siendo las políticas de seguridad informática, la carencia de documentación técnica, la seguridad física y ambiental los puntos más críticos.
- Para cada unidad de la DTIC deben establecerse políticas de seguridad de la información clasificada que permitan mejorar la seguridad, la organización, la concienciación y el rendimiento del trabajo, con el resultado final de una mayor seguridad de la información. Los puntos más cruciales son la falta de documentación técnica.

1.1.2. Antecedentes nacionales

Blas, J. (2017), en su tesis titulada: "Seguridad y Control de Acceso a las redes inalámbricas de la UNSM-T mediante Servidores de Autentificación Radius con el uso de Certificados Digitales", presentada en la Universidad Nacional de San Martin – Tarapoto. Perú. El propósito de la investigación es, plantear una plataforma de seguridad para el acceso inalámbrico al servicio de internet la UNSM-T. La investigación tuvo como muestra a 339 estudiantes de la Universidad Nacional San Martin – Tarapoto y se usaron los instrumentos de la observación directa y encuestas.

Llegando a las siguientes conclusiones:

- El uso de un servidor radius con certificados digitales reduce el peligro de robo de datos y asaltos a la red, mejorando la seguridad y la gestión en las redes UNSM-T.
- El servidor radius posee protocolos los cuales contienen certificados digitales, estos permiten que la nformacion generada entre el cliente y el servidor se mantenga segura.
- Fue posible resolver las debilidades de seguridad que se detectaron hoy por hoy en la red inalámbrica de la UNSM-T mediante el desarrollo del sistema de autenticación y autorización RADIUS con certificados digitales, lo que dio grandes resultados después de la investigación.

Montes, J. (2016), en su tesis titulada: "Diseño de Arquitectura de Seguridad Perimetral para una Empresa dedicada a la Actividad Inmobiliaria" presentada en la Universidad Ricardo Palma. Perú. El objetivo de la investigación es, Construir una arquitectura coherente que avale la integridad de los datos

internos y externos de la empresa en el campo inmobiliario proporcionando seguridad perimetral. La investigación se realizó para la empresa inmobiliaria Los Portales S.A.

Llegando a las siguientes conclusiones:

- Cada sistema es vulnerable a los ataques, por lo que prevenirlos es una buena idea. Conociendo cómo atacar te ayudará a defenderte de forma más eficaz. Como resultado, el objetivo de esta tesis es demostrar cómo se puede construir una barrera de seguridad para protegerse de muchos de los asaltos actuales.
- La solución de seguridad perimetral instalada en Los Portales se probó primero en un entorno de laboratorio antes de ser implementada en la red de Los Portales, con las validaciones necesarias y la aprobación del cliente.

1.1.3. Antecedentes locales

Fuentes, S. (2020), en su tesis titulada: "Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca", presentada en la Universidad Nacional Pedro Ruiz Gallo, Perú. El propósito de la investigación es, Contribuir a la mejora de la seguridad de la información basada en la norma ISO/IEC 27003, en la Universidad Nacional de Cajamarca. La investigación tuvo como muestra a 31 estudiantes de la UNC y se usaron los instrumentos de observación directa, entrevistas y llenado de formularios con la ayuda del jefe general de OTI.

Llegando a las siguientes conclusiones:

- Al analizar la información recogida se pudo conocer cómo se encuentra actualmente la seguridad de la información incumpliendo significativamente las normas, Permitiendo así, elaborar Políticas de Seguridad de la Información generales con el propósito de mantener niveles de riesgos aceptables según la norma.
- Aplicando el método MagerIT, se logró desarrollar un procedimiento para disminuir los riesgos no tolerables, definiendo un conjunto de medidas protección para los activos que se pusieron en marcha en beneficio de la UNC y para mejorar la seguridad de la misma.

- Con la aplicación del método MagerIT se logró definir roles y funciones, mejorando el proceso que detecta las irregularidades en la información y su seguridad, aumentando la seguridad en los servicios, aplicaciones y los equipos informáticos.

1.2. Base Teórica

1.2.1. Arquitectura de gestión de red

Gestión de Red: Es el elemento indispensable que tiene toda organización, ya que esta es necesaria para operar una red de comunicaciones, mediante la organización, planificación, instalación, operación y dominio de los elementos comunicacionales de la red, y así, garantizar una mejor calidad de servicio.

Si la arquitectura incluye todas las salvaguardas y actividades necesarias para permitir la utilización eficaz y eficiente de recursos y procesos dispersos, como los que conformarían una red de comunicaciones. lo que hace referencia a una arquitectura de gestión de red. (Irastorza, J., 2016. Pág., 8).

Sin embargo, para describir los procesos que constituyen una arquitectura de gestión de red se necesita de componentes o modelos para recoger y evaluar su información, en el siguiente apartado se exponen aquellos modelos.

1.2.1.1. Sub modelos de arquitectura de gestión de red.

Irastorza, J. (2016), Sostiene que existen cuatro submodelos de arquitectura de gestión de red, entre los que tenemos:

- **Modelo de información:** Es un elemento fundamental dentro de la arquitectura de gestión de red, ya que, este brinda el conocimiento necesario para luego gestionar diferentes funciones.

Irastorza, J. (2016), describe al modelo como: La información de gestión abarca diferentes elementos: componentes de red (host, repetidores, hubs, etc.); objetos administrativos (personas de contacto, lista de usuarios, tabla de precios, etc.); objetos dinámicos (circuitos virtuales X.25, conexiones TCP, etc.); entidades de protocolo (LLC, X.25, IP, etc.); relación entre objetos (es-parte-de, está-gestionado-por, está-anexado-a, etc.); descripción de servicios, perfiles de usuarios, alarmas, eventos y umbrales asociados, entre otros. (Pág., 10).

- **Modelo de organización:** Este modelo permite la flexibilidad en la distribución espacial de los componentes de gestión de red, así como en la asignación a las distintas áreas de responsabilidad.

Irastorza, J. (2016), sostiene que se encarga de: Implantar los diversos roles o funciones dentro del sistema, introduciendo, por ejemplo, existen nociones para para la gestión jerárquica y la gestión cooperativa entre sistemas iguales, en la que se establecen diferentes niveles de responsabilidad a los sistemas de gestión. (Pág., 11).

- **Modelo de comunicación.** El modelo de comunicación de una arquitectura de gestión define cómo se intercambia la información entre los distintos componentes de la arquitectura.

Para Irastorza, J. (2016), el modelo de comunicación cubre los siguientes puntos: definición de la sintaxis y semántica de las estructuras de datos usados en la comunicación; especificación de los servicios y protocolos para las aplicaciones de gestión; especificación de los elementos que intervienen en la comunicación; incorporación de los protocolos de gestión en la arquitectura de servicio e integración de las jerarquías de protocolos en la arquitectura de comunicación subyacente. (Pág., 12).

- **Modelo funcional.** Distribuye las responsabilidades de gestión en una serie de áreas operativas, especificando para cada área su tarea principal, los servicios necesarios para proporcionar dicha funcionalidad.

  Dentro de este modelo Irastorza, J. (2016), describe cinco áreas funcionales:

- Gestión de la configuración. Realiza una descripción geográfica, topológica y organizativa de la red y del sistema
- Gestión de fallos. Intenta mantener la red operativa en caso de avería.
- Gestión del rendimiento. No es habitualmente suficiente con que la red opere, sino que debe ejecutar correctamente, bajo principios de Calidad de Servicio y de Grado de Servicio.
- Gestión de la contabilidad. Registra el uso de los servicios y recursos de la red.
- Gestión de seguridad. Protege la red y los datos que contiene contra el acceso y el uso ilegal.

1.2.2. Medios de transmisión

1.2.2.1. Sistema de cableado estructurado (SCE).

El SCE radica en el tendido de cables (STP, UTP, fibra óptica) en el interior de un edificio, los cuales tienen la función de interconectar equipos, integrar servicios y permitir la comunicación.

Gallego J. (2019), lo define como: Un sistema de cableado para diferentes tipos de lugares, como edificios residenciales, públicos o comerciales, y campus, que se desarrolla y ejecuta de acuerdo con las normas de infraestructura de cableado especificadas.

Castillo J. (2019), dice que debe: Soportar los diferentes servicios de telecomunicaciones, principalmente de voz y de datos, que se integran en un edificio. (Pág. 59)

1.2.2.2. Estándares de cableado.

En un mecanismo de cable estructurado, es importante adherirse a las normas y reglamentos de TIA/EIA.

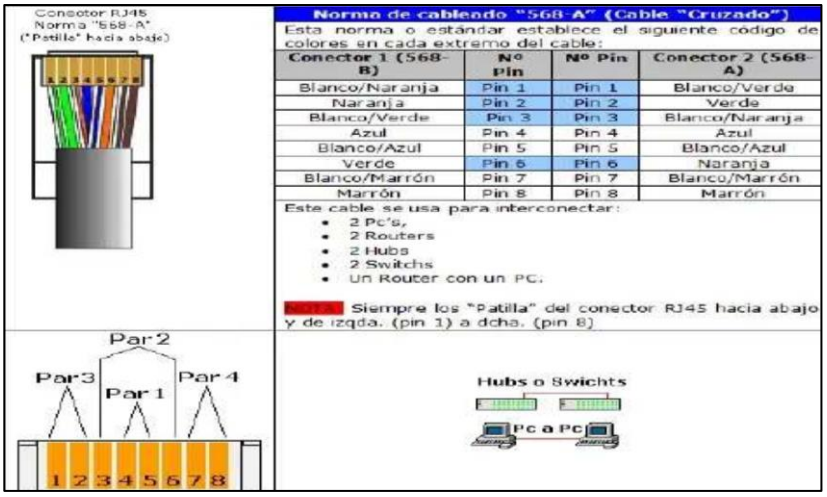
El objetivo es que la red tenga una alta banda ancha y pueda soportar una gran cantidad de flujo de datos. (2019, Marco N.)

- **ESTÁNDARES TIA/EIA:**

TIA/EIA-568-A: Este término hace referencia a un sistema de cableado de telecomunicaciones para edificios comerciales que pueden manejar una variedad de proveedores y productos. La finalidad de esta norma es facilitar el diseño y la instalación de los cables de telecomunicación casi no contengan información sobre los productos de telecomunicaciones que se instalarán en el futuro. El costo de instalar el sistema de cables durante la instalación y / o modificación o movimiento es mucho menor que después de que el edificio está ocupado, y hay menos interrupciones involucradas. Para conocer al detalle el estándar TIA/EIA-568-A como se muestra en las figuras 1 y 2, se debe tener en cuenta la siguiente codificación de colores en cada extremo del cable.

Figura 1

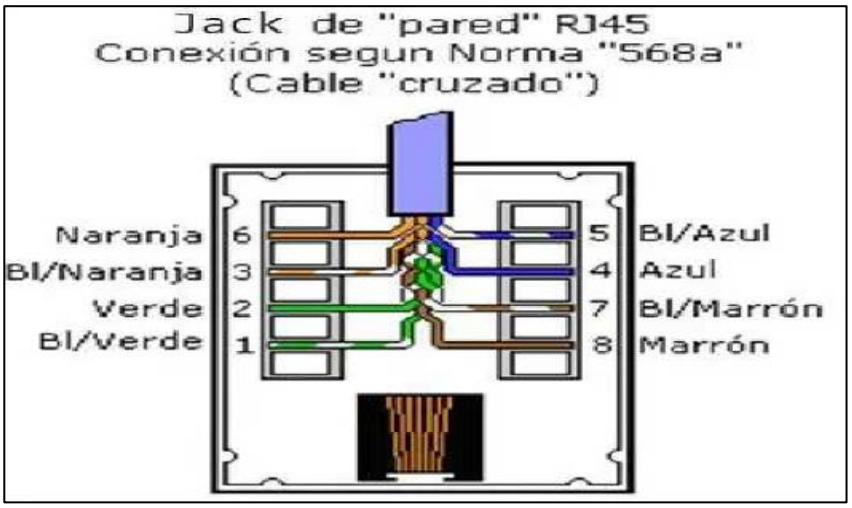
Estándar ANSI/TIA/EIA-568-A Para Conectores RJ-45



Nota. Normas ANSI/TIA/EIA-568-A. Reproducida de Normas Cableado de par Trenzado para RJ45, de Esther Quintana, 2019 (https://slideplayer.es/slide/13792796/), CC BY 2.0

Figura 2

TIA/EIA-568-B:



Nota. Normas ANSI/TIA/EIA-568-A. Reproducida de Codigo de Colores para Rosetas “murales” RJ45, de Esther Quintana, 2019 (https://slideplayer.es/slide/13792796/), CC BY 2.0

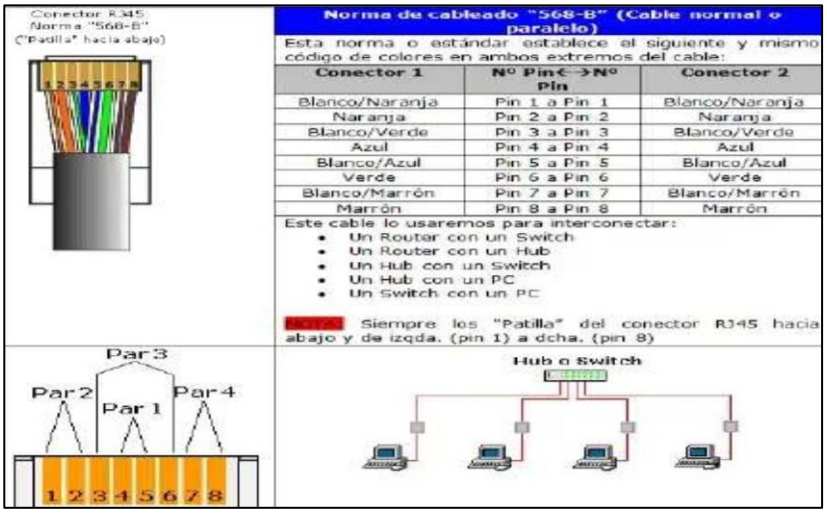
Tiene como objetivo establecer directrices para el diseño y la aplicación de sistemas de cableado estructurado entre edificios de comercio y universitarios. Explique los requisitos generales. Proporciona información sobre la planificación, instalación y verificación de cableado estructurado en edificios comerciales. (Cómo instalar cableado)

- Requisitos generales de la TIA / EIA 568-B1
- Conjunto de cable de par trenzado balanceado TIA / EIA 568-B2
- Conjunto de enrutamiento de cables TIA / EIA 568-B3, fibra óptica.

La representación del estándar TIA/EIA-568-B como se muestra en las figuras 3 y 4, hay que tener en cuenta la siguiente codificación de colores en ambos extremos del cable.

Figura 3

Estándar ANSI/TIA/EIA-568-B Para Conectores RJ-45.



Nota. Normas ANSI/TIA/EIA-568-B. Reproducida de Normas Cableado de par Trenzado para RJ45, de Esther Quintana, 2019 (https://slideplayer.es/slide/13792796/), CC BY 2.0

Figura 4

Estándar ANSI/TIA/EIA-568-B Para Jacks de Pared

Nota. Normas ANSI/TIA/EIA-56B-A. Reproducida de Codigo de Colores para Rosetas "murales" RJ45, de Esther Quintana, 2019 (https://slideplayer.es/slide/13792796/), CC BY 2.0

El Estándar para las rutas y espacios de telecomunicaciones en los edificios comerciales (TIA/EIA-569-A) especifica las prácticas de diseño y construcción dentro y entre los edificios que permiten el funcionamiento de los medios y equipos de telecomunicaciones.

- **ESTÁNDAR TIA/942:**

Infraestructura de telecomunicaciones para centros de datos. Proporciona una colección de normas y sugerencias para el diseño y la implementación de la infraestructura del centro de datos, con respecto a cuatro subsistemas establecidos: sistema mecánico, sistema eléctrico, arquitectura y telecomunicaciones.

La norma diferencia 4 tipos de centros, de acuerdo a su nivel de fiabilidad, llamados TIER:

- TIER I- Nivel Básico, disponibilidad 99,671%.
- TIER II- Nivel Componentes redundantes, disponibilidad 99,741%.
- TIER III – Nivel Mantenimiento concurrente, disponibilidad 99,982%.
- TIER IV - Nivel Tolerante a errores, disponibilidad 99,995%.

- **ESTÁNDAR IEEE 802.11:**

Redes Inalámbricas. Especifica el uso de la Capa de enlace y Capa física de datos de la arquitectura OSI, especificando las directrices de funcionamiento de una red de área local inalámbrica (WLAN).

- 802.11 n: Funciona en las bandas de 2,4GHz y 5GHz y admite conexiones de hasta 600 Mbps. La característica más significativa de 802.1l n es que integra múltiples antenas y puede usar múltiples canales simultáneamente. Este es el llamado MIMO
- 802.11ac: Operando en la frecuencia de 5GHz, soporta conexiones de hasta 1300 Mbps.

- **ESTÁNDAR IEEE 802.3 ESTÁNDAR DE ETHERNET.**

Es una especificación estándar para Ethernet, especifica los medios físicos y las características de trabajo en una red de área local (LAN).

- 802.3 AF: Alimentación sobre Ethernet Define todo lo necesario para usar tecnología PoE, voltajes, corrientes necesarias, el tipo de conexión, los cables que se deben usar, etc. Admite la entrega de energía hasta 15.4W por puerto.
- 802.3 AT: Mejoras de Alimentación sobre Ethernet Admite hasta 25.5W de potencia en los puertos.

1.2.3. Seguridad de la red

Cualquier computador conectado a internet siempre estará apto para ser víctima de un ataque cibernético, por lo tanto, es esencial que las instituciones, empresas y usuarios que usen equipos informáticos conectados a internet posean dispositivos que los protejan de intrusos.

1.2.3.1. Firewalls.

Según Lederkremer M. (2020), define un firewall como: conocido como cortafuegos, hace referencia a un nivel de seguridad, usado para limitar el acceso interno o externo de contenidos en la red, por personal no autorizado o evitar que este pueda descargar algún software dañino para el equipo-. (Pág. 04.)

Este sistema o combinación de sistemas, también llamado contrafuegos, cumplen con una serie de reglas específicas, las cuales finalmente van a permitir o denegar el tráfico en la red.

TIPOS DE FIREWALLS:

- Firewall Hardware: Este cortafuego, normalmente, proporcional una barrera que evita que intrusos tengan acceso a información de los servidores o router que empleamos para acceder a Internet. Este firewall hace su trabajo mediante la inspección de los paquetes de datos de la red y la decisión de dejar pasar paquetes e impedir su acceso. (Lederkremer M.).

- Firewall Software: Se trata del firewall que viene con el sistema operativo del ordenador y, por tanto, en este caso, la función principal es la proteger a un equipo y sus datos de accesos no autorizados–. Supervisa el tráfico para evitar accesos no deseados. (Lederkremer M. 2020).

1.2.3.2. VLAN-RED de ÁREA local virtual.

Las redes de área local virtual, o VLAN, son una tecnología de nivel 2 en el modelo de sreferencia OSI que ayuda a la optimización del tráfico de red, la seguridad y la segmentación se forman dominios de difusión individuales para cada VLAN construida en el switch o router, lo que permite que esta técnica aumente el rendimiento de la red. Cuando hay que asegurar muchos segmentos de red dentro de la misma infraestructura de red, las VLAN se utilizan habitualmente en contextos empresariales. (EcuRed, 2016).

1.2.3.2.1. Características de la VLAN.

Según Lederkremer M. (2020), la VLAN presenta las siguientes características:

- La VLAN proveen, seguridad en la red, puesto que si un usuario desea conectarse a un puerto no podrá escanear la red completamente.
- En la VLAN se puede definir que segmentos de red son visibles para los usuarios.
- Las VLAN no encriptan la información transmitida.

1.2.3.2.2. Ventajas de la VLAN.

Según Brihuega D. (2016), La VLAN permite la creación de una nueva red sobre una ya existente, aportando las siguientes ventajas:

- Dado que la arquitectura puede modificarse utilizando los parámetros de los interruptores, hay más transigencia en la gestión y los cambios en la red.
- Aumento el rendimiento, pues conserva el ancho de banda, controlan los dominios de broadcast y previenen las tormentas de broadcast.
- La información se encapsula a un nivel más alto y puede analizarse, lo que da lugar a una mayor seguridad.
- Decremento de la transmisión de tráfico en la red. (Pág. 99)

1.2.3.2.3. Tipos de la VLAN.

A continuación, especificamos los tipos de VLAN según (Barbosa, 2016):

a. VLAN DE NIVEL 1 (POR PUERTO).

También denominada como "port switching". Se especifica qué puertos del Switch forman parte de la VLAN, Los que se conectan a esos puertos son miembros de esa VLAN.

b. **VLAN de nivel 2 por direcciones MAC.**

Basándose en su dirección MAC, los hosts se asignan a un VLAN. Tiene la ventaja de evitar la necesidad de volver a configurar el dispositivo de conmutación si el usuario se mueve, es decir, se conecta a un puerto diferente en ese u otro dispositivo. La principal desventaja es que existiría una asignación por cada miembro si hay cientos de clientes.

c. VLAN DE NIVEL 3 POR DIRECCIONES DE SUBRED

La cabecera del nivel 3 se emplea para identificar a qué VLAN pertenece. Los paquetes, no las estaciones, son los miembros de la VLAN en este tipo de VLAN. Las estaciones que soportan múltiples protocolos de red (nivel 3) se dividirán en varias VLANs.

d. VLAN DE NIVELES SUPERIORES.

Cada aplicación, como FTP, flujos multimedia y correo electrónico, tiene su propia VLAN. La pertenencia a las VLAN puede determinarse por una serie de factores, como los puertos, las direcciones MAC, la red, el día de la semana, el formulario de acceso y las condiciones de seguridad del ordenador.

1.2.3.2.4. Ataques a la VLAN.

a. VLAN HOPPING

Es un ataque de red en el que un ordenador envía o recoge paquetes de una VLAN que el ordenador no debe tener acceso a. Esto se consigue asignar un ID de VLAN específico al tráfico invasivo o negociando un enlace de cabezal para enviar o recibir tráfico en la red VLAN penetrada. El intercambio de identidad de switch o el doble etiquetado pueden utilizarse para crear VLANs esperando(CISCO CCNA2, s.f.).

b. MAC FLOODING ATTACK

Este ataque implica anegar la tabla CAM de un Switch con miles de direcciones MAC generadas al azar por una herramienta como macof. Una tabla CAM (Memoria de contenido dinámico) es una lista que almacena el Switch con las direcciones MAC, interfaz y VLAN de todos los hosts conectados a él, permitiendo que los gráficos se muevan de un origen a una interfaz de destino en el Switch a mediante de la dirección MAC del terminal de destino.

La tabla CAM no es infinita; sólo puede almacenar una determinada cantidad de información, y cuando un ataque la agota, los gráficos enviados de un PC a otro en Unicast en el Switch se envían a través de todos los puertos, independientemente de si se configuran los dominios Brodcast (VLAN). Esto permite a un atacante capturar todo el tráfico que pasa por el Switch utilizando un sniffer como Wireshark o TCPDUMP. (Flores, 2017)

c. SPOOFING ATTACK – DHCP SPOOFING

Cuando se renueva o se solicita una nueva IP, se sustituye el servidor DHCP de la red y se actualiza la configuración de red que reciben los equipos asociados. (Flores, 2017)

1.2.3.2.5. VTP – Protocolo de la VLAN.

La VLAN Trunk Protocol (VTP) fue creado por Cisco, esencialmente es el encargado de mantener la consistencia de la configuración VLAN en la red, VTP gestiona todas las VLAN existentes en una red de redes. Los problemas más comunes que resuelve el VTP son: El cruce de VLANs causado por inconsistencias de configuración de VLANs. Y la carencia de configuración de VLANs mediante medios mezclados como Ethernet y FDDI. (Lederkremer M. 2020).

La facilidad que le brinda al administrador de la red es, que cuando se crea una nueva VLAN en un servidor VTP, se propaga a todos los switches del dominio. Esto elimina el requisito de establecer la misma VLAN en todos partes. Lo que ocasiona un ahorro en el tiempo y a su vez, disminuye el riesgo que existan errores o problemas de configuración.

a. BENEFICIOS DE VTP

Según Lederkremer M. (2020), El protocolo VTP presenta los siguientes beneficios:

- Consistencia en la configuración de la VLAN a través de la red, mediante los modos servidor, cliente o transparente.
- Informes dinámicos sobre las VLAN que se agregan a una red
- Seguimiento y monitoreo preciso de las VLAN.

b. FUNCIONAMIENTO VTP

De acuerdo a su funcionamiento el protocolo VTP le permite al administrador de la red lo siguiente:

- El VTP proporciona una manera fácil de mantener una configuración VIAN consistente en toda la red conmutada.
- VTP admite una fácil expansión a soluciones de red de conmutación de otros tamaños, lo que reduce la necesidad de configuración de red manual.

c. COMPONENTES VTP

Según Molina, J. (2012), entre los componentes del protocolo VTP tenemos los siguientes:

- Dominio de VTP: Se compone de uno o varios interruptores que están conectados entre sí. Utilizando las publicaciones de VTP, la información de configuración de la VLAN se comparte entre todos los switches de un dominio
- Servidor del VTP: Los servidores son responsables de crear y mantener toda la información de VLAN en la red y son los responsables de pasar esta información al resto de los conmutadores. De forma predeterminada, los conmutadores Cisco están en modo servidor.
- Cliente del VTP: Funcionan de forma análoga a los servidores VTP, sin embargo, no son capaces de crear, modificar o eliminar VLAN en un cliente VTP. Mientras el interruptor está activado, un cliente VTP sólo almacena la información de VLAN para todo el dominio. (Pág. 332)

1.2.4. Rendimiento de la red

Al utilizar la red, es importante comprender cómo se comunican los datos para poder realizar un análisis que permita determinar la calidad del enlace de comunicación. Por esta razón, es necesario analizar el comportamiento de la red para estimar su rendimiento, ya que una red configurada incorrectamente o una red de bajo rendimiento pueden causar una gran pérdida de tiempo y baja productividad en un gran sistema de comunicaciones.

Los parámetros más comunes que se utilizan para analizar el comportamiento de la red son la eficiencia y el retraso o la demora de los paquetes de datos debido a la congestión que pueden encontrar el origen y el destino.

Para tener un buen rendimiento dependerán de los dispositivos de monitorización. Los más habituales son los siguientes.

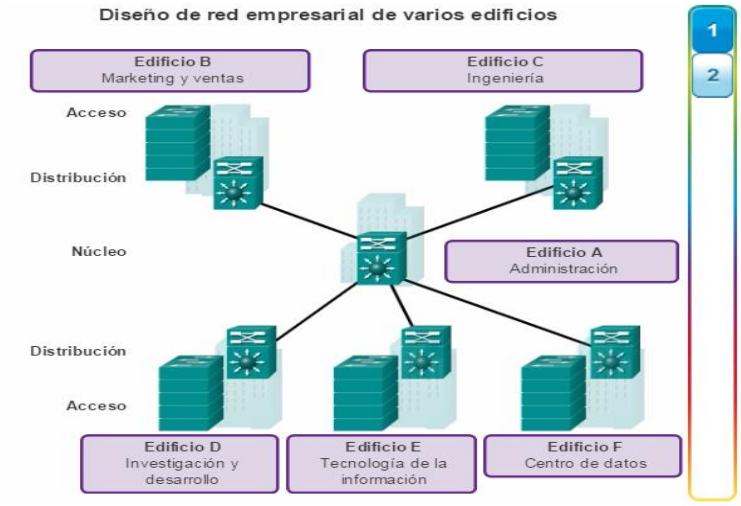
a. **ESTADO DE CPU DE LOS DISPOSITIVOS**. Si el dispositivo recibe demasiadas tramas por medio de su interfaz de red o habilita demasiados servicios (DHCP, DNS, PAT, firewall, antivirus, etc.), su procesador puede fallar y podemos notar una degradación del rendimiento (tramas esperando respuestas, lenta velocidad de respuesta, etc.)
b. **NIVEL DE USO DE LA MEMORIA**. Los dispositivos de la red almacenan varios datos en su memoria. Si esta memoria falla, el rendimiento de la red disminuirá (es posible que se conserven los fotogramas originales, es posible que el comportamiento del dispositivo no coincida con las expectativas, etc.).
c. **NIVEL Y TIPO DE TRÁFICO.** Saber el tamaño y el tipo de tráfico de la red es útil para detectar la congestión y los enlaces débiles que fácilmente la causan. El tipo de tráfico es muy importante porque nos ayuda a detectar la naturaleza del problema. Por tanto, demasiadas solicitudes HTTP pueden deberse a que no tenemos bien planificado el número de conexiones a recibir, pero el exceso continuación de solicitudes DHCP indica que hay un problema grave en la red. Los problemas comunes pueden incluso ser un virus.
d. **OTROS PARÁMETROS.** Otros elementos que pueden también monitorizarse son el espacio que le queda al disco duro, número de conexiones, errores, etc**.**
e. **AVISO Y ALARMAS.** El sistema de monitoreo se puede configurar para registrar cuando algunos de estos parámetros se desvían de sus niveles normales y emiten advertencias o alarmas. En muchos sistemas, estas advertencias y alarmas se envían automáticamente al administrador de la red por mensaje de texto o correo electrónico. Es importante configurar el sistema para avisar si aún no hay problemas, así podemos evitar que sucedan.

1.2.5. Topología de la Red Jerárquica.

Es la forma en que la está diseñada la red y puede definir como un mapa físico o lógico de una red para intercambiar datos. Como se puede ver en la Figura 5 se presenta la topología Jerárquica en donde los nodos se conectan formando una estructura jerárquica.

Figura 5

Topología de Red Jerárquica

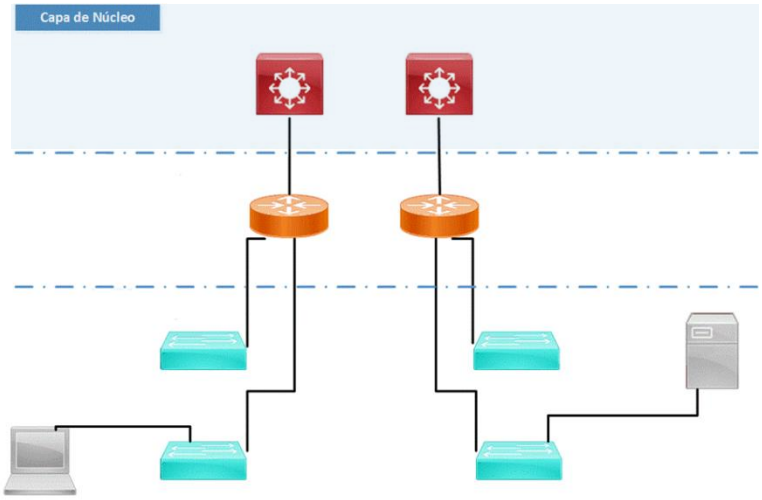


Nota. Modelo de Jerarquico de 3 capas. Reproducida de Jerarquia de Red, de CCNA, 2019 (https://www.reuter.com.ar/CCNA/CCNA4/index_all.html), CC BY 2.0

- **CAPA CENTRAL, NÚCLEO O CORE:** es el troncal de la red, se encuentra el Switch de capa 3, provee altas tasas de transferencia con latencias muy bajas, como se visualiza en la Figura 6.

Figura 6

Nivel central o núcleo

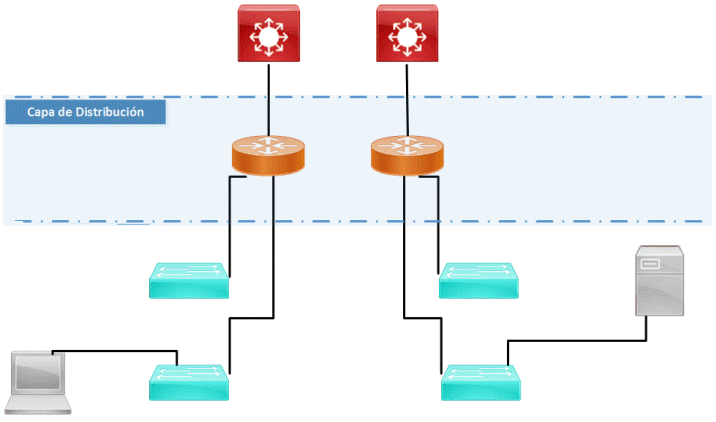


Nota. Capa de núcleo (CORE). Adaptada de Modelo de Tres Capas de Cisco, de Redes Cisco, 2016, Ru83n.c4 (https://ru83nc4.wordpress.com/2016/01/15/modelo-de-tres-capas-de-cisco/). CC BY 2.0

- **CAPA DISTRIBUCIÓN:** se encuentra los puntos de acceso inalámbricos, switch de capa 2, dividiendo los dominios de broadcast, por medio de VLANs, tal cual se muestra en la figura 7.

Figura 7

Nivel de Distribución.

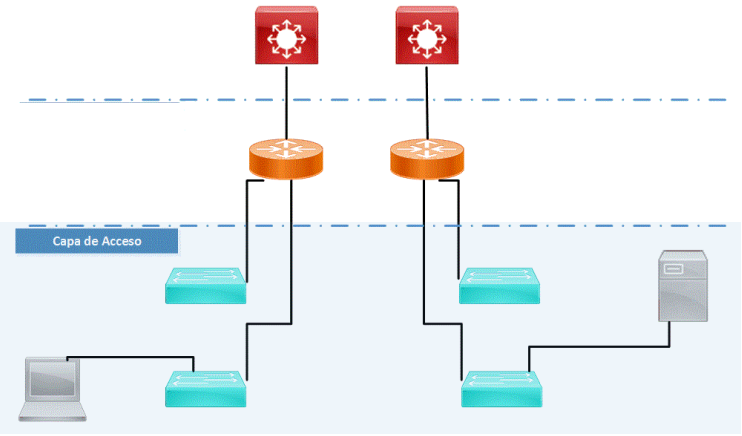


Nota. Capa de distribución. Adaptada de Modelo de Tres Capas de Cisco, de Redes Cisco, 2016, Ru83n.c4 (https://ru83nc4.wordpress.com/2016/01/15/modelo-de-tres-capas-de-cisco/). CC BY 2.0

- **CAPA DE ACCESO:** encontramos los dispositivos finales (computadoras, laptops, celulares) conectados al switch y a los Access Point. El objetivo central es mejorar el rendimiento y seguridad de la red del Colegio Santa María Reina, por ello los siguientes cuatro criterios serán los pilares para esta propuesta un ejemplo claro es la Figura 8.

Figura 8

Nivel de Acceso.



Nota. Capa de Acceso. Adaptada de Modelo de Tres Capas de Cisco, de Redes Cisco, 2016, Ru83n.c4 (https://ru83nc4.wordpress.com/2016/01/15/modelo-de-tres-capas-de-cisco/). CC BY 2.0

1.2.6. Protocolo de Enrutamiento

1.2.6.1. El protocolo OSPF.

Su métrica se llama coste, y considera una serie de factores como la banda ancha y la congestión de los enlaces.

OSPF construye además una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los routers de la zona.

1.2.6.1.1. Ventajas de OSPF.

- OSPF ofrece rápida convergencia y escalabilidad en redes muchos mayores.

- Al ser un estándar abierto soporta dispositivos de todos los fabricantes.
- Cada router posee una imagen completa y sincronizada de la red.
- Permite la agrupación de redes.
- Soporte de múltiples métricas.
- Seguridad ante los cambios.
- Balance de carga en múltiples caminos.

1.2.6.1.2. Elementos para la implementación de OSPF.

- **TEMPORIZADORES:** Se requieren 2 tipos de temporizadores: el primero denominado temporizador de un solo disparo y el segundo temporizador de intervalo.
- **IP MULTICAST:** ciertos paquetes OSPF toman la forma de datagramas IP Multicast. Estos paquetes nunca viajan más de un segundo de salto.
- **SOPORTE PARA SUBREDES DE LONGITUD VARIABLE:** el protocolo IP debe soportar la división de subredes de longitud variable.
- **IP SUPERNETTING:** el protocolo IP del router debe soportar la habilidad de agrupar grupos de IP de redes de clase A, B o C en tamaños más grandes llamados super redes.
- **MANEJO DE LISTAS PRIMITIVAS:** gran parte de las funcionalidades de OSPF son descritas en términos de su operación.

1.2.6.1.3. Protocolo Hello.

Es el encargado del establecimiento y mantenimiento de las relaciones entre vecinos. Determina que la comunicación entre vecinos sea bidireccional, son enviados periódicamente a todas las interfaces del router.

1.2.6.1.4. Sincronización de base de datos.

Como OSPF es un algoritmo de enrutamiento de estado de enlace, es muy importante para todas las bases de datos en los routers permanecer sincronizadas, simplifica esto exigiendo que solo los routers adyacentes permanezcan sincronizados.

Router designado

Cada red en OSPF tiene un router designado. El router designado realiza dos funciones principales:

- Generar una publicación de estado de enlace de red en nombre de la red.
- Convertirse en adyacente a todos los demás routers de la red.

Este router designado es elegido por el protocolo Hello, el cual es enviado por un router que contiene la prioridad de dicho router, esta prioridad puede ser configurada en cada interfaz.

Router Designado secundario

Existe un router designado secundario o de respaldo para cada red OSPF siendo también adyacente a todos los routers de la red. Pasa a ser router designado cuando el anterior router designado falla.

1.2.7. Metodología de Diseño de Red Top Down

1.2.7.1. Fase I: Identificación de las necesidades y objetivos de su cliente.

La fase I cubre la fase de análisis de requisitos. Esta fase comienza con la identificación de objetivos de negocio y requisitos técnicos. A continuación, se detalla la tarea de caracterizar la red existente, incluida la arquitectura y el rendimiento de los principales segmentos y dispositivos de la red. Esta fase concluye con un análisis del tráfico de la red, incluyendo el flujo de tráfico y la carga, el comportamiento del protocolo y los requisitos de calidad del servicio. (Oppenheimer, P. 2011, pág.14).

1.2.7.2. Sub- fases.

1.2.7.2.1. Analizar metas y restricciones de negocios.

Implica analizar los objetivos comerciales, entender la estructura corporativa y determinar las necesidades del cliente para diseñar una red eficiente y adecuada. La red debe diseñarse dentro de las restricciones comerciales, como productividad, personal de redes limitado y plazos ajustados, así como también las políticas del lugar de trabajo que podrían afectar el proyecto.

1.2.7.2.2. Análisis de objetivos técnicos y compensaciones.

Implica analizar los objetivos técnicos del cliente para identificar si se implementara una nueva red o se actualizará la red actual, lo que facilita el trabajo de seleccionar la tecnología adecuada que funcionará de acuerdo con las expectativas del cliente.

Los objetivos técnicos típicos incluyen escalabilidad, disponibilidad, performance, manejabilidad, administración, seguridad, adaptabilidad y asequibilidad.

1.2.7.2.3. Caracterización de la red interna existente.

Implica examinar la red existente del cliente, es decir su topología, la estructura física, el rendimiento y comportamiento de la red. Esto a su vez permite identificar los cuellos de botella, así como también la problemática en el rendimiento, pudiendo así identificar los dispositivos de interconexión y los enlaces que deban reemplazarse debido a su capacidad insuficiente para el nuevo diseño.

1.2.7.2.4. Caracterización del tráfico de red.

Implica caracterizar el flujo de tráfico, el volumen de tráfico y el comportamiento del protocolo. Reconociendo las fuentes de tráfico y los almacenes de datos, la documentación del uso de aplicaciones y protocolos, y la evaluación del tráfico de red causado por protocolos comunes. Esto a su vez permite seleccionar las soluciones de red físicas y lógicas adecuadas para cumplir los objetivos del cliente, garantizando la calidad de servicio.

1.2.7.3. Fase II: diseño de redes lógicas.

Durante la fase de diseño de red lógica, el diseñador de red desarrolla una topología de red. Según el tamaño de la red y las características del tráfico, la topología puede variar de simple a compleja, lo que requiere jerarquía y modularidad. Durante esta fase, el diseñador de red también diseña un modelo de direccionamiento de capa de red y selecciona los protocolos de conmutación y enrutamiento. La planificación de la seguridad también forma parte del diseño lógico, el diseño de la administración de la red y la investigación inicial sobre qué proveedores de servicios pueden cumplir con los requisitos de acceso remoto y WAN. (Oppenheimer, P. 2011, pág.14).

1.2.7.3.1. Diseño de una topología de red.

Este diseño es el primer paso en la fase de diseño lógico de la metodología Top Down. La topología de una red interna es un diagrama que muestra los segmentos de la red, los puntos de interconexión y las comunidades de usuarios.

En esta fase se debe identificar las redes y los puntos de interconexión, el tamaño y alcance de la red y las clases de dispositivos de interconexión de redes que serán necesarios.

Para el diseño de redes WAN, la metodología sugiere un diseño de red jerárquico, utilizando un modelo modular por capas.

1.2.7.3.2. Diseño de modelos para direccionamiento y numeración.

Implica utilizar un modelo estructurado sistemático para direccionamiento y denominación de la capa de red (componentes de internetwork, redes, subredes, enrutadores, servidores y sistemas finales), el cual va a permitir ver la jerarquía en la red y reconocer dónde existen los límites de las direcciones e identificar posteriormente los protocolos de direccionamiento a seleccionar.

1.2.7.3.3. Selección de protocolos de conmutación y enrutamiento.

Depende de los objetivos comerciales y técnicos del cliente, teniendo en cuenta una serie de atributos como:

- Características del tráfico de red
- Ancho de banda, memoria y uso de la CPU
- El número aproximado de enrutadores o conmutadores homólogos compatibles
- La capacidad de una red interna para adaptarse rápidamente a los cambios.
- La capacidad de autenticar actualizaciones de ruta por razones de seguridad.

1.2.7.3.4. Desarrollo de estrategias de seguridad de red.

Implica seleccionar las técnicas correctas para implementar estrategias efectivas de seguridad, es decir políticas de seguridad que protejan todas las partes de una red compleja, que incluyen servidores públicos para comercio electrónico, conexiones extranet para socios comerciales y servicios de acceso remoto para usuarios que llegan a la red desde su hogar, sitios de clientes, etc.

1.2.7.3.5. Desarrollo de estrategias de gestión de red.

La gestión de la red es un aspecto importante del diseño lógico de la red, ayuda a la organización a lograr los objetivos de disponibilidad, rendimiento y seguridad, permite analizar el comportamiento de la

red actual, aplicar las actualizaciones de manera adecuada y solucionar cualquier problema con las actualizaciones.

Esta fase debe darse lugar dentro del diseño de la red y no al finalizar, por ello deben identificarse estrategias de gestión y seleccionar las seleccionar las herramientas y productos correctos para implementarlas.

1.2.7.4. Fase III: Diseño de red física.

En estafa se, se seleccionan tecnologías y productos específicos que realizan el diseño lógico. El proceso de diseño de la red física comienza con la selección de tecnologías y dispositivos de red del campus, como el cableado, los interruptores Ethernet, los puntos de acceso inalámbricos, los puentes inalámbricos y los routers. El proceso de selección de tecnologías y dispositivos para los requisitos de acceso remoto y WAN continúa. Además, la investigación de los proveedores de servicios que se inició durante la fase de diseño lógico debe completarse durante esta fase. (Oppenheimer, P. 2011, pág.14).

1.2.7.4.1. Selección de tecnologías y dispositivos para redes de campus.

El campus es un conjunto de segmentos LAN con área menor a una milla de diámetro, esta fase implica seleccionar tecnologías LAN para diseños de red del campus, como seleccionar el tipo de cableado, los protocolos de capa de enlace de datos y físicos, y los dispositivos de conexión a red (como conmutadores, enrutadores y puntos de acceso inalámbricos), teniendo en cuenta sus características de escalabilidad, rendimiento, asequibilidad y capacidad de administración.

1.2.7.4.2. Selección de tecnologías y dispositivos para redes empresariales.

Aquí se identifican los protocolos físicos y de capa de enlace de datos y los dispositivos de red empresariales, como los servidores de acceso remoto, tecnología de acceso remoto (PPP, DSL, módems de cable), enrutadores, cortafuegos y concentradores de red privada virtual (VPN). Se ve influenciada por las tecnologías de campus, identificadas inicialmente como el ancho de banda y los requisitos de rendimiento del tráfico que fluye de un campus a otro.

1.2.7.5. Fase IV: Probar, optimizar y documentar el diseño de su red.

Los pasos finales en el diseño de red descendente son escribir e implementar un plan de prueba, crear un prototipo o piloto, optimizar el diseño de la red y documentar su trabajo con una propuesta de diseño de red. Si los resultados de su prueba indican algún problema de rendimiento, durante esta fase debe actualizar su diseño para incluir funciones de optimización tales como la configuración del tráfico y los mecanismos avanzados de puesta en cola y conmutación del enrutador. (Oppenheimer, P. 2011, pág.14).

1.2.7.5.1. Probar el diseño de red.

Es un paso crítico en el análisis de sistemas. Ayuda a probar que el diseño de red, cumple con los objetivos comerciales y técnicos del cliente. Probar, predecir y medir el rendimiento, permite definir la calidad de servicio que proporcionara el diseño de red. Seleccionar los procedimientos y herramientas adecuadas de prueba depende de los objetivos, generalmente incluye:

- Verificar que cumpla con los objetivos comerciales y técnicos clave.
- Validación de la tecnología LAN y WAN y selecciones de dispositivos.
- Verificación de que un proveedor de servicios proporciona el servicio acordado.
- Identificar cuellos de botella o problemas de conectividad.
- Probar la redundancia de la red.
- Análisis de los efectos en el rendimiento de las fallas de enlace de red.

1.2.7.5.2. Optimizar el diseño de red.

Esta fase, es crítica para toda aquella organización que utiliza aplicaciones de ancho de banda y son sensibles al retraso. Es indispensables una comprensión solida de la topología lógica y física de la red, para determinar que enlaces que comparten las aplicaciones, necesitan técnicas de optimización.

1.2.7.5.3. Documentar el diseño de red.

En esta fase del proceso de diseño, se debe contar con un diseño integral que se basa en los objetivos técnicos y comerciales del cliente, con componentes lógicos y físicos, probados y optimizados. En el documento de diseño, se debe describir:

- Los requisitos del cliente, así como la explicación de cómo el diseño implementado cubre dichos requerimientos.
- La red existente, el diseño lógico y físico.
- Planes para implementar la red, medir los avances y adaptar el diseño a medida que surjan nuevos requerimientos.

CAPÍTULO II

2. MÉTODOS Y MATERIALES

2.1. Diseño de la investigación

La investigación es de tipo aplicada, explicativa y observacional por lo que no se intercede o manipula las variables del estudio, por lo tanto, se observará lo que ocurre con las variables de estudio en condiciones naturales en la realidad, además es experimental.

Para el desarrollo del trabajo se han tenido en cuenta las siguientes etapas y procedimientos:

- **RECOLECCIÓN DE INFORMACIÓN:** para cada tiempo considerado se colectaron datos sobre:
- **DISEÑO Y ARQUITECTURA DE GESTIÓN Y SEGURIDAD:** relacionado a las redes y su conexión óptima entre cualquier cantidad de nodos, teniendo en consideración los niveles de seguridad que se puedan requerir.
- **RENDIMIENTO DE LA RED INFORMÁTICA:** relacionado con el conjunto de mecanismos que se utilizan para configurar, operar, gestionar, disponer y listar los recursos en la red que soportan los tráficos de flujo de información

Diseño de tipo cuasi experimental.

$$G \quad 0_1 \quad X \quad 0_2$$

Donde:

G	**=**	**Grupo de estudio**
O1	**=**	Diseño y arquitectura de Gestión y Seguridad en el colegio Santa María Reina, antes de aplicar la solución propuesta.
X	**=**	Diseño y Arquitectura de Gestión y Seguridad para Mejorar el Rendimiento de la Red Informática del Colegio Santa María Reina de Chiclayo
O2	**=**	Diseño y arquitectura de Gestión y Seguridad en el colegio Santa María Reina, después de aplicar la solución propuesta.

Fuentes: Elaboración Propia

Las técnicas aplicadas (encuestas), se realizaron de forma manual, los Software Cisco Packet Tracer v.7.1, Software VMware Workstation Pro, Software Autocad, Software GNS3, para simular la red, y realizar diseños técnicos. También utilizaremos el paquete Microsoft Office para la sistematización de datos, concretamente Microsoft Excel, que es un programa integrado que combina una hoja de cálculo, gráficas y macros en un mismo paquete, bajo el sistema operativo Windows 10.2.2. Población y muestra

2.1.1. Población

El trabajo de investigación se desarrollará en las instalaciones del Colegio Santa María Reina, de Chiclayo, y estará conformada como se muestra en la Tabla 1:

Tabla 1.
Resumen de la Población.

DESCRIPCIÓN	SUBTOTAL	%
Alumnas	1036	92.01
Profesores	60	5.33
Administrativos	30	2.66
TOTAL	**1126**	**100,00**

Fuente: Registros del Colegio Santa María Reina de Chiclayo.

Interpretación:

- Alumnas:	Está comprendido por el total de alumnas que tienen entre 10 a 17 años, es decir que cursan el 5to y 6to de primaria y del 1ro a 5to de secundaria. Debido a que a partir de esa edad puedan responder al cuestionario y equivale el 92.01% de la población
- Profesores:	Esta comprendido por el total de profesores contratados en el año 2018 y equivale el 5.33% de la población.
- Administrativos:	Esta comprendido por el total de administrativos contratados en el año 2018 y equivale el 2.66% de la población.

Fuente: Elaboración propia

2.1.2. Muestra

Para la muestra se hará uso de la siguiente fórmula estadística

$$n = \frac{Z^2\ p\ q\ N}{E^2\ (N-1) +\ Z^2\ p\ q}$$

Dónde:

Z = 1,96

p = 0,7

q = 1-p =1-0,7 =0.3

E = 0,1

Entonces:

$$n = \frac{(1{,}96)^2\ (0{,}7)(0{,}3)(1126)}{(0{,}1)^2\ (1126-1) +\ (1{,}96)^2\ (0{,}7)(0{,}3)}$$

$$n = \frac{908.385}{12.057}$$

$n = 75.34 = 75$

Para obtener mejores estimadores duplicamos el tamaño de la muestra de esta primera aproximación:

n = 75 (2) = 150

Lo que representa que deben aplicarse 150 encuestas, que serán asignadas proporcionalmente al tamaño de la sub población.

Para determinar el tamaño mínimo óptimo de muestra de cada sub población utilizamos la siguiente fórmula:

(Ni / N) n

Tamaño de muestra para las alumnas:

$n_1 = (N_1 / N)\ n = (1036 / 1126) *150 = 138.01 = 138$

Tamaño de muestra para los profesores:

$$n_2 = (N_1 / N)\ n = (60 / 1126) *150 = 7.99 = 8$$

Tamaño de muestra para los administrativos:

$$n_3 = (N_1 / N)\ n = (30 / 1126) *150 = 3.99 = 4$$

Tabla 2.

Resumen de la muestra.

DESCRIPCIÓN	SUBTOTAL	%
Alumnas	138	92.01
Profesores	8	5.33
Administrativos	4	2.66
TOTAL	**150**	**100,00**

Fuente: Elaboración propia

Interpretación:

Como se muestra en la Tabla 2, se cuenta con 138 alumnas, 8 profesores y 4 administrativos, que forma un total de 150 muestras del Colegio Santa María Reina, de Chiclayo.

2.2. Técnicas e instrumentos de recolección de datos

2.2.1. Técnicas

En esta investigación se utilizó la técnica de observación directa, revisiones documentales y cuestionarios.

a. Documentaria.

- Sobre el Diseño y Arquitectura de gestión y seguridad: emplear libros, revistas, diarios y textos, así como otros materiales pertinentes.
- Sobre el Rendimiento de la red informática: Al utilizar libros, revistas, periódicos, documentos, memorias y compendios estadísticos, así como materiales necesarios relacionados con el tema.

b. Observación directa.

A través de la observación se identificará los indicadores a evaluar en la investigación.

c. Cuestionarios.

Se realizaron cuestionarios al personal involucrado para conocer el nivel de conocimiento que tienen los mismos sobre: el servicio de internet, el funcionamiento de la red y el uso de los equipos tecnológicos del colegio Santa María Reina; de esta manera se reforzó los resultados obtenidos.

2.2.2. Instrumentos

Cuestionario.

Se utilizó este instrumento, ya que, facilita al momento de recabar, cuantificar, universalizar y finalmente, comparar la información recolectada.

2.3. Procedimiento de recolección de datos

Se realizó una charla informativa con los directivos de la institución, para ver sus inquietudes acerca de la problemática de la institución aplicando los cuestionarios y/o encuestas respectivas. El procedimiento para recoger los datos, fueron los siguientes:

- Se tiene claro los objetivos propuestos y la variable de estudio.
- Se seleccionó la muestra adecuadamente para obtener la información requerida.

  Se definió las técnicas de recolección de información

  Se elaboró la encuesta para ser entregado a las alumnas, profesores y administrativos en la muestra y así procesar la información para su descripción, análisis y discusión.

2.4. Metodología

2.4.1. Descripción de la Metodología Top Down

La Metodología Top Down es porque nos ayuda a pensar en el problema, está metodología se basa en el paradigma “Divide y Vencerás” lo que significa en dividir el problema en un conjunto de subproblemas menores y empezar con un diseño inicial de cómo debería resolverse es decir nos permite diseñar redes que satisfagan los objetivos técnicos de cualquier organización. Nos facilita procesos y herramientas probados para ayudar a cumplir con los requisitos a lo que se refiere a funcionalidad, disponibilidad, escalabilidad, accesibilidad y seguridad.

Esta metodología que se ha empleado en el desarrollo del proyecto cuenta con cuatro fases. La primera fase análisis del negocio objetivos y limitaciones, aquí conoceremos la línea de negocio, estructura

organizacional de la empresa, así como conocer la situación actual en la que se encuentra la red de la organización. La segunda fase diseño lógico, se diseñará la topología y desarrollaremos estrategias de seguridad y gestión de red, dentro de esta fase hemos creído conveniente aplicar las áreas funcionales de gestión de red: gestión de configuración, gestión de prestaciones, gestión de fallos, gestión de seguridad y gestión de costos. Siguiendo la fase tres, diseño físico aquí se seleccionará que tecnologías y dispositivos se usaran que satisfaga las necesidades de la organización de acuerdo a lo propuesto en la fase anterior. Por último, tendremos la cuarta fase de prueba, optimización y documentación gracias a esta fase podremos saber si nuestro diseño cuenta con los objetivos comerciales y técnicos. La ejecución de esta metodología da lugar a un esquema bien organizado y estructurado que garantiza una solución a largo plazo, auditable e integrada a las diferentes plataformas de comunicación de la ABC.

CAPÍTULO III

3. RESULTADOS

3.1. Fase 1: Identificar las necesidades y objetivos de sus clientes

3.1.1. Parte 1: Análisis de los objetivos y limitaciones del negocio

3.1.1.1. Identificación de las necesidades.

- Nombre de la organización: Centro Educativo Particular “Santa María Reina”.
- Rubro de la organización: Educación.
- Razón Social: Colegio Santa María Reina.
- Fecha de Creación: 22 de agosto de 1963.
- Dirección: Av. Miguel Grau 1132 – Urb. Santa Victoria.
- Contacto: Hna. Aleyda Alejandrina Carrasco Correa.
- Cargo: directora.

El centro educativo, con el avance tecnológico y la evolución de las redes, servicios TI, servidores, seguridad, el cual frente a estas innovaciones de hoy en día se ven obligados a adecuarse y optar por una

tecnología como fuente que permita ir avanzando de acuerdo a su rubro dándole mayor seguridad y gestión a la red.

En la actualidad, el diseño de red existente no cumplen con requisitos de seguridad y sobre todo no tiene un buen rendimiento dentro de la red ya que no se encuentra estructurada de manera correcta y no hay interconexión entre áreas, el cual no permite dar buen servicios a la parte administrativa, a los alumnos en sus clases donde usan laptops, pc's, el cual carece de limitaciones, por eso motivo se ha propuesto el diseño de una arquitectura de gestión y seguridad para mejorar todo lo que con lleva a la red y dar sobre todo integridad, confiabilidad y confidencialidad a los trabajadores de la organización.

3.1.1.1.1. Misión.

"Somos un Centro Educativo Particular acreditado internacionalmente, promovido por la Congregación de Religiosas Franciscanas de la Inmaculada Concepción, que educa integralmente a la mujer, porque de ella depende la familia y la sociedad, en las dimensiones: personal, cognitiva y espiritual, sobre la base de los valores cristianos de Responsabilidad, Respeto, Honradez, Minoridad y fraternidad con una cultura institucional innovadora e inclusiva, para la formación de personas con sentido crítico-creativo, capaces de lograr su transformación personal, social, cultural, académica y espiritual, en bien de nuestra comunidad educativa y de la sociedad peruana".

3.1.1.1.2. Visión.

"Al año 2021, el Centro Educativo Particular "Santa María Reina" se convertirá en el mejor colegio femenino de la región norte, evangelizador de los procesos educativos, promotor de la investigación científica brindando una educación de calidad con una sólida base cristiana y humana, formando personas fraternas, proactivas y competitivas, que afrontan con ética, dignidad y éxito los desafíos y retos de un mundo globalizado".

3.1.1.1.3. Objetivos.

- **NIVEL INSTITUCIONAL**

“Elevar el nivel de organización y competitividad con la participación activa de toda la comunidad educativa que permite el desarrollo de la institución y garantice una sólida formación de la persona en su dimensión humana cristiana y el mejoramiento del servicio que se brinda”.

- **NIVEL PEDAGÓGICO**

“Brindar a nuestras estudiantes una formación humana, científica y cristiana, así como la práctica de valores, actitud crítica, fomentando el espíritu para la investigación y desarrollo de la creatividad, valiéndose de metodología activa, las TIC, con docentes permanentemente actualizados, que garanticen una debida relación consigo misma, con los demás, la familia, la iglesia, la naturaleza y la patria; enmarcados en un currículo pertinente”.

- **NIVEL ADMINISTRATIVO**

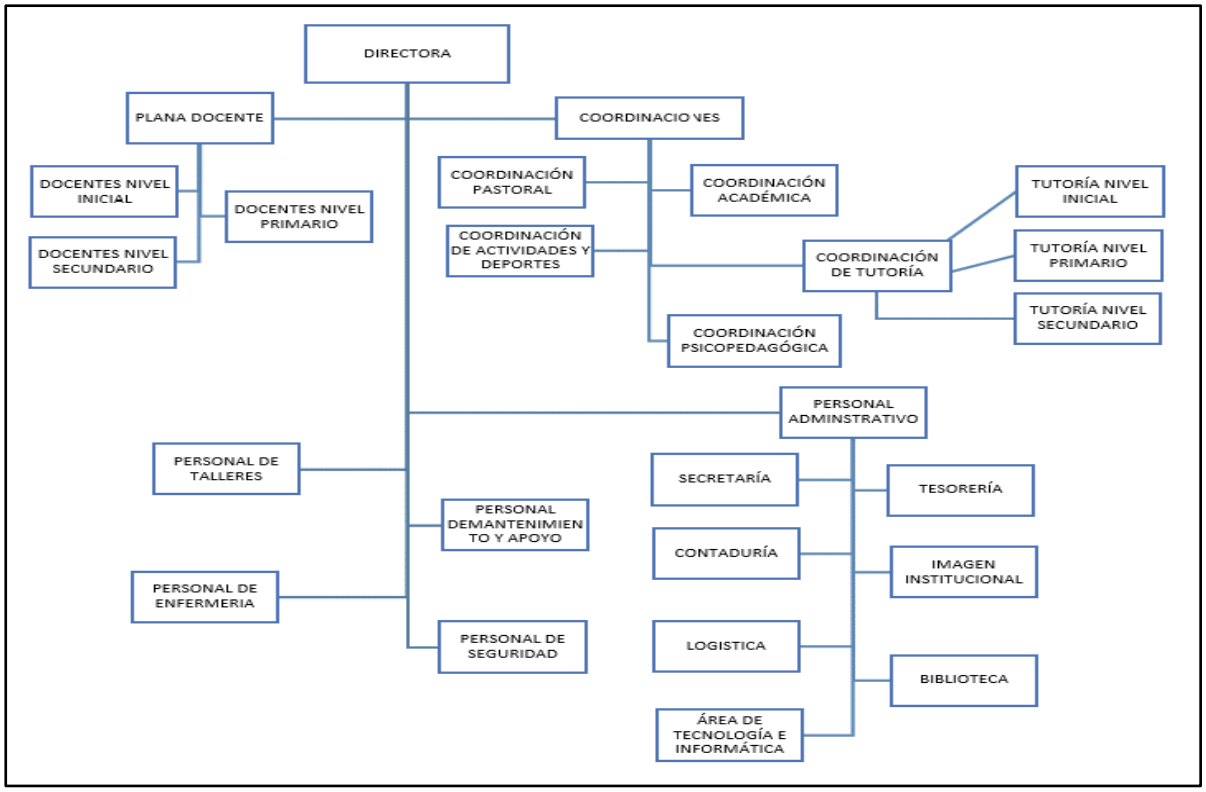
Mejorar la infraestructura y equipamiento, así como el desempeño del personal administrativo en base a una actitud innovadora y práctica de valores, acorde con los adelantos de la tecnología e informática, para propiciar el uso óptimo de los recursos físicos y financieros, efectivizar su labor y favorecer la formación científica y tecnológica en las estudiantes.

3.1.1.2. Organigrama empresarial.

La organización de la institución educativa se detalla de la siguiente forma como se visualiza en la Figura 9.

Figura 9

Organigrama del Colegio Santa María Reina



3.1.1.3. Análisis de restricciones.

La mayor restricción para llevar a cabo un proyecto es el presupuesto en toda organización, además de la actualidad en tema de materiales, mano de obra, infraestructura que nos permita realizar el proyecto, también hay que tener en cuenta que la institución no cuenta con el personal especializado en temas de redes y de proyectos.

3.1.1.4. Objetivos de la implementación de la red informática.

3.1.1.4.1. Objetivo general.

Diseñar la Arquitectura de Gestión y Seguridad en el Rendimiento de la red informática de la C. E. P. Santa María Reina, de Chiclayo.

3.1.1.4.2. Objetivos específicos.

- Identificar y Analizar los objetivos generales y técnicos del colegio Santa María Reina para poder así conocer e implementar nuevas tecnologías que cumplan con las expectativas de la Institución Educativa.
- Analizar el estado actual de la red, así como el nivel de seguridad Informática para poder identificar posibles y potenciales problemas, que permita mejorar la infraestructura de Red y Seguridad.
- Diseñar una topología de red que cumpla con los requerimientos técnicos para poder identificar los puntos de interconexión, el alcance de la red y los tipos de dispositivos que serán requeridos.
- Diseñar estrategias y políticas de seguridad que más se ajusten a las necesidades de la institución educativa para salvaguardar la información en su totalidad, y que usuarios autorizados puedan acceder a ella.
- Proponer y seleccionar las tecnologías y productos para la red del Colegio Santa María Reina, según la topología de red que se va a implementar y las políticas de seguridad que se van a establecer.
- Organizar, desplegar y controlar todos los recursos necesarios para aumentar eficiencia, reducir riesgos, incrementar calidad, proveer mejores servicios o incrementar la rentabilidad organizacional.
- Probar el diseño de la red ya establecida para así poder verificar que las soluciones que hemos desarrollado proporcionaran la performance y la calidad que el Colegio Santa María Reina espera.

3.1.2. Parte 2: Análisis de los objetivos y limitaciones del negocio

3.1.2.1. Objetivos del negocio.

3.1.2.1.1. Escalabilidad.

El esquema de nuestra red debe ser eficiente para adaptarse al rendimiento de la red en términos de uso y alcance; en otras palabras, indica al crecimiento que debe acomodar un diseño de red. Es fundamental recordar que las tecnologías de red tienen muchas limitaciones en lo que respecta a la escalabilidad.

Disponibilidad.

En el colegio Santa María Reina la red estará disponible las 24 horas del día los 7 días a la semana, Es un objetivo crítico común para el diseño de redes, y basándonos en los datos que calculamos, el alumno está de acuerdo a esperar un máximo de 10 minutos.

A continuación, se detalla si nuestra red estará en alto nivel de disponibilidad:

Disponibilidad de la Red:

Tiempo Ideal = 24 (horas/día) x 7 (días/semana)

Tiempo Ideal = 168 (horas/semana) x 60 minutos

Tiempo Ideal = 10080

Tiempo Aceptable = Tiempo Ideal – Tasa de Perdida

Tiempo Aceptable = 10080 – 10

Tiempo Aceptable = 10070

Tasa de Disponibilidad (TD) = (TA/TI) *100

Tasa de Disponibilidad (TD) = (10070/10080) *100

Tasa de Disponibilidad (TD) = 99.90%

Nuestro índice de disponibilidad es alto, lo que indica que la red de datos funciona correctamente. Asimismo, los servicios de TI serán fiables y operativos y estarán correctamente mantenidos.

3.1.2.1.2. Performance.

Nuestra red nos facilitará evaluar el rendimiento y la protección de la estructura de la red. A través de una serie de técnicas y estudios, mediante mediciones de tráfico y un minucioso análisis del comportamiento de la red.

3.1.2.1.3. Seguridad.

El diseño de nuestra red ofrecerá protección en los datos, servicios y otros recursos que se puedan perder, dañar o que sean de gran importancia para la Institución educativa. Las alumnas y el personal del colegio tendrán diferentes políticas de acceso a internet, de esta forma estarán proseguidos de contenidos maliciosos. La Institución Educativa está distribuida de la siguiente manera. Ver Tabla 3.

Tabla 3.

Atributos de Seguridad.

ÍTEM	ATRIBUTO	ATRIBUTOS TÉCNICOS
1	**SISTEMAS OPERATIVOS EN PC´S DE TRABAJO**	• Windows 7 de 32 y 64 bits. • Windows 10 de 64 bits.
2	**ANTIVIRUS**	• NOD 32.
3	**PREVENCIÓN Y DEFENSA FRENTE A ATAQUES EN PORTÁTILES Y PC'S.**	• Se controlará y/o autorizará el uso de aplicaciones no deseadas. • Resolver la seguridad integrada para las estaciones y los servidores incluye un único agente que protege contra virus, spyware, adware, rootkits, conducta sospechosa, filtrado de la seguridad de las URL, En todos los protocolos de red, detecta ataques de scripts maliciosos en la Web y en aplicaciones potencialmente peligrosas.
4	**SEGURIDAD**	• Para garantizar que sus procesos, servicios, archivos o archivos de registro no se detienen, deshabilitan, borran o modifican en caso de un ataque de virus. • La solución debe incluir características de seguridad para garantizar que el usuario de la estación de trabajo, ya sea un administrador de la red o un PC, no viola las políticas de seguridad corporativa.

Fuentes: Elaboración Propia

3.1.2.1.4. Adaptabilidad.

Nuestra red va a estar diseñada para adaptar tecnología futura, el Colegio Santa María Reina tiene conspirado crecer a nivel local, por lo que diseñaremos una red para que llegue a un área geográficamente extensa cuando llegue el instante de implementar un enlace de red WAN.

3.1.2.1.5. Manejabilidad (Administración).

El diseño de la red que proponemos será fácil de gestionar y monitorizar, es por ello que debemos saber los objetivos de los de los usuarios y de los servidores, gracias a ello simplificaremos las metas de los administradores de red con sus clientes.

3.1.3. Parte 3: Graficando la red existente

3.1.3.1. Descripción de la red existente.

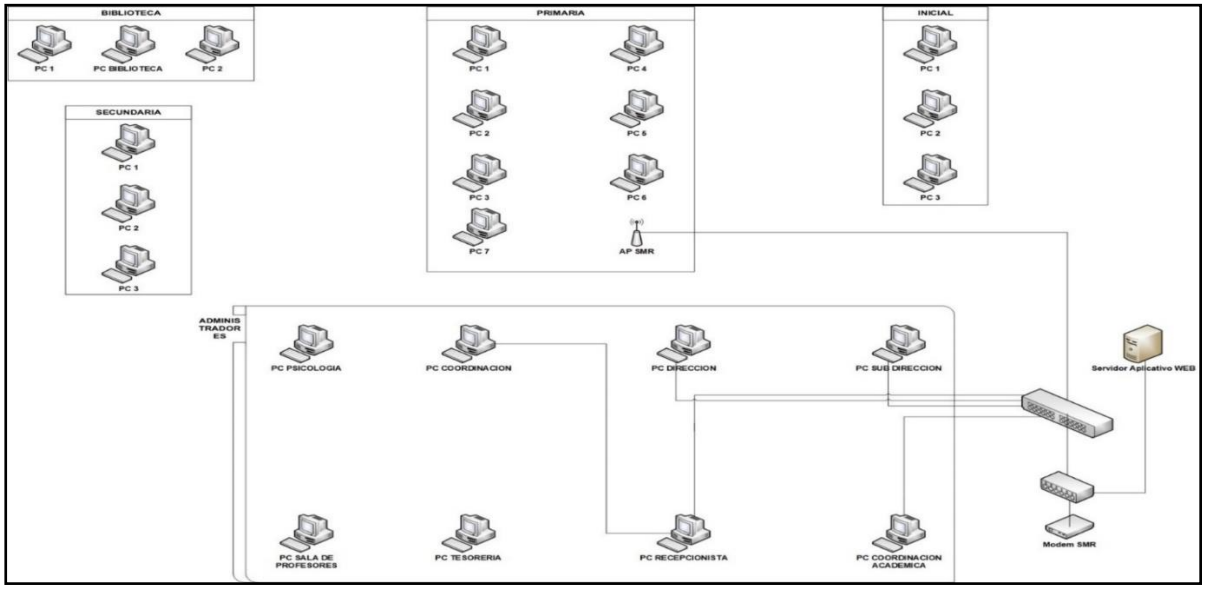
Actualmente la institución educativa cuenta con una red LAN Y WLAN, la red de área local instalada en el año 2013, inicialmente se contaba con 12 puntos de red distribuidos en los principales sectores administrativos, cabe indicar que para efectuar dicha instalación se utilizó la Categoría 5, con el transcurrir del tiempo se ha incrementado los requerimientos de instalación de puntos de red en los demás sectores del colegio como aulas, biblioteca y laboratorios pero no se ha llegado a efectuar. El total de computadoras son 20 pero conectadas a la red solamente son 12 computadora todas del sector administrativo. Además, alberga dos aulas móviles de 30 laptops cada una y 60 laptops en un laboratorio con lo cual hacen un total de 100 laptops que las alumnas no pueden usar en su totalidad, por lo que el WIFI no llega a algunas aulas y pabellones, es lento y sólo abastece el 30% de todos los ambientes del colegio. Con respecto a los estándares de red no cuentan con ningún estándar de red dentro de su red física, ni de su cableado estructurado, ni sobre la gestión de redes, con respecto a la seguridad física y lógica, actualmente no tienen un inventario general de sus redes, no cuenta con una buena distribución de la red dentro de sus áreas (subneteo, VLANs, etc., no tienen control de la red, por lo cual se tiene acceso por ejemplo a todas las páginas, descargas, etc., saturando la red del colegio, por lo cual no tienen una gestión de red para limitar estos tipos de accesos y descargas.

Se han aplicado encuestas para poder decepcionar este tipo de información y así tomar decisiones para mejorar el rendimiento de la red dentro del Colegio Santa María Reina, de Chiclayo.

3.1.3.2. Gráfico del diseño de la red actual.

Figura 10

Red actual de Colegio Santa María Reina de Chiclayo



3.1.3.3. Descripción física de los equipos en el Colegio Santa María Reina.

La red informática del Colegio Santa María reina, consta de computadoras y laptops, además indicar que el cableado estructurado de la red se ha ido modificando y adaptando según las necesidades dentro de la organización, también indicar que los algunos equipos de cómputo no se encuentran prevenidos de manera adecuada, ya que no tienen estabilizadores. A continuación, se muestra un detalle de los equipos de la institución educativa, Ver tabla 4.

Tabla 4.

Computadoras existentes en el Colegio Santa María Reina.

ÁREA	N° COMPUTADORAS		
	CONECTADAS A LA RED	**NO CONECTADAS A LA RED**	**TOTAL**
ADMINISTRATIVOS	**12**	07	12
AULAS DE INICIAL	Ninguna	07	07
AULAS DE PRIMARIA	Ninguna	24	24
LABORATORIO INICIAL	Ninguna	15	15
LABORATORIOS SECUNDARIA	Ninguna	20	20
AULAS MOVIL 01	Ninguna	30	30
AULAS MOVIL 02	Ninguna	30	30
BIBLIOTECA PRIMARIA	Ninguna	05	05
BIBLIOTECA SECUNDARIA	Ninguna	03	03

Fuentes: Elaboración Propia

3.1.3.3.1. Inventario del Software.

Sobre el inventario de software que se tiene en la institución, podemos indicar que se cuenta con lo siguiente, Ver tabla 5.

Tabla 5.

Software utilizado en el Colegio Santa María Reina

AREA	SISTEMA OPERATIVO	LICENCIAS
ADMINISTRATIVOS	Ms Window10	Home Single Languaje
LABORATORIOS	Ms Window07	Home Basic
BIBLIOTECA	Ms Window07	Home Basic
AULAS	Ms Window07	Home Basic
TALLERES	Ms Window07	Home Basic

Fuente: Elaboración Propia

3.1.4. Parte 4: Caracterizando un diseño del tráfico de la red

3.1.4.1. Análisis de la red actual.

La red del Colegio Santa María Reina cuenta con una infraestructura de red de datos de topología anillo ya que los puntos finales de la red están conectados a un conmutador central a través de un enlace punto a punto, cuyo funcionamiento no se encuentra segmentado, la asignación de IP's privados en las PC de los administrativos este direccionamiento es por DHCP.

Sus equipos de comunicación son un modem router de marca TP-Link, cinco switches de marca TP-Link no configurables y un switch Cisco 877. El cableado estructurado no está implementado de acuerdo a los estándares de calidad.

La red WLAN del colegio Santa María Reina es desordenada que no cumple con los requerimientos de las estudiantes ni del personal administrativo ya que no tiene acceso a la información de manera oportuna, existe pérdida de tiempo e ineficiencia. La Institución Educativa cuenta con una Antena TP-LINK de 2.4 GHZ, a velocidad media de 5dBi con un enlace inalámbrico de 5 km y esta se encuentra mal ubicada.

3.1.4.2. Análisis del tráfico de la red.

Velocidad de la Red: El análisis tráfico de la red es muy bajo contando con tan solo 16 MBps, pero la velocidad que le llega a cada ordenador es aproximada 2.37 Mbps con 136 ms de latencia, ya que no abastece todas las aplicaciones y la cantidad de usuarios que circulan por la red. Se realizó un análisis que permite identificar qué tipo de información circula por la red y como es que este afecta sobre la misma, así como diferentes servicios que se emplea en el Colegio Santa María Reina. Para poder realizar un análisis de la red actual se ha usado Speedtest por Ookla como se detalla en la Figura 11.

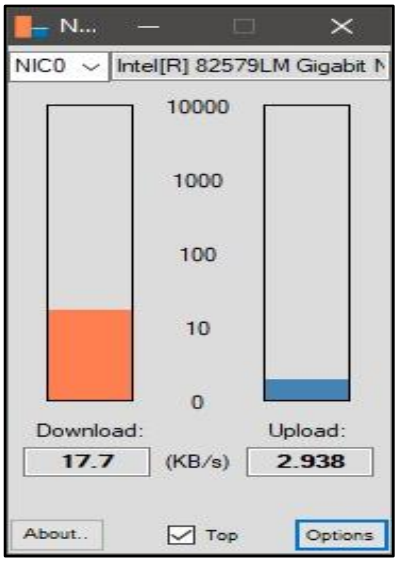
Figura 11

Análisis de red del Colegio Santa María Reina

Ancho de Banda usando NetTraffic: NETTRAFFIC es una aplicación para Windows que permite medir y visualizar el ancho de banda de nuestros dispositivos de red, ya sean adaptadores WiFi o tarjetas Ethernet tradicionales, sin tener que recurrir a servicios online como Speed.io o Speedtest.net, siendo así posible también la medida de nuestro ancho de banda local, si por ejemplo utilizamos un servidor de ficheros en nuestro sistema.

Figura 12

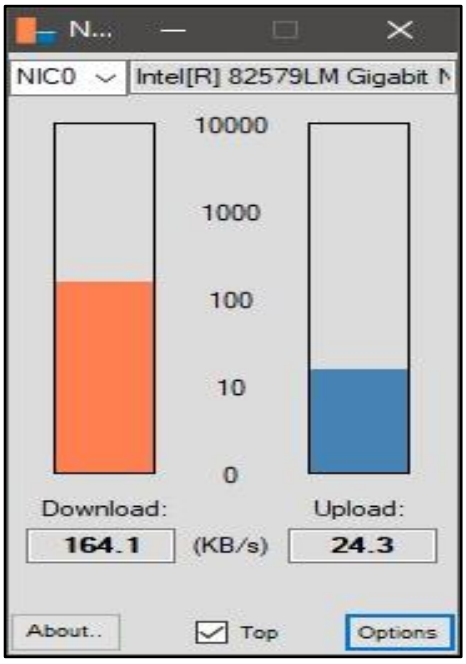
Ancho de banda utilizando navegador



En la figura 12, podemos visualizar con el software NetTraffic el ancho de banda consumido en un ordenador del colegio Santa María reina, cuando se conectan al sistema del colegio usando el navegador web Google Chrome. Es por ello que tenemos un menor consumo de Download y de Upload.

Figura 13

Ancha de banda utilizando Gmail.



En la figura 13, podemos visualizar con el software NetTraffic el ancho de banda consumido en un ordenador del colegio Santa María reina, cuando se estaba usando el servidor de correo Gmail y algunas pestañas del navegador web. Es por ello que tenemos más consumo de Download y de Upload.

Correo Electrónico: El personal administrativo, docentes y alumnas hacen uso del correo electrónico gratuito gmail y hotmail.

Base de Datos: Almacena un sistema básico de Registro de Matrícula hecho en PHP con una base de datos en MySQL que la almacena las estudiantes, dicho sistema es manejado por el área de secretaria.

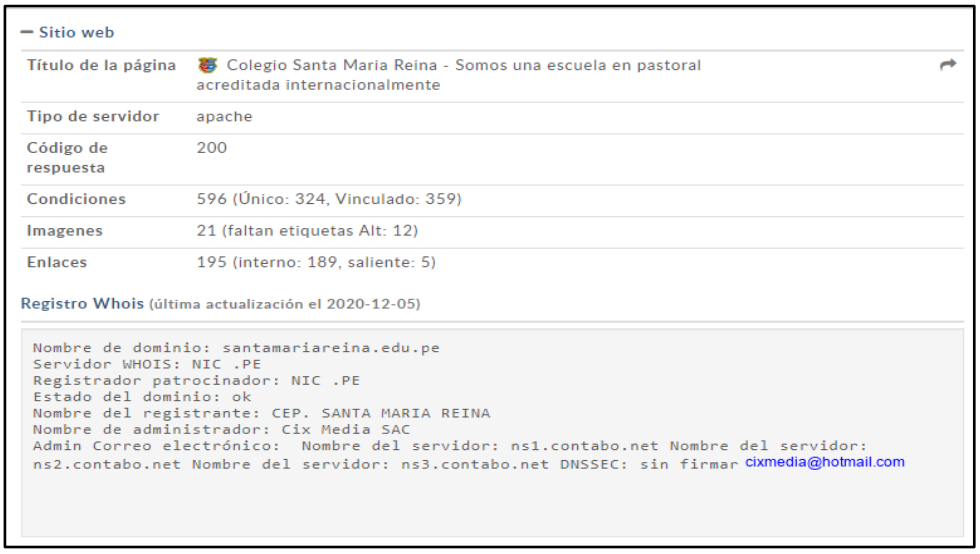
Web: El colegio tiene una página web cuyo link es https://www.santamariareina.edu.pe/, está almacenado en la nube, para conocer la situación actual del dominio Ver Figura 14 y Figura 15.

Figura 14

Situación actual del dominio

Figura 15

Características del dominio.



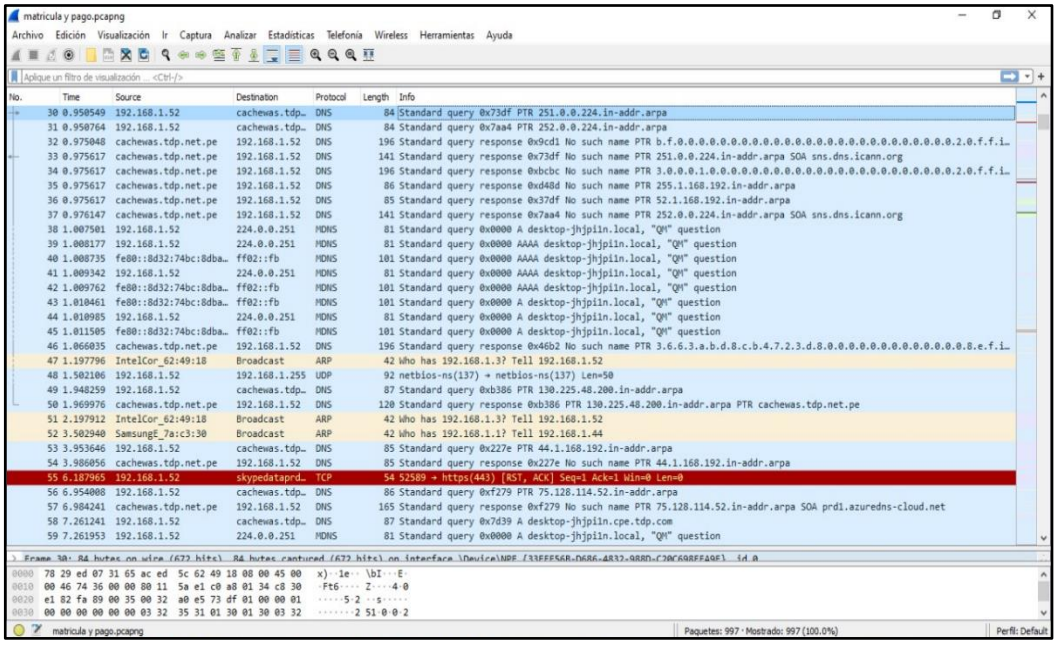
3.1.4.3. Análisis de rendimiento de la red.

En este análisis se puede notar lo congestionada que esta la red debido a la velocidad insuficiente de las líneas, carencias de estrategias de calidad de servicio y mala infraestructura tecnológica que no cumple con las normas adecuadas de velocidad. Para verificar el rendimiento de la red, hemos usado Wireshark, el cual nos ayudó a verificar el uso de la red dentro del colegio por parte de los docentes, administrativos, etc., el cual no solo se usa para ver el rendimiento de la red, sino también para examinar algún problema de seguridad, para la implementación de protocolos de red.

Wireshark nos ayuda a verificar la captura de paquetes en vivo desde una interfaz de red, filtrado de información de paquetes, importa y exporta diferentes formatos de paquetes, etc. Es por ello, que se realizó un análisis obteniendo lo resultados como se detalla en la Figura 16 y Figura 17.

Figura 16

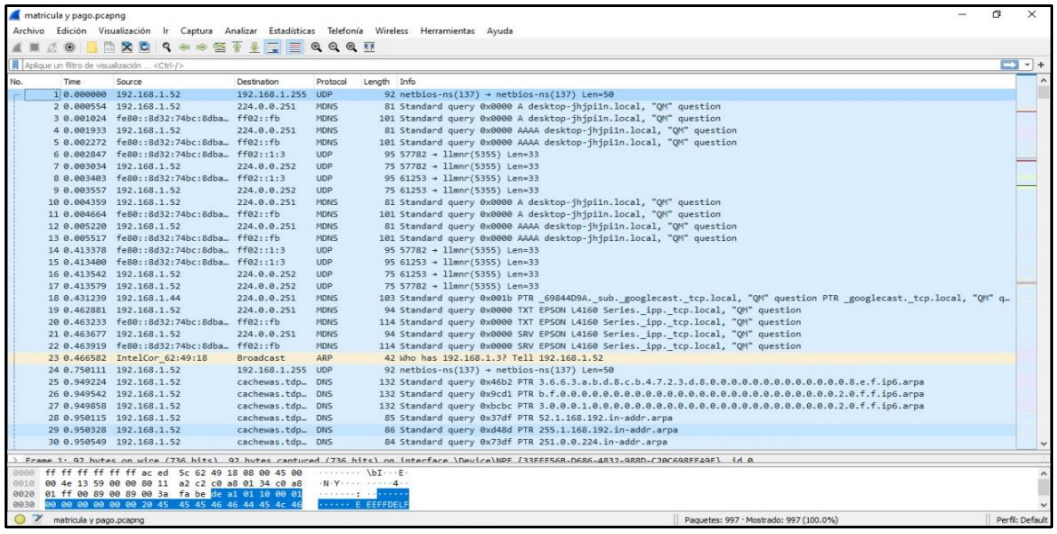
Rendimiento de la red usando, Wireshark



.

Figura 17

Tráfico de la Red usando Wireshark



3.1.4.4. Análisis de seguridad de la red.

En el Colegio Santa María Reina, de Chiclayo, se detectaron las siguientes vulnerabilidades:

- No hay ningún firewall que ayude a controlar los problemas dentro de la institución asimismo no hay una gestión de red adecuada, haciendo que todo procedimiento o uso de ella sea vulnerable a los ataques o robo de información dentro de la institución.
- La red interna carece de políticas de seguridad, como permisos y restricciones sobre dispositivos intermediarios en la red.
- Falta de parametrización al acceder a recursos compartidos. Falta la ACL (Lista de control de acceso) para el filtrado de paquetes interno y externo.
- No existe un servidor de autenticación para el acceso, control y gestión de los dispositivos intermediarios de la red.
- Acceso incontrolado a los servicios de Internet.
- Falta de mecanismos de protección y aislamiento de equipos finales.
- El enrutador principal no tiene seguridad avanzada.

- Los servidores no están alojados adecuadamente en armarios rack con climatización y sistemas de enfriamiento, también se encuentran en un lugar accesible de manera sencilla, lo que provoca que exista una inseguridad a nivel físico, debilidades y peligros para los datos de la entidad educativa.
- Cualquier personal administrativo puede acceder a la máquina de otro usuario, ya que este no cuenta con contraseñas seguras, ni políticas de seguridad que debería tener el computador.

3.2. Fase 2: Diseño lógico

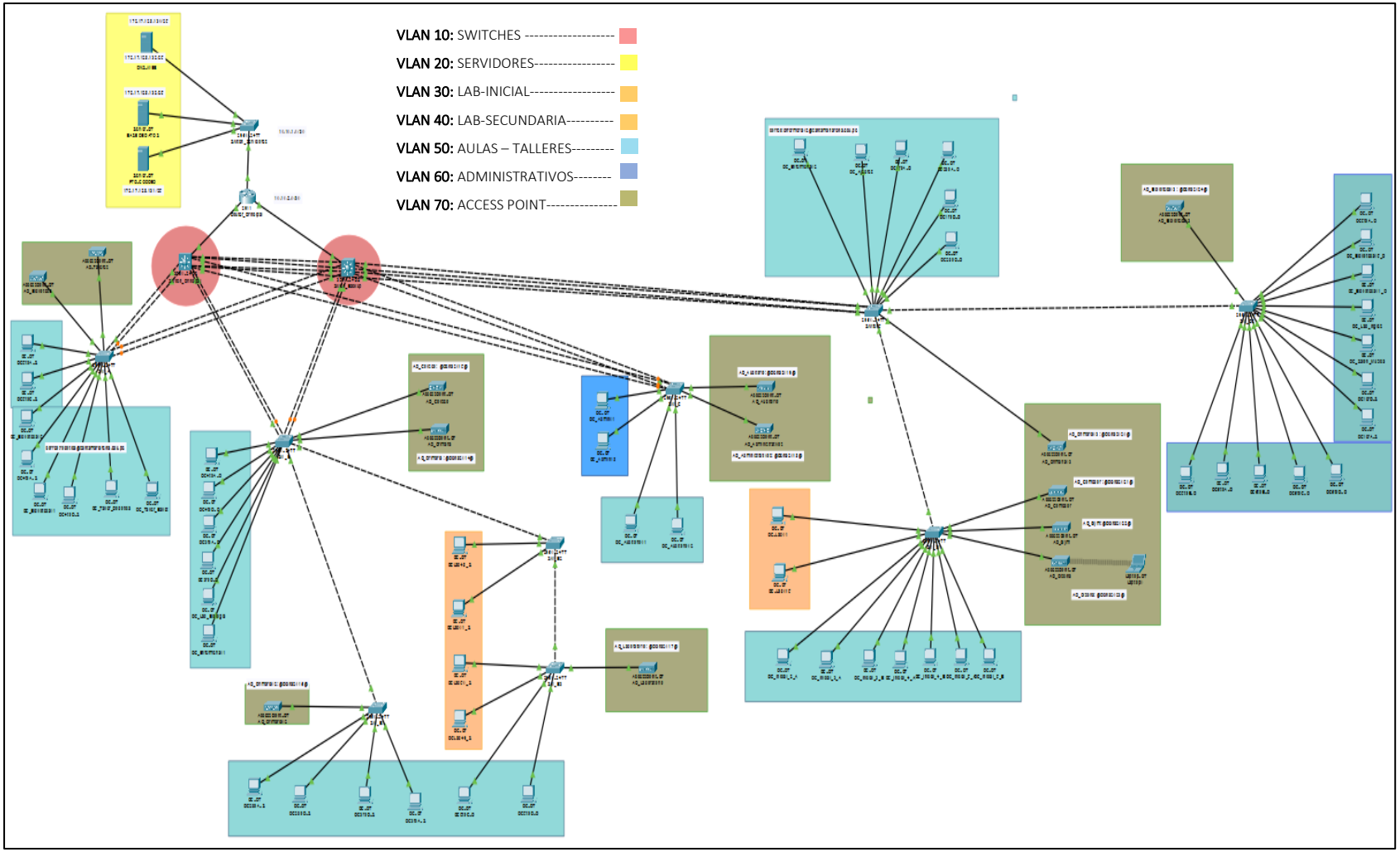
3.2.1. Parte 5: Diseño de una topología

3.2.1.1. Diseño de la topología de la red.

Con el modelado y topología planteada con el fin de dar solución en mejorar el rendimiento de la red del Colegio Santa María Reina se usará una red jerárquica en tres capas, cuyo estudio y de acuerdo a las necesidades se realizó una segmentación adecuada para el diseño. Para plantear nuestra solución hemos decidido usar el software Packet Trasert, y poder distribuir las diferentes áreas y nivel de educación en VLAN's para un mejor entendimiento, que se detalla en la Figura 18.

Figura 18

Diseño de la Topología de la Red del Colegio Santa María Reina, de Chiclayo



3.2.1.2. Desarrollo de la seguridad de la red.

A continuación, se detallará los métodos que utilizaremos para mantener niveles altos de seguridad en nuestra red.

3.2.1.2.1. Nivel de seguridad de software.

- **CERTIFICADO DIGITALES**

Se comprará certificado digital para darle seguridad a la página web del Colegio Santa María Reina, de Chiclayo.

- **CONTROL DE ACCESO**

Se requiere restringir el acceso a los dispositivos e internautas que no tienen autorización, en caso intenten ingresar a la red. Los usuarios a los que se les ha concedido acceso a Internet sólo pueden acceder a utilizar la página web, esto se podrá lograr con Grupos de Active Directory, todo el personal administrativo estará bajo el control del servicio de Active Directory y con la creación de los grupos de distribución y seguridad se le podrá asignar derechos y privilegios de usuario a grupos de seguridad, asignar permisos. Es por ello que la organización de Active Directory, el contenido limpio y claro serán la clave para tener un control de los usuarios en la red. Para garantizar que los GPO funcionen en las estaciones de trabajo de los usuarios finales, deben aplicarse de acuerdo con ciertas reglas establecidas y siguiendo una jerarquía bien definida.

- **ANTIVIRUS**

Implantación de una aplicación para prevenir y detectar programas peligrosos como virus, troyanos y scripts, con el fin de reducir el riesgo de fallo del sistema o pérdida de datos, la idea es prevenir infecciones que se dirige a la red.

Se realizó un estudio de mercado de los antivirus corporativos tales como, ESET, Kaspersky y McAfee, optando por el Antivirus Kaspersky Endpoint Security Select ya que ofrece una mejor seguridad a un menor costo. En la Figura 19, se detalla una comparación entre los mejores antivirus.

Figura 19

Comparación de Antivirus.

Nota. Comparación de los mejores antivirus. Reproducida de Los Mejores Antivirus en General, de SafetyDetectives, 2022, SafetyDetectives (https://es.safetydetectives.com/comparison/). CC BY 2.0

Asimismo, se ha realizado una cotización del antivirus KASPERSKY mostrando un precio que es accesible para los gastos de la institución educativa. Ver Figura 20.

Figura 20

Cotización de Antivirus Karpesky.

Engi Perú

KASPERSKY certified partner

FORTINET PARTNER

Adobe

Sophos Gold Partner

24/11/2020

Emitido desde ENGIPERU CRM

Cotización Nro. 10445- 2020

Sres:I.E Santa María Reina

Contacto: Sr. Diego Antonio Valdera Limo
Dirección: Av. Miguel Grau 1132 (Urb. Santa Victoria), CHICLAYO CHICLAYO LAMBAYEQUE
Incluye :
- Soporte ilimitado 8x5
- Renovación de Licencias
- Tiempo de Licencias: 3 meses

Forma de pago: Contado
Tiempo de entrega: 72 Horas hábiles
Tipo de cambio: Tipo de cambio de venta del día del BCP
Emitido por :Rosmeri Zea

Producto	Duración	Precio Unit.	Cantidad	Total
KASPERSKY ENDPOINT SECURITY SELECT Ofrece la solución de protección y manejo que necesita su organización para aplicar la política de TI, mantener a los usuarios libres de malware, evitar perdida de datos y mejorar la eficiencia de TI. Licencia Corporativa - System Watcher (Detecta comportamiento anómalo en los equipos y lo detiene) - Auditoria de Hardware y Software - Antimalware, Firewall, Control Web - Control de aplicaciones. - Marcado de aplicaciones en lista blanca - Control de dispositivos - Protección de servidor de archivos - Manejo del dispositivo móvil - Seguridad para Endpoint móvil: Para tablets y Smartphones - Proteccion asistida en la Nube con Kaspersky Security Network.	Meses	$7.00	80	$560.00

Total	$ 560.00
Descuento	$ 0.00
SubTotal	$ 560.00
IGV (18%)	$ 117.18
Envio	$ 0.00
Gran Total	$ 677.18

- **FIREWALL DE SEGURIDAD**

Se implementará un Firewall de seguridad para permitir o denegar accesos, descargas, a los usuarios de la red.

- **SEGURIDAD EN CORREO ELECTRÓNICO**

Hacer uso de certificaciones digitales que aseguren la integridad de los datos y un programa que sirva para filtrar información, así como medidas de protección para la organización evitando programas maliciosos que se propagan por estos canales.

- **SEGURIDAD PARA LAS APLICACIONES**

Aplicación de máquinas y tecnologías para asegurar la confidencialidad de la información y el monitoreo de accesos, así como analizar las vulnerabilidades de los programas, utilizando un conjunto de recomendaciones y estándares de seguridad.

3.2.1.2.2. Nivel de seguridad de hardware

- **EQUIPOS MIKROTIK ROUTEROS**

Se implementará en nuestra red, el Mikrotik RouterOS, siendo el sistema operativo y programa del router. Se tomó esta alternativa por la seguridad, la versatilidad y la rentabilidad del equipo, lo que genera mayor beneficio hacia el Colegio Santa María Reina debido a que la red en esta institución es de una extensión intermedia. Mikrotik RouterOS mantendrá la red segura puesto que se crearán reglas de acceso restringiendo y monitoreando la navegación de los usuarios de la red a través de internet, permitiendo establecer políticas y limitaciones a los equipos de las diversas áreas del colegio reduciendo los peligros de exposición de la información que circula en la red. Además, la red es más segura gracias a la seguridad de los puertos a nivel de acceso y a las políticas a nivel de distribución.

- **ACTIVE DIRECTORY EN WINDOWS SERVER**

Los usuarios deben conectarse e introducir una contraseña para identificarse en el sistema; esta combinación se utiliza para determinar las aplicaciones y la información a la que tiene acceso cada usuario, delimitando funcionalidades.

- **SEGURIDAD PARA LOS SERVIDORES**

La realización de configuraciones de la seguridad del servidor, para proporcionarle más control sobre el uso de los servicios y los recursos que tiene a su disposición.

Se protegen los valores de la red definiendo reglas de directiva de servidor de seguridad. Se permite o deniega el acceso a las redes conectadas con reglas de acceso. El servidor deberá estar configurado de forma predeterminada con un conjunto de reglas de directiva del sistema para el equipo servidor.

De manera predeterminada, todos los usuarios deberán tener acceso solo a una lista de dominios permitidos que puede ser modificada para agregar o eliminar según necesidades de acceso. Reglas de acceso especial a Internet, permitiéndose a los usuarios que integran la lista, acceso a todos los servicios de Internet.

3.2.1.3. Funcionalidad.

La red ofrecerá conectividad las 24 horas del día a todos los usuarios, con una alta velocidad, reduciendo los broadcasts y los dominios de colisión, es por ello que se propone agrupar los beneficiarios por medio de VLANs.

En el modelado expuesto se ejecutó el establecimiento de 8 VLANs distribuido en las diferentes áreas que tiene el colegio. Ver tabla 6.

Tabla 6.

Direccionamiento IP – VLAN de Administración de Switches.

VLAN ID	NOMBRE VLAN
VLAN 10	SWITCHES
VLAN 20	SERVIDORES
VLAN 30	LABORATORIO INICIAL
VLAN 40	LABORATORIO NIVEL SECUNDARIA
VLAN 50	AULAS – TALLERES
VLAN 60	ADMINISTRATIVOS
VLAN 70	ACCESS POINT

Fuentes: Elaboración Propia

Para asegura la comunicación se planteó el enrutamiento utilizando la tecnología OSPF que permite realizar las conexiones entre las partes de la red. Consideramos utilizar este tipo de enrutamiento ya que

brinda una rápida convergencia y escalabilidad en redes un poco extensas. Además, siendo un estándar libre tolera equipos de diversos y la mayoría de los creadores donde para cada uno de los routers disponen de una vista completa que está en sincronía con la red.

3.2.1.4. Escalabilidad.

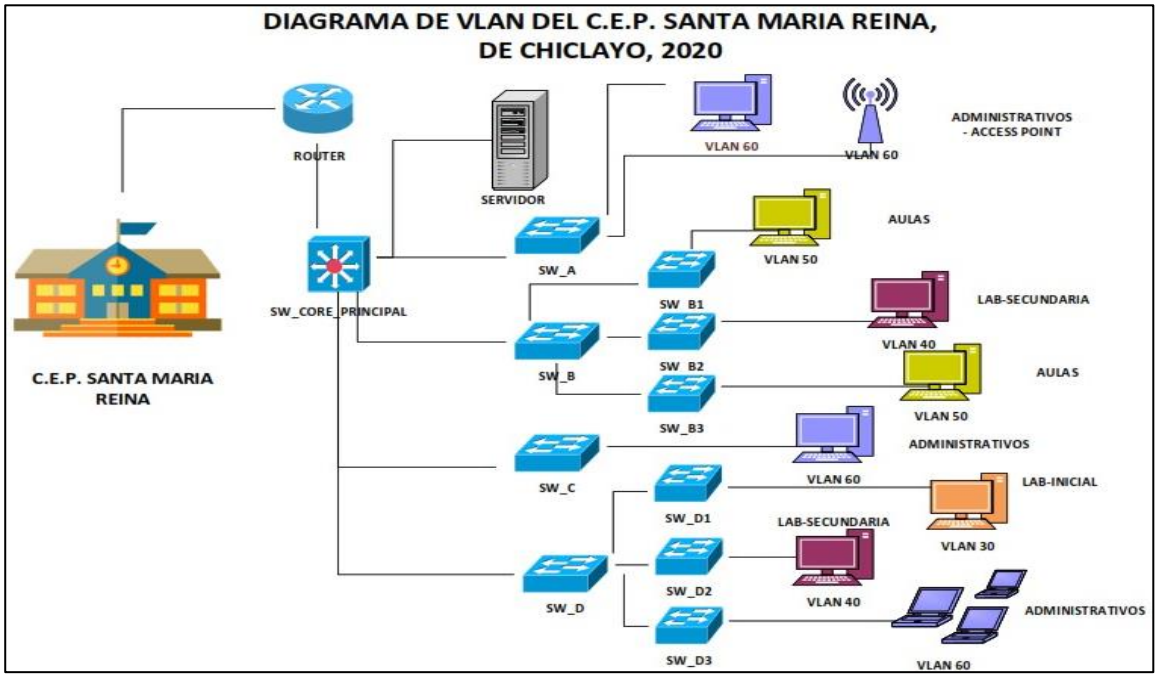
La red del Colegio Santa María Reina podrá aumentar de tamaño, ya que el diseño propuesto brinda una cantidad aceptable de VLANs. Los dispositivos de distribución siguen manteniendo su propiedad de escalabilidad, lo que quiere decir que permite el incremento del número de puertos que soporten el crecimiento exponencial.

3.2.1.5. Adaptabilidad.

La red propuesta está diseñada teniendo en cuenta los futuros avances tecnológicos que se puedan dar en la institución educativa, es por ello que decidimos implementar en nuestra la red la tecnología OSPF puesto que es un protocolo que reacciona rápido antes los cambios topológicos y es administrado fácilmente. A continuación, se detalla un diagrama de VLAN's propuesto.

Figura 21

Diagrama de VLAN.



3.2.2. Parte 6: Diseño de un modelo de direccionamiento

3.2.2.1. Distribución de direcciones IP de la red.

Para la asignación IP a los equipos y dispositivos que tiene la Institución Educativa Santa María Reina usaremos la clase "B", cuyas direcciones serán como se muestra en la tabla.

Así mismos la división de cada subred se ha realizado según la distribución del colegio áreas y nivel de educación que ofrece este centro educativo. Ver Tabla 7.

Tabla 7.

Direccionamiento IP – VLAN de Administración de Switches

	DIRECCIONAMIENTO IP			
VLAN - ID	**RED**	**RANGO DE HOST**	**BROADCAST**	**MÁSCARA**
SWITCHES 10	172.17.128.0/25	172.17.128.1 -- 172.17.128.126	172.17.128.127	255.255.255. 128/25
SERVIDORES 20	172.17.128.128/25	172.17.128.129 -- 172.17.128.254	172.17.128.255	255.255.255. 128/25
LAB-INICIAL 30	172.17.129.0/25	172.17.129.1 -- 172.17.129.126	172.17.129.127	255.255.255. 128/25
LAB-SECUNDARIA 40	172.17.129.128/25	172.17.129.129 -- 172.17.129.254	172.17.129.255	255.255.255. 128/25
AULAS-TALLERES 50	172.17.130.0/25	172.17.130.1 -- 172.17.130.126	172.17.130.127	255.255.255. 128/25
ADMINISTRATIVOS 60	172.17.130.128/25	172.17.130.129 -- 172.17.130.254	172.17.130.255	255.255.255. 128/25
ACCESS-POINT 70	172.17.131.0/25	172.17.131.1 -- 172.17.131.126	172.17.131.127	255.255.255. 128/25

Fuentes: Elaboración Propia

3.2.2.1.1. Switch A.

Tabla 8.

Características del switch "SW_A" cliente.

SWITCH	N° HOST	UBICACIÓN
SW_A	17 HOST	1ER PISO - BIBLIOTECA PAB-C

Fuentes: Elaboración Propia

Tabla 9.

Distribución de VLAN y Host del switch A

EQUIPO	SWITCH	VLAN	IP
PC_Biblioteca01	SW_A	VLAN 50	DHCP
PC_Biblioteca02	SW_A	VLAN 50	DHCP
PC_Biblioteca03	SW_A	VLAN 50	DHCP
PC_Biblioteca04	SW_A	VLAN 50	DHCP
PC_Biblioteca05	SW_A	VLAN 50	DHCP
PC5toA-S	SW_A	VLAN 50	DHCP
PC5toB-S	SW_A	VLAN 50	DHCP
PC5toC-S	SW_A	VLAN 50	DHCP
AP_Biblioteca	SW_A	VLAN 70	DHCP
PC4toA-S	SW_A	VLAN 50	DHCP
PC4toB-S	SW_A	VLAN 50	DHCP
PC4toC-S	SW_A	VLAN 50	DHCP
PC4toD-S	SW_A	VLAN 50	DHCP
PC_Taller_Robotica	SW_A	VLAN 50	DHCP
AP_Talleres	SW_A	VLAN 70	DHCP
PC_Taller_Ballet	SW_A	VLAN 50	DHCP
PC5toD-S	SW_A	VLAN 50	DHCP

Fuentes: Elaboración Propia

3.2.2.1.2. Switch B.

Tabla 10.

Características del switch “SW_B” cliente y distribución.

SWITCH	Nª HOST	UBICACIÓN
SW_B	11 HOST	1ER PISO - DATA CENTER -PAB-A
SW_B_1	9 HOST	2DO PISO PAB-A
SW_B_2	48HOST	LABORATORIO SECUN. 2DO PISO PAB-A
SW_B_3	5HOST	LABORATORIO SECUN. 2DO PISO PAB-A

Fuentes: Elaboración Propia

Tabla 11.

Distribución de VLAN y Host del switch B.

EQUIPO	SWITCH	VLAN	IP
PC4toA-P	SW_B	VLAN 50	DHCP
PC4toB-P	SW_B	VLAN 50	DHCP
PC4toC-P	SW_B	VLAN 50	DHCP
PC4toD-P	SW_B	VLAN 50	DHCP
PC3roA-P	SW_B	VLAN 50	DHCP
PC3roB-P	SW_B	VLAN 50	DHCP
PC3roC-P	SW_B	VLAN 50	DHCP
PC3roD-P	SW_B	VLAN 50	DHCP
PC_Lab_Biologia	SW_B	VLAN 50	DHCP
PC_Enfermeria01	SW_B	VLAN 60	ESTATICA
AP_Primaria	SW_B	VLAN 70	DHCP
AP_Coliseo	SW_B	VLAN 70	DHCP
PC3roA-S	SW_B_1	VLAN 50	DHCP
PC3roB-S	SW_B_1	VLAN 50	DHCP
PC3roC-S	SW_B_1	VLAN 50	DHCP
PC3roD-S	SW_B_1	VLAN 50	DHCP
PC2doA-S	SW_B_1	VLAN 50	DHCP
PC2doB-S	SW_B_1	VLAN 50	DHCP
PC2doC-S	SW_B_1	VLAN 50	DHCP
PC2doD-S	SW_B_1	VLAN 50	DHCP
AP_Primaria02	SW_B_1	VLAN 70	DHCP
PCLab01_S	SW_B_2	VLAN 40	DHCP
PCLab02_S	SW_B_2	VLAN 40	DHCP
PCLab03_S	SW_B_2	VLAN 40	DHCP
PCLab04_S	SW_B_2	VLAN 40	DHCP
PCLab05_S	SW_B_2	VLAN 40	DHCP
PCLab06_S	SW_B_2	VLAN 40	DHCP
PCLab07_S	SW_B_2	VLAN 40	DHCP
PCLab08_S	SW_B_2	VLAN 40	DHCP
PCLab09_S	SW_B_2	VLAN 40	DHCP

PCLab10_S	SW_B_2	VLAN 40	DHCP
PCLab11_S	SW_B_2	VLAN 40	DHCP
PCLab12_S	SW_B_2	VLAN 40	DHCP
PCLab13_S	SW_B_2	VLAN 40	DHCP
PCLab14_S	SW_B_2	VLAN 40	DHCP
PCLab15_S	SW_B_2	VLAN 40	DHCP
PCLab16_S	SW_B_2	VLAN 40	DHCP
PCLab17_S	SW_B_2	VLAN 40	DHCP
PCLab18_S	SW_B_2	VLAN 40	DHCP
PCLab19_S	SW_B_2	VLAN 40	DHCP
PCLab20_S	SW_B_2	VLAN 40	DHCP
PCLab21_S	SW_B_2	VLAN 40	DHCP
PCLab22_S	SW_B_2	VLAN 40	DHCP
PCLab23_S	SW_B_2	VLAN 40	DHCP
PCLab24_S	SW_B_2	VLAN 40	DHCP
PCLab25_S	SW_B_2	VLAN 40	DHCP
PCLab26_S	SW_B_2	VLAN 40	DHCP
PCLab27_S	SW_B_2	VLAN 40	DHCP
PCLab28_S	SW_B_2	VLAN 40	DHCP
PCLab29_S	SW_B_2	VLAN 40	DHCP
PCLab30_S	SW_B_2	VLAN 40	DHCP
PCLab31_S	SW_B_2	VLAN 40	DHCP
PCLab32_S	SW_B_2	VLAN 40	DHCP
PCLab33_S	SW_B_2	VLAN 40	DHCP
PCLab34_S	SW_B_2	VLAN 40	DHCP
PCLab35_S	SW_B_2	VLAN 40	DHCP
PCLab36_S	SW_B_2	VLAN 40	DHCP
PCLab37_S	SW_B_2	VLAN 40	DHCP
PCLab38_S	SW_B_2	VLAN 40	DHCP
PCLab39_S	SW_B_2	VLAN 40	DHCP
PCLab40_S	SW_B_2	VLAN 40	DHCP
PCLab41_S	SW_B_2	VLAN 40	DHCP
PCLab42_S	SW_B_2	VLAN 40	DHCP
PCLab43_S	SW_B_2	VLAN 40	DHCP

PCLab44_S	SW_B_2	VLAN 40	DHCP
PCLab45_S	SW_B_2	VLAN 40	DHCP
PCLab46_S	SW_B_2	VLAN 40	DHCP
PCLab47_S	SW_B_2	VLAN 40	DHCP
PCLab48_S	SW_B_2	VLAN 40	DHCP
PCLab49_S	SW_B_3	VLAN 40	DHCP
PCLab50_S	SW_B_3	VLAN 40	DHCP
PC5toD-P	SW_B_3	VLAN 50	DHCP
PC5toC-P	SW_B_3	VLAN 50	DHCP
AP_Laboratorio	SW_B_3	VLAN 70	

Fuentes: Elaboración Propia

3.2.2.1.3. Switch C.

Tabla 12.

Características del switch "SW_C" cliente.

SWITCH	**Nª HOST**	**UBICACIÓN**
SW_C	22 HOST	ATENCION PADRES DE FAMILIA - 1ER PISO PAB- A

Fuentes: Elaboración Propia

Tabla 13.

Distribución de VLAN y Host del switch C.

EQUIPO	**SWITCH**	**VLAN**	**IP**
PC_Admin01	SW_C	VLAN 60	172.17.130.132
PC_Admin02	SW_C	VLAN 60	172.17.130.133
PC_Admin03	SW_C	VLAN 60	172.17.130.134
PC_Admin04	SW_C	VLAN 60	172.17.130.135
PC_Admin05	SW_C	VLAN 60	172.17.130.136
PC_Admin06	SW_C	VLAN 60	172.17.130.137
PC_Admin07	SW_C	VLAN 60	172.17.130.138
PC_Admin08	SW_C	VLAN 60	172.17.130.139
PC_Admin09	SW_C	VLAN 60	172.17.130.140
PC_Admin10	SW_C	VLAN 60	172.17.130.141
PC_Admin11	SW_C	VLAN 60	172.17.130.142

PC_Admin12	SW_C	VLAN 60	172.17.130.143
PC_Admin13	SW_C	VLAN 60	172.17.130.144
PC_Admin14	SW_C	VLAN 60	172.17.130.145
PC_Admin15	SW_C	VLAN 60	172.17.130.146
PC_Admin16	SW_C	VLAN 60	172.17.130.147
PC_Admin17	SW_C	VLAN 60	172.17.130.148
PC_Admin18	SW_C	VLAN 60	172.17.130.149
AP_Administrativos	SW_C	VLAN 70	DHCP
PC_Auditorio01	SW_C	VLAN 50	DHCP
PC_Auditorio02	SW_C	VLAN 50	DHCP
AP_Auditorio	SW_C	VLAN 70	DHCP

Fuentes: Elaboración Propia

3.2.2.1.4. Switch D.

Tabla 14.

Características del switch “SW_D” cliente.

SWITCH	Nª HOST	UBICACIÓN
SW_D	10	2DO C - 1ER PISO PAB-A
SW_D1	24	AULA INICIAL- 5_A PAB -B
SW_D2	18	5TO B - 2DO PISO PAB -A

Fuentes: Elaboración Propia

Tabla 15.

Distribución de VLAN y Host del switch D.

EQUIPO	SWITCH	VLAN	IP
PC_Enfermeria02	**SW_D**	VLAN 60	172.17.130.150
PC1roA-P	**SW_D**	VLAN 50	DHCP
PC1roB-P	**SW_D**	VLAN 50	DHCP
PC1roC-P	**SW_D**	VLAN 50	DHCP
PC1roD-P	**SW_D**	VLAN 50	DHCP
PC_Ajedrez	**SW_D**	VLAN 50	DHCP
PC2doA-P	**SW_D**	VLAN 50	DHCP
PC2doB-P	**SW_D**	VLAN 50	DHCP

PC2doD-P	**SW_D**	VLAN 50	DHCP
PC6toD-P	**SW_D**	VLAN 50	DHCP
AP_Primaria03	**SW_D**	VLAN 70	DHCP
PC-Lab01	**SW_D1**	VLAN 30	DHCP
PC-Lab02	**SW_D1**	VLAN 30	DHCP
PC-Lab03	**SW_D1**	VLAN 30	DHCP
PC-Lab04	**SW_D1**	VLAN 30	DHCP
PC-Lab05	**SW_D1**	VLAN 30	DHCP
PC-Lab06	**SW_D1**	VLAN 30	DHCP
PC-Lab07	**SW_D1**	VLAN 30	DHCP
PC-Lab08	**SW_D1**	VLAN 30	DHCP
PC-Lab09	**SW_D1**	VLAN 30	DHCP
PC-Lab10	**SW_D1**	VLAN 30	DHCP
PC-Lab11	**SW_D1**	VLAN 30	DHCP
PC-Lab12	**SW_D1**	VLAN 30	DHCP
PC-Lab13	**SW_D1**	VLAN 30	DHCP
PC-Lab14	**SW_D1**	VLAN 30	DHCP
PC-Lab15	**SW_D1**	VLAN 30	DHCP
PC_Inicial_2_A	**SW_D1**	VLAN 50	DHCP
PC_Inicial_3_A	**SW_D1**	VLAN 50	DHCP
PC_Inicial_3_B	**SW_D1**	VLAN 50	DHCP
PC_Inicial_4_A	**SW_D1**	VLAN 50	DHCP
PC_Inicial_4_B	**SW_D1**	VLAN 50	DHCP
PC_Inicial_5_A	**SW_D1**	VLAN 50	DHCP
PC_Inicial_5_B	**SW_D1**	VLAN 50	DHCP
AP_Comedor	**SW_D1**	VLAN 70	DHCP
AP_Gym	**SW_D1**	VLAN 70	DHCP
AP_Piscina	**SW_D1**	VLAN 70	DHCP
PC5toA-P	**SW_D2**	VLAN 50	DHCP
PC5toB-P	**SW_D2**	VLAN 50	DHCP
PC6toA-P	**SW_D2**	VLAN 50	DHCP
PC6toB-P	**SW_D2**	VLAN 50	DHCP
PC6toC-P	**SW_D2**	VLAN 50	DHCP
PC6toD-P	**SW_D2**	VLAN 50	DHCP

PC1erA-S	**SW_D2**	VLAN 50	DHCP
PC1erB-S	**SW_D2**	VLAN 50	DHCP
PC1erC-S	**SW_D2**	VLAN 50	DHCP
PC1erD-S	**SW_D2**	VLAN 50	DHCP
LAB_INGLES	**SW_D2**	VLAN 50	DHCP
PC_Biblioteca01_P	**SW_D2**	VLAN 50	DHCP
PC_Biblioteca02_P	**SW_D2**	VLAN 50	DHCP
PC_Biblioteca03_P	**SW_D2**	VLAN 50	DHCP
PC_Biblioteca04_P	**SW_D2**	VLAN 50	DHCP
PC_Biblioteca05_P	**SW_D2**	VLAN 50	DHCP
PC_Salon_Musica	**SW_D2**	VLAN 50	DHCP
AP_Biblioteca03	**SW_D2**	VLAN 70	DHCP

Fuentes: Elaboración Propia

3.2.3. Parte 7: Selección de protocolos de switching y routing

La decisión tomada con respecto a los protocolos a usar es de acuerdo a la recolección de datos que se ha tomado de los clientes y de los objetivos que se tiene de la organización.

3.2.3.1. Selección de métodos de routing.

El método de enrutamiento que se usará será el protocolo OSPF, ya que nos permitirá lo siguiente: Como es un protocolo de redes de fuente abierta, puede utilizarse por ordenadores que no están asociados con la marca Cisco. OSPF es un estándar abierto ampliamente aceptado que permite la integración de manera rápida, cambia el protocolo de certificados para lograr el cumplimento de los objetivos referidos a la seguridad y pueda diseñarse en áreas jerárquicas, reduciendo los requisitos de memoria y CPU en los routers, no usa mucho ancho de banda y brinda un concepto lógico de redes en la que los routers tienen la capacidad de fraccionarse en partes.

Lo que reduce el flujo ejecución de actualización de estado de las conexiones a lo largo de la red. Además, que brinda un mecanismo para añadir rutas y disminuir la dispersión que no es necesaria de los datos de la red. A continuación, en la Tabla 16 y 17 se detalla una comparación del protocolo OSPF con otros tipos de protocolos de enrutamiento.

OSPF vs RIP

Tabla 16.

Tabla de comparación entre protocolo OSPF Y RIP.

OSPF	RIP
• Apropiado para redes grandes y escalables. • Usa el algoritmo de la situación del enlace. • Es considerada como mejor ruta de acceso la que cuenta con un nivel mayor de velocidad. • Ofrece un sistema libre de bucles de enrutamiento. • Permite trabajar con VLSM.	• Para redes pequeñas. • Usa el algoritmo de vector de extensión. • Es considerada como mejor ruta de acceso la que llega a su destino con una cantidad menor de saltos. • Puede utilizar algunas soluciones para evitar bucles de enrutamiento. • No puede usar VLSM, aunque en versión 2 si es posible.

Fuentes: Elaboración Propia

OSPF vs EIGRP

Tabla 17.

Tabla de comparación entre protocolo OSPF Y EIGRP.

OSPF	EIGRP
• Estándar abierto. • Como no resume por defecto, la tabla de enrutamiento puede crecer rápidamente en tamaño. • Utiliza el concepto de áreas para dividir la red en dominios jerárquicos e individuales.	• Propiedades de Cisco Systems. • Es mucho más fácil de configurar. • Realizan actualización de las tablas de enrutamiento solo cuando se produce un cambio en la red.

Fuentes: Elaboración Propia

En esta ocasión se presenta la configuración del protocolo de enrutamiento dentro del Switch_Core_Principal, el cual nos permite realizar las conexiones con la red completa. Ver Figura 22.

Figura 22

Configuración de Protocolo de enrutamiento

```
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 10.10.0.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.15 area 0
 network 192.168.1.16 0.0.0.15 area 0
 network 192.168.1.32 0.0.0.15 area 0
 network 192.168.1.64 0.0.0.63 area 0
 network 192.168.1.128 0.0.0.63 area 0
 network 192.168.1.192 0.0.0.63 area 0
!
```

3.2.3.2. Selección de métodos de switching.

Elegir un buen método de switching nos permitirá una mejor comunicación libre de colisiones (broadcast), múltiples conversaciones a la vez, ancho de banda dedicado a cada puerto del switch, se tendrá facilidad de mantenimiento y la administración será simple y básica, se realizará la reutilización del cableado dentro de la infraestructura de la red. Por lo tanto, el método que usaremos será el de SRS (Source-Router Switching), el cual se basará en el Source Route Transparent Bringing.

3.2.4. Parte 8: Desarrollo de estrategias de seguridad de la red

Para el desarrollo de estrategias de seguridad de la red, debemos aplicar las mejores prácticas:

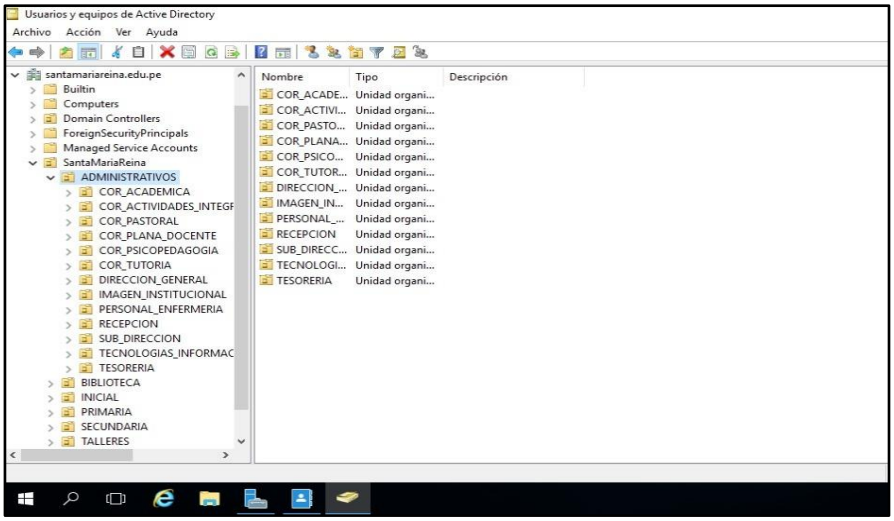
- **ACCESO CONTEXTUAL**

Obtenga los controles necesarios para garantizar los niveles adecuados de los accesos para cada persona dentro y fuera de su organización, en función de sus perfiles de usuario, terminal, red y seguridad.

En esta ocasión, dentro del Colegio Santa María Reina, de Chiclayo, se implementará un servidor de Active Directory, el cual será el encargado de brindar los servicios de autenticación, confiabilidad y que se encuentren siempre disponibles los bienes a los usuarios de la red dentro de la institución. Ver Figura 23.

Figura 23

Estándar Configuración de Active Directory.



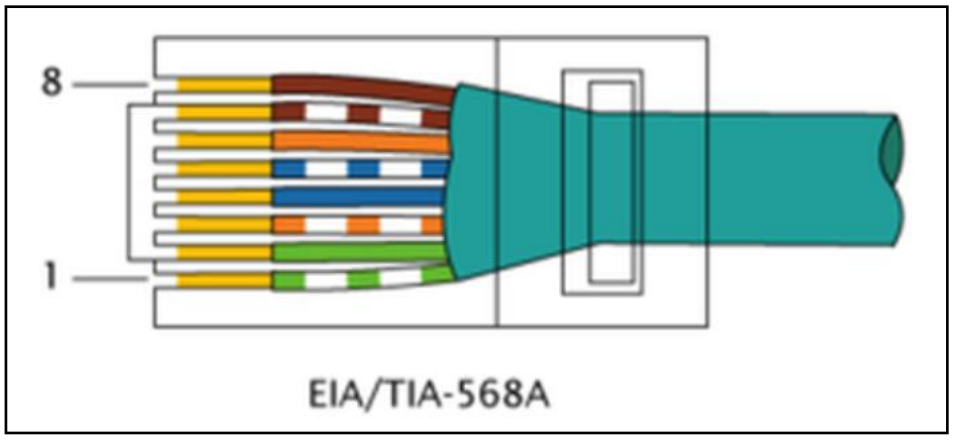
- **SEGURIDAD DE RED**

Proporcione aplicaciones con técnicas de cifrado, como un puesto de trabajo a los colaboradores y a terceros, así como control de acceso a la red y redes microsegmentadas para el cumplimiento de la normativa y la seguridad, todo ello manteniendo el máximo grado de tiempo de actividad y rendimiento del servicio.

Dentro del colegio se están aplicando el estándar de seguridad de la red que es el estándar 802.1Q y la norma ANSI/TIA/EIA-568-A para proteger la seguridad de la red en todas las áreas del Colegio Santa María Reina, de Chiclayo. Ver Figura 24.

Figura 24

Norma ANSI/TIA/EIA-568-A



Nota. Cable directo 568A. Reproducida de Conectar cable de red con cable UTP, conectores RJ45 con el estándar TIA/EIA 568-A, de Proyecto Electrónico.com, 2018, Proyecto Electronico.com (https://www.proyectoelectronico.com/computadora/conectar-cable-red-utp.html). CC BY 2.0

- **SEGURIDAD DE APLICACIONES**

La gestión centralizada de los programas, las actualizaciones de SO y configuración del sistema, garantizan un acceso seguro a los recursos de la organización, incluso desde los dispositivos propiedad de los empleados, al tiempo que reducen las amenazas avanzadas y los ataques de denegación de servicio.

Dentro del colegio se va a crear perfiles o imágenes donde estarán las aplicaciones a usar dentro de la institución, además de realizar auditorías para proteger esta parte de la red.

También se ha creado un servidor de BD dentro de la entidad, el cual nos va a servir para que los clientes remotos o locales soliciten información y poder verificar si se encuentra en la BD de la aplicación, ya sea desde la web o del mismo aplicativo.

- **SEGURIDAD DE LOS DATOS**

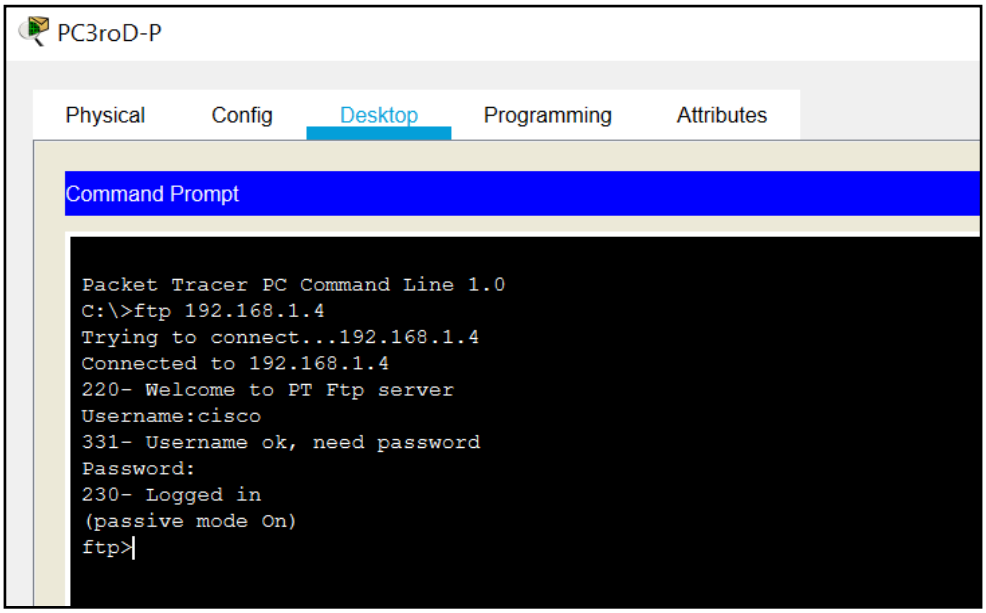
En la seguridad de datos enfocaremos los elementos comunes que toda organización debe tener en cuenta a la hora de aplicar medidas de seguridad: las personas, los procesos y las herramientas tecnológicas es por ello que dentro del colegio, se bloquearán los puertos USB para así evitar robo de datos,

traspaso de datos de un lugar a otro, además de eso se ha creado un servidor FTP, el cual ayudará a todo el personal del Colegio Santa María Reina, de Chiclayo a usar sus archivos, trabajos, dentro de la red.

En la siguiente imagen se muestra el uso del FTP a nivel de Packet Tracer, pero en la realidad, este servicio se implementará dentro del servidor de Windows Server. A continuación, se detalla configuración del FTP, ver Figura 25.

Figura 25

Acceso a FTP.



3.2.4.1. Diseño de la seguridad de la red.

3.2.4.1.1. Análisis de riesgos de seguridad.

- **Amenazas**

Eventos que pueden causar alteraciones a la información de la institución, por lo cual ocasiona pérdidas económicas, de alumnos y sobre todo de imagen. Estas amenazas son difíciles de controlar, por lo cual podemos indicar lo siguiente:

- **Software**

Aquel software bajado de internet o de manera incorrecta puede ser una amenaza lógica, lo cual puede ocasionar daños, ya que al instalar puede dejar abierto algún puerto en el cual un hacker puede entrar y explotar la red ocasionando lentitud e incluso robo de información, aparte de eso el no realizar backups periódicamente.

- **Hardware**

Los fallos físicos pueden producirse como consecuencia de algún desperfecto durante su fabricación o un modelado de hardware malo, sin embargo se puede producir como consecuencia del uso inadecuado, la falta de mantenimiento o el fin de la vida útil del producto, puede producirse de forma regular durante las temporadas de invierno como resultado por la degradación causada debido a una utilización prolongada, y por la climatización del lugar si no es conducente porque produce un ambiente de humedad ; A poco tiempo de la instalación, los dispositivos empiezan a corroerse. En la institución, no hay inventario.

- **Red**

La falta de tener la red disponible, así como la extracción lógica de datos por medio de ella, suponen una amenaza. Los cableados de la red son visibles porque están expuestos.

- **Humanas**

La amenaza más latente en la red es el personal que trabaja en nuestra institución; se utilizan varios bienes para controlar y prevenir sus consecuencias; ya se pueden identificar los atacantes pasivos entre el personal de la institución, por lo cual este personal debe ser de confianza, que maneja de manera cuidado la información del alumnado y de los trabajadores internos de la institución.

- **Desastres Naturales**

Las amenazas naturales hacen alusión a incendios, terremotos; que afectan aun vulnerabilidad como contar con de cables de electricidad sin protección; es conveniente tomar un punto necesario para instalar de los dispositivos de la red, un centro de servicio, un centro de ordenadores, equipos electrónicos y otros, teniendo en cuenta las diversas de catástrofes de la naturaleza que ponen en peligro las vulnerabilidades de un sistema de red de información.

3.2.4.1.2. Vulnerabilidades.

Elemento que puede ser aprovechado por algún hacker que trate de entrar y violar la seguridad de la red, por lo cual generaría daños, también considerados elementos internos que hay que tener en cuenta, ya que estamos expuestos a muchas vulnerabilidades dentro de nuestra red:

- **Software**

Cualquier programa, ya sea bajado de internet, comprado en un centro comercial, puede ser usado como medio para entrar a la red y atacar y ocasionar daños, en la institución no se encuentra restringido la instalación de programas.

- **Hardware**

Las vulnerabilidades a nivel de hardware aparecen en que los componentes físicos fallen (desgaste, un mal modelado, mal uso), lo que genera que una red se encuentre son protección ante posibles ataques o amenazas.

- **Física**

Mayormente sucede en las malas prácticas del ingreso de la persona, por ejemplo: el uso de dispositivos externos para la extracción de datos de una manera no autorizada.

- **Natural**

Las amenazas naturales incluyen una amplia gama de catástrofes causadas por las fuerzas naturales. No ser consciente de que hay un incendio. No saber cómo utilizar un extintor de incendios correctamente.

3.2.4.2. Mecanismo de seguridad.

3.2.4.2.1. Seguridad Física.

- Dado que el hardware es el recurso más caro, es fundamental no colocarlo en sitios elevados o peligrosos para prevenir caídas.
- Se corre el riesgo de dañar el equipo y hacer que deje de funcionar si se ponen objetivos móviles sobre él.
- Para los elementos cruciales, se utilizan fijadores (gabinetes para switch).
- Para evitar que los objetos lanzados de otro punto caigan, evite colocar los equipos cerca de las ventanas.

3.2.4.2.2. Seguridad Perimetral.

- Instalar detectores de movimientos.
- El acceso a los servidores estará limitado y se mantendrá en una zona segura.
- Instalar circuitos cerrado de cámaras.
- Instalación de vallas eléctricas si la infraestructura lo requiere

3.2.4.2.3. Seguridad de Equipos.

- Hacer una lista de todos los ordenadores vinculados a nuestra red.
- Los usuarios deben notificar inmediatamente al director de Administración de la Red si experimentan cualquier dificultad con los ordenadores.

3.2.4.2.4. Mantenimiento de Equipos.

- El personal autorizado se encargará del mantenimiento del equipo.
- Todas las formas de averías y el mantenimiento preventivo deben documentarse.
- El plan de mantenimiento de los equipos debe ser ratificados y los horarios deben ser respetados.
- Incluya un manual de procedimientos en caso de que se produzcan fallos comunes y típicos.

3.2.4.3. Desarrollo de un plan de seguridad – LAN.

3.2.4.3.1. Router – Firewall.

Tabla 18.

Cuadro comparativo de tipos de firewall

SOFTWARE	HARDWARE
• Programa Software • Utilizado en Ordenadores o PC • Es mucho más barato o incluso gratuito. • Su objetivo es evitar que se produzcan conexiones potencialmente perjudiciales. • Va a recibir más actualizaciones y por tanto ante amenazas más actuales puede hacer frente. • Segyte Personal, Keiro, TnyWall, ZoneAlarm, Solarwinds NPM.	• Dispositivo Físico. • Utilizado en las Redes WAN o MAN • Es una alternativa más cara. • Se sitúa entre la red y el cable de la conexión a internet. • Hay una variedad de alternativas disponibles que pueden ser instaladas en varios dispositivos y sistemas operativos. • Hace una protección de los puertos de la PC y archivos maliciosos. • Entre ellos están: Cisco System, Ubiquiti, Huawei, Sophos, Fortinet

Fuentes: Elaboración Propia

En este plan de desarrollo de Seguridad LAN, se está implementando como proteger a la red a través de un firewall dentro del Router, aplicando las Listas de Control de Acceso, el cual va a permitir o denegar algún acceso o requerimiento que se solicite a la red. Se muestra un cuadro comparativo del firewall.

- **SOFTWARE FIREWALL SOLARWINDS NPM**

Si el presupuesto del centro educativo no permite la compra de un firewall de software, se recomienda lo siguiente, SOLARWINDS NPM ya que este puede identificar, diagnosticar y solucionar rápidamente problemas y fallas de rendimiento de la red antes de recibir llamadas que le pregunten por qué la red no funciona. Además, NPM es la solución más fácil de su tipo de implementar, usar y mantener, lo que significa que puede utilizar el tiempo para administrar la red en lugar de brindar soporte.

Los profesionales de TI pueden utilizar este software para obtener métricas de rendimiento y alertas precisas para sus aplicaciones basadas en Windows y Linux que están instaladas en centros de datos distribuidos geográficamente, oficinas remotas o nubes públicas como Rackspace, Google cloud, plataform, Microsoft Azure, Amazon AWS.

Su costo por suscripción es de: S/. 9100.

Pros:

- Los cambios en el firewall le enviarán alertas o notificaciones.
- Se pueden utilizar métodos específicos para hacer un seguimiento de las actividades a dispositivos.
- Sólo los administradores de firewall aprobados podrán realizar modificaciones en las políticas del mismo.
- Se pueden crear filtros personalizados para destacar determinados eventos del firewall en función de parámetros personalizados o predefinidos.

Contras:

- No existe una versión gratuita de Security Events Manager.

En otro caso si el Centro Educativa no contara con el presupuesto correspondiente para adquirir un firewall de software licenciado se recomienda lo siguiente, TINYWALL es una extensión que amplifica las acciones del firewall del sistema operativo. Su misión es aumentar esta protección mediante el uso de opciones de configuración simples. Una vez instalado y activado, TinyWall habilita la función que bloquea la mayoría de las conexiones entrantes y salientes. Se elige entre dos opciones posibles: Permitir manualmente la lista de aplicaciones que deseas, o usar el modo de aprendizaje, que te permite deshabilitar inicialmente todas las conexiones y luego desactivar aquellas que no creas necesarias.

Cuenta con las siguientes características.

- Es un programa no intrusivo. Puede trabajar en su computadora sin ningún problema sabiendo que el dispositivo está completamente protegido.

- No absorbe muchos recursos, es fácil de usar. El impacto en la pérdida de rendimiento del sistema es insignificante.
- No hay controladores ni componentes instalados en el kernel del sistema, lo que contribuye a la estabilidad.
- Agrega nuevas funciones a Windows que lo hacen más seguro.
- Es muy fácil de usar, no requiere configuraciones complicadas.

Teniendo en cuenta sus pros y contras.

Pros:

- Ventanas emergentes no hay.
- La capacidad de autoaprendizaje facilita la creación de excepciones.

Contras:

- Para ataques de exploits no es protección.

3.2.4.3.2. Implementación de ACL.

Planteamos implementar ACL's extendidas pues permitirá no solo filtrar por dirección IP de origen, sino que también están disponibles filtros por dirección IP de destino, número de puerto y protocolo, asimismo ayudará al Switch de capa 3 a filtrar los tipos de paquetes de datos que deben aceptarse o rechazarse según las condiciones establecidas

3.2.4.3.3. Objetivos ACL's.

- Limitará el tráfico de la red puede, a su vez, aumentar la mejora del rendimiento en la red de la institución educativa.
- Proporcionará seguridad básica para el acceso a la red del colegio.
- Determinará el tipo de tráfico que se envía o bloquea en la interfaz del Switch de capa 3.
- A determinados tipos de archivos, como FTP o HTT permitirá o denegará a los usuarios el acceso

3.2.4.3.4. Políticas de acceso.

- Denegar que la red de aulas y laboratorios acceda a la red de administrativos.

- Denegar el tráfico de redes sociales en todas las redes comprendido entre las 8:00am hasta las 4:00pm.
- Denegar que la red de Access Point no pueda acceder a la red de servidores.
- Permitir que la red de administrativos pueda acceder al servidor FTP Y HTTP.
- Denegar el acceso de la red de aulas y laboratorios por TELNET.

3.2.4.4. Desarrollo de un plan de seguridad – WLAN.

El primer paso para asegurar una red WLAN es invertir esfuerzos en la correcta configuración WLAN y en su administración, esto permitirá a la institución educativa asegurar la red en un futuro. Detallaremos los pasos más importantes para una seguridad en la red WLAN. Ver Tabla 19.

Tabla 19.

Elaboración de un plan de Seguridad WLAN

PLAN DE SEGURIDAD WLAN		
RIESGO ESPECÍFICO	**Trabajo a Realizar**	**Plan de Acción**
Configuración incorrecta o débil de los Access Point que facilite a los intrusos a interceptar información sensible, que puede estar distorsionada o filtrada	Localización de puntos de acceso (AP) en lugares que cubran únicamente las áreas internas de la Institución Educativa.	Utiliza un firewall para separar completamente las partes inalámbrica y cableada de la red que establece las reglas necesarias para facilitar una unión segura.
	Sólo los administradores de red tienen privilegios para ejecutar permisos estrictos por ejemplo la opción "reset" de los equipos.	Definición de listas de control de acceso basadas en direcciones MAC para garantizar la seguridad de la red permitiendo que sólo se unan los dispositivos inalámbricos aprobados.
	Las opciones de seguridad se encuentren activas en los equipos WLAN	Los firewalls pueden colocarse en cualquier lugar para ayudar a protegerse de los asaltos a la red inalámbrica y proporcionar protección adicional a los puntos de acceso contra los intrusos.
Acceso no controlado o invadido por usuarios no autorizados en la red inalámbrica.	Las contraseñas iniciales suministradas a los usuarios nuevos sólo son válidas para una sesión antes de pedir al usuario que sustituya su contraseña. Válida para una sesión antes de pedir al usuario que la actualice.	El SSID debe configurarse para que no contenga información que identifique a la institución educativa, no debe contener productos, nombres o cualquier otra información que una persona no autorizada pueda usar para intentar acceder al servicio.
La aplicación de normas y reglas para el control y la gestión de la seguridad de la wlan para ayudar al mantenimiento de una red segura es difícil.	Se deberá tener en cuenta las políticas de seguridad establecidas.	Utilización de las actuales políticas de seguridad por cable para integrar las políticas inalámbricas.

Fuentes: Elaboración Propia

3.2.4.5. Desarrollo de políticas de seguridad.

Habrá una red de datos, y las políticas de seguridad son descripciones minuciosas de las normas que los usuarios deben seguir, en consecuencia, los empleados autorizados pueden utilizarlo; sin embargo, dado que el acceso a la red es un privilegio y no un derecho, los usuarios deben ser conscientes de lo siguiente:

- El usuario recibirá los permisos necesarios para acceder a los datos que necesita en la red.
- Para salvaguardar la información que circula por la red, se tomarán las medidas necesarias, asegurando del servicio la integridad y disponibilidad.
- El departamento de informática se encargará de la administración de la red, que será dirigido por un administrador de la red.
- Cualquier aumento del número de estaciones de trabajo que desean conectarse a la red debe ser informado al gestor de la red.
- El personal del área de ordenadores debe instalar y configurar cualquier estación de trabajo.
- No se permitirá conectar equipos de fuera de la institución a la red de datos.
- Si no se ha dado el permiso, el usuario no podrá acceder a los recursos de la red.
- El usuario no podrá instalar programas por su cuenta sin la autorización del administrador de la red.
- Es contra la ley enviar mensajes que revelen información personal o privada sobre otra persona.

3.2.4.5.1. Vulnerabilidades encontradas bajo la norma ISO 27001 de la red Colegio Santa María Reina.

1. **Colocación de cables.**

   Debido a que el cableado no está estructurado, es más difícil y costoso mantenerlo y solucionarlo.

2. **Inadecuado nivel de conocimiento y/o concienciación de empleados y mantenimiento inadecuado.**

La institución no cuenta con un personal adecuado para un buen mantenimiento de los equipos de red y sobre el uso de los equipos.

3. **Inadecuada gestión de redes.**

No se ve reflejado en la falta de supervisión y control de los elementos que forma la red de la Institución educativa y no garantiza el nivel de servicio de acuerdo a las necesidades.

4. **Inadecuada supervisión de proveedores externos.**

Los proveedores que ofrecen sus servicios tecnológicos no brindan soporte ni mantenimiento adecuado a los equipos de red.

5. **Redes accesibles a personas no autorizadas.**

La información reservada es brindada a un personal no autorizado sobre el manejo de la red.

6. **Inadecuada o falta de implementación de auditoría interna.**

No elaboran un plan anual de auditoría interna en base a riesgos. Ya que hacen siempre el mismo enfoque de trabajo y una lista de trabajo igual que los periodos pasados.

7. **Bases de datos con protección desactualizada contra códigos maliciosos.**

Cuentan con una base de datos sin mantenimiento, alojado en un servidor el cual le dan poco uso.

8. **Susceptibilidad del equipamiento a la humedad, la contaminación, a la temperatura y alteraciones en el voltaje.**

Los equipos no cuentan con un gabinete y un data center adecuado, por lo que están expuestos y desprotegidos.

9. **Acceso no autorizado a instalaciones.**

Como los se encuentran en una sala a la cual cualquier personal de la institución tiene acceso, no se lleva un control de que personal ha estado en dicha sala.

10. **Reglas organizacionales no definidas con claridad.**

La distribución, el control y la coordinación de las funciones, los mandos y los deberes, así como el modo en que se mueve la información entre los distintos niveles de gestión, no son estructuras organizativas bien definidas.

11. **Integridad de la Información manejada por el personal administrativo.**

Confidencialidad de la Información.

12. **No existe constate una vigilancia y registro de los posibles incidentes y de actividades sospechosas de forma que podamos prevenir los eventos no deseados.**

La seguridad de la información no está cubierta por ninguna ley, norma u obligación contractual.

13. **Descargas de Internet sin control.**

Como no tienen un filtro adecuado del uso de internet, las descargas y la navegación no son seguras y no llevan un control correcto del ancho de banda usado por cada equipo conectado a la red.

Uso no controlado de sistemas de información.

14. **Software no documentado.**

Tienen un sistema web el cual no se encuentra documentado y no cuenta con manuales o instrucciones, por lo que se ven obligado a llamar al creador del sistema constantemente.

15. **Empleados desmotivados o disconformes.**

Tanto el personal administrativo como académico se encontraba disconforme puesto que el colegio no cuenta con las herramientas tecnologías necesarias que permita usar la tecnología como un medio educativo para las estudiantes del centro educativo.

16. **Conexiones de red pública sin protección.**

Este problema es más evidente en los puntos de acceso Wi-Fi que son atractivos para los consumidores, lo que los hace deseables para quienes quieren unirse, especialmente porque no requieren autenticación para crear una conexión de red. Cualquiera que tenga acceso incontrolado a dispositivos no protegidos en la misma red tiene ahora una enorme oportunidad.

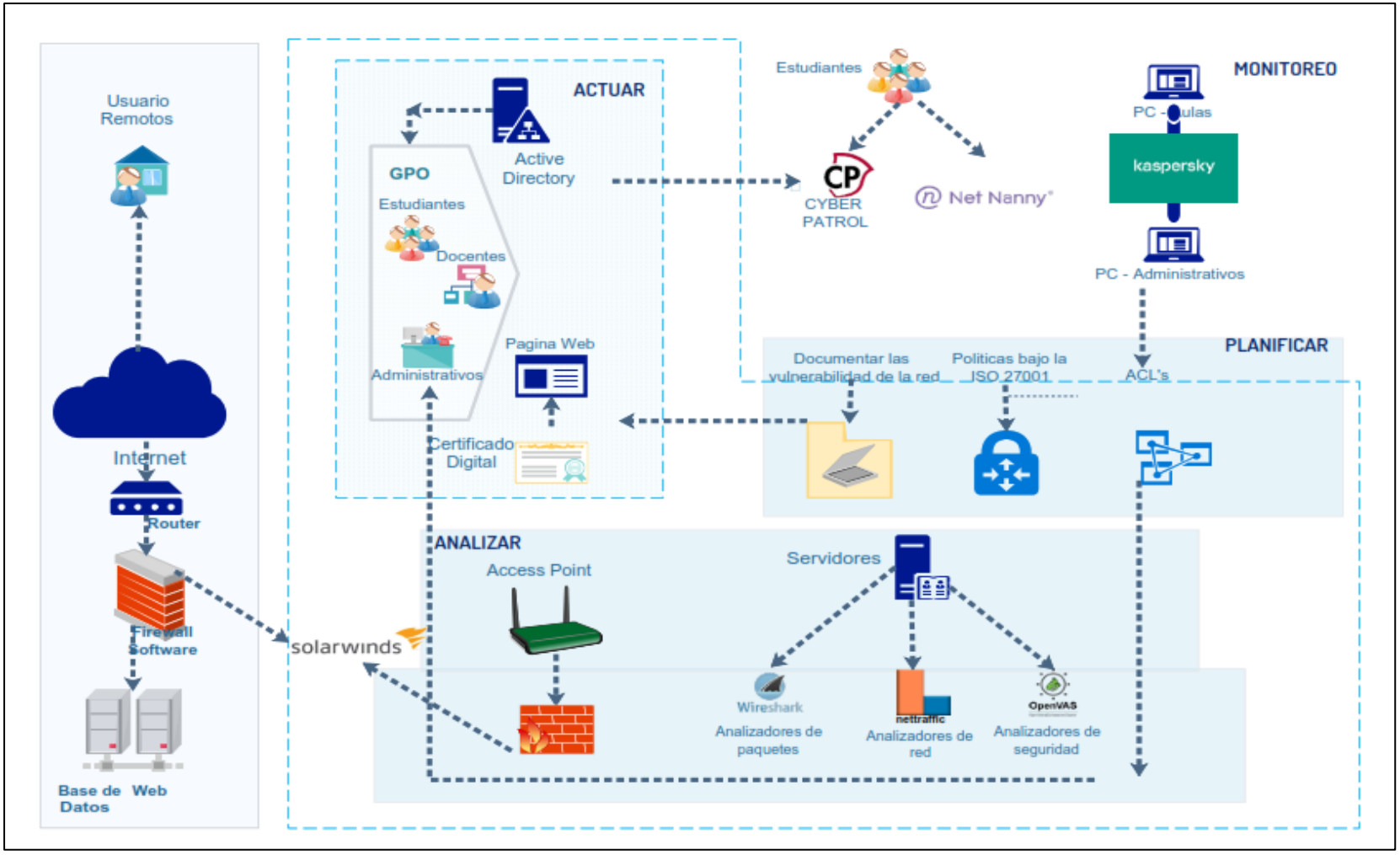
17. **Uso de equipamiento obsoleto.**

a. El colegio contaba con dos equipos obsoletos era un servidor de la marca Dell, y un switch de marca CISCO, estos equipos se encontraban prendidos, pero no se le daba ningún uso alguno, Lo que se puede deducir la falta de capacidad para poder implementar novedades tecnológicas.

b. Se usarán otros estándares también para la seguridad de la red, para el uso de las redes inalámbricas se usará el estándar 802.11, para el uso de las Redes privados virtuales se usará el estándar 802.1q, como así el estándar 802.1b para la administración de las redes locales.

Figura 26

Diseño de Arquitectura de Seguridad



3.2.5. Parte 9: Desarrollo de arquitectura de gestión de red

Una red en un centro de aprendizaje puede utilizarse para una variedad de fines. En consecuencia, lo primero que debemos hacer es definir los objetivos y funciones a los que se dedicará nuestra red. La importancia, o el ámbito, al que dedicaremos nuestra red se determinará por estos recursos, e influirá en otras decisiones; al fin y al cabo, es evidente que podemos subcontratar la tarea a una empresa si tenemos suficientes recursos financieros. Sin embargo, en su gran mayoría de los casos la Institución Educativa dispone de recursos muy escasos por ello se propone diferentes métodos para poder gestionar la red. Desde este punto de vista, la gestión de redes abarca una amplia gama de aplicaciones, que Stalling (2000) denomina áreas de gestión de redes o áreas funcionales.

Para cumplir estos objetivos, OSI establece una división por áreas funcionales, que se considera útil para cualquier sistema de gestión (con o sin OSI). La gestión de la configuración, la gestión del rendimiento, la gestión de los fallos, la gestión de la seguridad y la gestión de los costos son algunos de los ámbitos o áreas funcionales de la gestión de redes:

3.2.5.1. Gestión de fallos.

La gestión de errores se supervisa e identificar los fallos de la red lo antes posible y de evaluar sus causas para corregirlos para conservar la red en funcionamiento en alguna situación. Estas acciones se llevan a cabo mediante la evaluación de la red y del sistema (Activar, Desactivar: Activado, brevemente o desactivado), la recepción y el procesamiento de alarmas, el análisis continuo de los elementos de la red y las iniciativas de recuperación de errores. Para alcanzar estos objetivos, encontramos útil recomendar el software ZABBIX, que controla muchos parámetros de la red, así como la integridad y estado del servidor. Zabbix tiene un sistema de notificación flexible que permite a los usuarios crear notificaciones basadas en el correo electrónico para casi cualquier acontecimiento. Esto permite una respuesta rápida a los problemas del servidor. A partir de los datos registrados, Zabbix proporciona grandes herramientas de generación de informes y visualización de datos. En consiguiente, Zabbix es adecuado para planificar la eficacia de la red. Gestor Zabbix.

Por su actualización y rendimiento, la versión de Zabbix elegida para la gestión del laboratorio será la 3.4. Los requisitos de memoria y almacenamiento para la instalación de Zabbix varían en función del número de equipos y parámetros a monitorizar, así como su intervalo de recogida.

La siguiente tabla muestra las necesidades medias de varios entornos de supervisión, desde las infraestructuras más pequeñas hasta las más grandes y complejas.

Dado que el número de equipos que hay que vigilar es inferior a 1.000, se utilizan como ejemplo para este proyecto las indicaciones suministradas para un entorno largo.

3.2.5.2. Gestión de costes.

Tabla 20.

Elaboración de características de servidores.

TIPO	CARACTERISTICAS	OPERACIONES QUE REALIZARÁ	SISTEMA OPERATIVO SOPORTADOS	PRECIO
SERVIDOR	**MARCA:** Lenovo Thinksystem Sr530 **PROCESADOR:** Intel® Xeon® Bronze 3106 (11M Cache, 1.7 GHz) - 8 núcleos **RAM:** 8GB - PC-DDR4 2666MHz DIMM (12 Ranuras), ampliable hasta 768 GB **DISCO DURO:** Unidades no incluidas **VIRTUALIZACION:** Si **CONTROLADOR RED:** Gigabit Ethernet, 2 X Rj-45 Gbe **CONTROLADOR RAID:** RAID 530-8i, Tipo SAS 12GB/S, SATA 6GB/S **FUENTE:** 550 WATTS	En este Servidor se va a virtualizar: **SERVIDOR DNS:** Para que los ordenadores de los clientes utilizan nombres en lugar de direcciones IP numéricas. **SERVIDOR WEB:** Para poder alojar las páginas web, facilitar su mantenimiento y permitir su acceso por parte de los usuarios. **SERVIDOR DE BASE DE DATOS:** Para almacenar la base de datos del sistema de la Institución educativa y para futuros sistemas que quieran implementar	**LINUX:** Red Hat Enterprise Linux Server 6 y 7 SUSE Linux Enterprise Server 11 y 12 **WINDOWS:** Microsoft Windows Server 2012 R2, 2016	S/4,059.05

Fuente: Elaboración Propia

ROUTER GIGABIT INTEGRATED SERVICES ROUTER CISCO 2901 - CISCO2901/K9

Tabla 21.

Especificaciones de Cisco2901/K9

ESPICIFICACIONES DE CISCO2901/K9	
Imagen de Dispositivo	
TIPO DE DISPOSITIVO:	Cisco 2901 Integrated Services Router - encaminador
TIPO DE PRODUCTO ROUTER	Factor de forma Externo - modular - 1U
PESO	6,1 kg
DIMENSION	43.9 cm x 43.8 cm x 4.5 cm
DRAM MEMORIA	512 MB (instalados) / 2 GB (máx.)
MEMORIA FLASH	256 MB (instalados) / 8 GB (máx.)
PROTOCOLO DE DIRECCIONAMIENTO	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático, enrutamiento IPv6 estático
PROTOCOLO DE GESTIÓN REMOTA:	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH
PROTOCOLO DE INTERCONEXIÓN DE DATOS	Ethernet, Fast Ethernet, Gigabit Ethernet
PROTOCOLO DE GESTIÓN REMOTA	NMP, RMON
	Caracteristicas del Cisco IOS IP Base, soporte de MPLS, soporte para Syslog, soporte IPv6, Queue Server (CBWFQ), Detección ponderado Class-Based Fair Weighted Random Early (WRED)
CUMPLIMIENTO DE NORMAS	IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag
ALIMENTACIÓN	CA 120/230 V (50/60 Hz)
PRECIO	S/. 4055

Fuente: http://ds3comunicaciones.com/cisco/CISCO2901.html

Esta serie incluye servicios de aplicaciones, buzón de voz, procesamiento de llamadas, prevención de intrusiones, así como un cortafuegos, buzón de voz, procesamiento de llamadas, prevención de intrusiones, firewall, voz y vídeo con ranuras opcionales de capacidad de señalización digital (DSP) y aceleración de cifrado por hardware. Además, las plataformas permiten la más amplia variedad de opciones de conectividad por cable e inalámbrica disponibles en la industria, incluyendo fibra y cobre, fibra GE, xDSL y T1/E1.

SWITCH PRINCIPAL

SWITCH ADMINISTRABLE CAPA L3, 24 PUERTOS CISCO SF300-24P SRW224G4P-K9-NA

Tabla 22.

Especificaciones de Cisco SRW224G4P-K9-NA

ESPICIFICACIONES CISCO SRW224G4P-K9-NA	
IMAGEN DE DISPOSITIVO	
TIPO DE DISPOSITIVO:	Enrutador inalámbrico - módem (analógico) - conmutador de 8 puertos (integrado)
TIPO INCLUIDO	Sobremesa
TAMAÑO DE TABLA DE DIRECCIÓN MAC	8K DE ENTRADAS
PROTOCOLO DE INTERCONEXIÓN DE DATOS ETHERNET	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n (draft 2.0)
PUERTOS	24 X Ethernet 10base-T, Ethernet 100Base-TX
ALIMENTACIÓN	FUENTE DE ALIMENTACIÓN - INTERNA - CA 120/230 V (50/60 HZ)
RENDIMIENTO	Capacidad de conmutación: 12.8 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes): 9.52 Mbps
CAPACIDAD	Rutas estáticas: 32

PROTOCOLO DE GESTIÓN REMOTA	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, TELNET, SNMP 3, SNMP 2C, HTTP, HTTPS, SSH, CLI
VELOCIDAD DE TRANSFERENCIA DE DATOS	100 MBPS
CUMPLIMIENTO DE NORMAS	IEEE 802.1D, IEEE 802.1Q, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.1x, Wi-Fi CERTIFIED, IEEE 802.11n (draft 2.0)
PESO	3.1 KG
DIMENSIONES (ANCHO X PROFUNDIDAD X ALTURA)	44 cm x 25.7 cm x 4.5 cm
PRECIO	S/. 2980

- Las listas de control de acceso (ACL) y las LAN virtuales (VLAN) para usuarios temporales, así como otras sofisticadas funciones de seguridad para una gestión rigurosa de la red, son todas ellas características de seguridad sólidas.
- La compatibilidad con IPv6 permite emplear aplicaciones de red y sistemas operativos de última generación sin necesidad de sustituir el hardware.
- Estas redes pueden conectarse sin comprometer el rendimiento de las aplicaciones gracias al enrutamiento estático y al enrutamiento IP de capa 3 entre las VLAN.

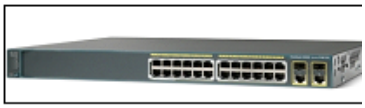
Fuente: http://ds3comunicaciones.com/cisco/Cisco-SRW224G4.html

SWITCH ADMINISTRABLE CAPA L2 24 PUERTOS POE CISCO CATALYST 2960 WS-C2960-24PC-L

Tabla 23.

Especificaciones de Cisco 2960

ESPICIFICACIONES DE CISCO 2960 CATALYST WS-C960-24TC-L	
TIPO DE DISPOSITIVO:	Cisco 2901 Integrated Services Router - encaminador
IMAGEN	
	2x 10/100/1000Base-T/SFP (mini-GBIC) E/S Total 24 puertos
PESO	5.4 kg
DIMENSIÓN	445 x 332 x 44 mm
DRAM MEMORIA	64 MB
TAMAÑO DE TABLA DE DIRECCIÓN MAC	8000 entradas
TAZA DE TRANSFERENCIA	0.1 Gbit/s
MEMORIA FLASH	32 MB
PROTOCOLO DE DIRECCIONAMIENTO	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático, enrutamiento IPv6 estático
PROTOCOLO DE GESTIÓN REMOTA:	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH
PROTOCOLO DE INTERCONEXIÓN DE DATOS	Ethernet, Fast Ethernet
PROTOCOLO DE GESTIÓN REMOTA	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH-2
TEMPERATURA	-5 - 45 °C
ALIMENTACIÓN	AC
PRECIO	S/.3806



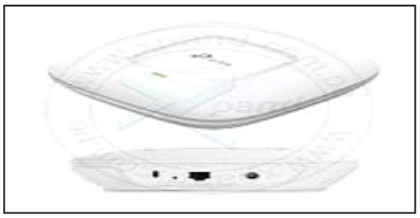
Los modelos con capacidad para enlazar PCs, servidores, teléfonos IP, puntos de acceso inalámbricos, cámaras de circuito cerrado de televisión y otros dispositivos de red vienen en una gran variedad de configuraciones.

Posibilidad de crear redes LAN virtuales que conecten a las personas en función de las funciones de la organización, los equipos de proyectos o las aplicaciones, en lugar de por criterios geográficos o físicos.

Fuente: http://ds3comunicaciones.com/cisco/WS-C2960-24PC-L.html

Tabla 24.

Especificaciones de TP-LINK

ESPECIFICACIONES DE ACCESS POINT TP-LINK AC1750		
IMAGEN DE DISPOSITIVO		
MODELO	AC1750	
DATOS DE OPERACION	MODO DE OPERACION	AP
	FRECUENCIA DE OPERACION	2.4 GHZ
		5 GHZ
	ESTANDARES	802.11a
		802.11b
		802.11g
		802.11n
		802.11ac
	SSID	HASTA 8 POR BANDA
	POTENCIA MAXIMA DE TRANSMISION	<20 dBm (2.4 GHZ) <23 dBm (5 GHZ)
	Seguridad	802.1X
		WEP 64/128/152-BIT
		WPA
		WPA-PSK
		WPA2-ENTERPRISE
		WPA2-PSK
	Ganancia	2.4 GHZ: 4 DBI
		5 GHZ: 4 DBI
	Velocidad de transferencia: 2.4 ghz: hasta 450 mb/s 5 ghz: hasta 1300 mb/s	
ESTRUCTURA	Montaje	TECHO / PARED (KIT INCLUIDO)
ALIMENTACION	Alimentación	12 VDC / 1.5 A

Fuente: http://www.tiendadecomputoperu.com/redes-inalambricas-wifi-empresa-inter-eap245-ac1750-dual-band-p-89437.html

3.2.5.2.1. Presupuesto de arquitectura de red.

Para poder presentar el presupuesto de la red propuesta hemos identificado y evaluado en primer lugar los dispositivos de la red en la Institución Educativa Privada Santa María Reina que cuenta actualmente siendo uno de los grandes problemas la conexión de red, debido a que se utiliza únicamente switch no administrables. Asimismo, la red carece de los puntos de conexión necesarios, lo que provoca lentitud y fallos frecuentes.

- **Análisis de dispositivos de redes actuales**

Tabla 25.

Análisis de dispositivos de redes actuales.

DISPOSITIVO	MARCA	CARACTERISTICA	CANTIDAD	MANTENIMIENTO
ROUTER	TP-LINK	4 PUERTOS	1	SIN MANTENIMIENTO
SWITCH	CISCO 877	4 PUERTOS	1	SIN MANTENIMIENTO
ANTENA	TP-LINK	1 PUERTO	1	SIN MANTENIMIENTO
SWITCH	TP-LINK	8 PUERTOS	1	SIN MANTENIMIENTO
SWITCH	TP-LINK	4 PUERTOS	4	SIN MANTENIMIENTO
CABLEADO		5E	N METROS	SIN MANTENIMIENTO
SERVIDOR DE BASE DE DATOS	DELL	INTEL INSIDE	2	SIN MANTENIMIENTO

Fuente: Elaboración Propia

Los equipos de red actuales de la Institución Educativa Privada Santa María Reina requieren un mantenimiento a nivel de software y de hardware, ya que están presentando problemas de lentitud e inoperatividad pudiendo ser vulnerables ante cualquier ataque.

Debido a la falta de mantenimiento preventivo, licencias originales y actuales, el servidor, que está en funcionamiento, sufre problemas de red. Los demás equipos se encuentran en un cuarto no acondicionado para ser centro de datos no teniendo la capacidad para suplir los roles necesarios que requiere la Institución Educativa. Los 4 switch restantes, se encuentran una en cada oficina de administración, no estando en un lugar adecuado, corriendo el riesgo de dañarse. Del mismo modo, según las normas de cableado estructurado, el cableado y el ponchado no son los más organizados. No contando por caja toma datos en cada puesto de trabajo, por lo que en el piso se encuentra el cableado.

No es el adecuado sistema de refrigeración, el lugar donde está ubicado no es el correcto, porque es una sala de reunión donde ingresa personal no autorizado donde se encuentran los equipos de red. Teniendo que apagar el equipo de refrigeración por varias horas corriendo el riesgo de que los equipos se calienten y puedan apagarse como ha sucedido a menudo.

- **Análisis de los dispositivos de la red propuesta.**

Nuestra red propuesta pretende implementar dispositivos que sean aptos para nuestra arquitectura de red y ante un avance o mejora en el futuro para ello se ha realizado exhaustivo, de acuerdo con las numerosas actividades que se realizan regularmente en el centro de estudios, En la Tabla 26 se detallan los costos a nivel de Hardware, es importante resaltar que se eligieron estos equipos de optimo rendimiento (calidad precio) siendo los siguientes:

Tabla 26.

Costos de Hardware

DISPOSITIVO	MARCA	CARACTERISTICA	CANTIDAD	MANTENIMIENTO	PRECIO
ROUTER	CISCO 2901	4 PUERTOS	1	CADA 1 AÑO	S/. 4055
SWITCH PRINCIPAL	CISCO SF300	24 PUERTOS	2	CADA 1 AÑO	S/. 2980
SWITCH DISTRIBCIÓN	CISCO 2960	24 PUERTOS	2	CADA 1 AÑO	S/. 3806

ACCESS POINT	TP-LINK	1 PUERTO	1	CADA 1 AÑO	S/. 358
CABLEADO		CAT6	N METROS	CADA 1 AÑO	S/. 5 EL METRO
SERVIDOR DE BASE DE DATOS	LENOVO	INTEL XEON	1	CADA 1 AÑO	S/. 4059

Fuentes: Elaboración Propia

Por otro lado, para la implantación de sistemas operativos, siempre hemos creído en proponer equipos con licencia porque permite aumentar las oportunidades de competitividad, productividad y mejora en la institución educativa, lo que redunda en el beneficio del usuario porque permite a los fabricantes seguir investigando e innovando en cuanto a la mejora técnica del producto; un desarrollo del sector educativo es que lleva al usuario a una mejor comprensión del producto. A continuación, en la Tabla 27 se detalla la inversión estimada en cuanto a licenciamiento de los sistemas operativos.

Debido al entorno en que se utilizan los equipos, requieren sistemas operativos como Windows 10 y Windows 7 de 64bits. Microsoft Windows es el Sistema Operativo más usado y utilizado en la mayor parte del mundo. Gran parte de los softwares educativos sólo son accesibles en las plataformas de Microsoft

Tabla 27.

Costos de Software

SISTEMA OPERATIVO	**CARACTERISTICA**	**CANTIDAD**	**PRECIO**
WINDOWS + VMs	SERVER 2012 R2	1	S/. 3466
WINDOWS 7	PRO	1	S/. 619
WINDOWS 10	PRO	2	S/. 649

Fuentes: Elaboración Propia

En la Tabla 28, hemos detallado los costos para la implementación de la red cableada, destacando los siguientes equipos y herramientas.

Tabla 28.

Costos de Implementación de la Red Cableada

DESCRIPCION	PRECIO
Gabinete de piso 37RU	S/. 2097
Rack de pared NEGRO 6RU	S/. 360
Patch panel de 24 Cat 6	S/. 980
Jacks categoría 6	S/. 19 x unid
Canaletas 100 x 60	S/. 30 x 4 unid
Canaletas 24 x 14	S/. 5 x 4 unid

Fuentes: Elaboración Propia

3.2.5.3. Gestión de configuración.

3.2.5.3.1. Configuración de equipos.

a. Configuración del router_principal

- **CONFIGURACIÓN DE ENTRADA**

```
hostname ROUTER_PRINCIPAL
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN CONEXIÓN A SERVIDORES**

```
spanning-tree mode pvst
interface GigabitEthernet0/0
description 'CONECTADO A SWITCH DE SERVIDORES'
ip address 172.17.128.129 255.255.255.128
duplex auto
speed auto
interface GigabitEthernet0/1
description 'CONECTADO A SWTICH PRINCIPAL'
ip address 10.10.1.1 255.255.255.252
duplex auto
speed auto
interface GigabitEthernet0/2
description 'CONECTADO A SWTICH BACKUP'
ip address 10.10.2.1 255.255.255.252
duplex auto
speed auto
```

- **ENRUTAMIENTO OSPF**

```
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
network 10.10.1.0 0.0.0.3 area 0
network 10.10.2.0 0.0.0.3 area 0
network 172.17.131.0 0.0.0.127 area 0
 network 172.17.128.128 0.0.0.127 area 0
```

- **Configuración de servicio de encriptación de contraseña**

```
banner motd ^CBIENVENIDO AL ROUTER PRINCIPAL^C
line con 0
 password 7 0812617C0C100B37475D
 login
line aux 0
line vty 0 4
 password 7 0812617C0C100B37475D
 login
end
```

3.2.5.3.2. Configuración del switch_principal.

- **CONFIGURACIÓN DE ENLACES TRONCALES**

```
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode desirable
!interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode desirable
!interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode desirable
!interface FastEthernet0/4
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode desirable
!interface FastEthernet0/5
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode desirable
!interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode desirable
!interface FastEthernet0/7
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 4 mode desirable
```

- **CONFIGURACIÓN DE PUERTOS A UNA VLAN**

```
interface Vlan1
no ip address
shutdown
!
interface Vlan30
mac-address 0060.5c24.cc01
ip address 172.17.129.2 255.255.255.128
standby 30 ip 172.17.129.1
standby 30 priority 200
standby 30 preempt
!
interface Vlan40
mac-address 0060.5c24.cc02
ip address 172.17.129.130 255.255.255.128
standby 40 ip 172.17.129.129
standby 40 priority 200
standby 40 preempt
!
interface Vlan50
mac-address 0060.5c24.cc03
ip address 172.17.130.2 255.255.255.128
standby 50 ip 172.17.130.1
standby 50 priority 200
standby 50 preempt
!

interface Vlan70
mac-address 0060.5c24.cc05
ip address 172.17.131.2 255.255.255.128
standby 70 ip 172.17.131.1
standby 70 priority 200
standby 70 preempt
```

- **CONFIGURACIÓN DE SERVIDOR DHCP**

```
ip dhcp excluded-address 172.17.130.2
ip dhcp excluded-address 172.17.130.3
ip dhcp excluded-address 172.17.130.1
ip dhcp excluded-address 172.17.131.2
ip dhcp excluded-address 172.17.131.3
ip dhcp excluded-address 172.17.131.1
ip dhcp excluded-address 172.17.130.130
ip dhcp excluded-address 172.17.130.131
ip dhcp excluded-address 172.17.130.129
ip dhcp excluded-address 172.17.129.130
ip dhcp excluded-address 172.17.129.131
ip dhcp excluded-address 172.17.129.129
ip dhcp excluded-address 172.17.130.132
ip dhcp excluded-address 172.17.130.149
ip dhcp excluded-address 172.17.130.150
ip dhcp excluded-address 172.17.129.2
ip dhcp excluded-address 172.17.129.3
ip dhcp excluded-address 172.17.129.1
!
ip dhcp pool AULAS-TALLERES
 network 172.17.130.0 255.255.255.128
 default-router 172.17.130.1
 dns-server 172.17.128.130
ip dhcp pool ACCESS-POINT
 network 172.17.131.0 255.255.255.128
 default-router 172.17.131.1
 dns-server 172.17.128.130
ip dhcp pool ADMINISTRATIVOS
 network 172.17.130.128 255.255.255.128
 default-router 172.17.130.129
 dns-server 172.17.128.130
ip dhcp pool LAB-SECUNDARIA
 network 172.17.129.128 255.255.255.128
 default-router 172.17.129.129
 dns-server 172.17.128.130
ip dhcp pool LAB-INICIAL
 network 172.17.129.0 255.255.255.128
 default-router 172.17.129.1
 dns-server 172.17.128.130
```

- **ENRUTAMIENTO OSPF**

```
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 10.10.2.0 0.0.0.3 area 0
network 172.17.130.0 0.0.0.127 area 0
network 172.17.131.0 0.0.0.127 area 0
network 172.17.130.128 0.0.0.127 area 0
network 172.17.129.128 0.0.0.127 area 0
network 172.17.129.0 0.0.0.127 area 0
```

- **CONFIGURACIÓN DE SERVICIO DE ENCRIPTACIÓN DE CONTRASEÑA**

```
banner motd ^CBIENVENIDO AL ROUTER PRINCIPAL^C
line con 0
 password 7 0812617C0C100B37475D
 login
line aux 0
line vty 0 4
 password 7 0812617C0C100B37475D
 login
end
```

3.2.5.3.3. CONFIGURACIÓN DEL SWITCH_BACKUP.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname ROUTER_PRINCIPAL
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN DE SERVIDOR DHCP**

```
ip dhcp excluded-address 172.17.130.2
ip dhcp excluded-address 172.17.130.3
ip dhcp excluded-address 172.17.130.1
ip dhcp excluded-address 172.17.131.2
ip dhcp excluded-address 172.17.131.3
ip dhcp excluded-address 172.17.131.1
ip dhcp excluded-address 172.17.130.130
ip dhcp excluded-address 172.17.130.131
ip dhcp excluded-address 172.17.130.129
ip dhcp excluded-address 172.17.129.130
ip dhcp excluded-address 172.17.129.131
ip dhcp excluded-address 172.17.129.129
ip dhcp excluded-address 172.17.130.132
ip dhcp excluded-address 172.17.130.149
ip dhcp excluded-address 172.17.130.150
ip dhcp excluded-address 172.17.129.2
ip dhcp excluded-address 172.17.129.3
ip dhcp excluded-address 172.17.129.1
ip dhcp pool AULAS-TALLERES
 network 172.17.130.0 255.255.255.128
 default-router 172.17.130.1
 dns-server 172.17.128.130
ip dhcp pool ACCESS-POINT
 network 172.17.131.0 255.255.255.128
 default-router 172.17.131.1
 dns-server 172.17.128.130
ip dhcp pool ADMINISTRATIVOS
 network 172.17.130.128 255.255.255.128
 default-router 172.17.130.129
 dns-server 172.17.128.130
ip dhcp pool LAB-SECUNDARIA
 network 172.17.129.128 255.255.255.128
 default-router 172.17.129.129
 dns-server 172.17.128.130
ip dhcp pool LAB-INICIAL
 network 172.17.129.0 255.255.255.128
 default-router 172.17.129.1
 dns-server 172.17.128.130
```

- **CONFIGURACIÓN DE ENLACES TRONCALES**

```
ip routing
spanning-tree mode pvst
spanning-tree vlan 30,40,50,60,70 priority 28672
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Port-channel4
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Port-channel5
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode auto
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode auto
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
```

```
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 4 mode desirable
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
 description 'CONECTADO A ROUTER PRINCIPAL'
 no switchport
 ip address 10.10.2.2 255.255.255.252
 ip ospf cost 20
 ip ospf 1 area 0
 duplex auto
 speed auto
```

- **CONFIGURACIÓN DE PUERTOS A UNA VLAN**

```
interface Vlan1
 no ip address
                                    shutdown
interface Vlan30
 mac-address 00d0.ff27.d201
 ip address 172.17.129.3 255.255.255.128
 standby 30 ip 172.17.129.1
 standby 30 priority 150
 standby 30 preempt
interface Vlan40
 mac-address 00d0.ff27.d202
 ip address 172.17.129.131 255.255.255.128
 standby 40 ip 172.17.129.129
 standby 40 priority 150
 standby 40 preempt
```

```
interface Vlan50
 mac-address 00d0.ff27.d203
 ip address 172.17.130.3 255.255.255.128
 standby 50 ip 172.17.130.1
 standby 50 priority 150
 standby 50 preempt
interface Vlan60
 mac-address 00d0.ff27.d204
 ip address 172.17.130.131 255.255.255.128
 standby 60 ip 172.17.130.129
 standby 60 priority 150
 standby 60 preempt
interface Vlan70
 mac-address 00d0.ff27.d205
 ip address 172.17.131.3 255.255.255.128
 standby 70 ip 172.17.131.1
 standby 70 priority 150
 standby 70 preempt
```

- **ENRUTAMIENTO OSPF**

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 10.10.1.0 0.0.0.3 area 0
 network 172.17.130.0 0.0.0.127 area 0
 network 172.17.131.0 0.0.0.127 area 0
 network 172.17.130.128 0.0.0.127 area 0
 network 172.17.129.128 0.0.0.127 area 0
```

- **CONFIGURACIÓN DE ENCRIPTACIÓN DE CONTRASEÑA**

```
banner motd ^CBIENVENIDO AL SWITCH BACKUP^C
line con 0
 password 7 0812617C0C100B37475D
 login
line aux 0
line vty 0 4
 password 7 0812617C0C100B37475D
 login
end
```

3.2.5.3.4. Configuración de SWITCH_A.

- **CONFIGURACIÓN DE ENCRIPTACIÓN DE CONTRASEÑA**

```
hostname SW_A
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface Port-channel1
interface Port-channel2
interface FastEthernet0/1
 switchport access vlan 70
interface FastEthernet0/2
 switchport access vlan 70
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
 switchport access vlan 50
interface FastEthernet0/8
 switchport access vlan 50
```

```
interface FastEthernet0/9
 switchport access vlan 50
interface FastEthernet0/10
 switchport access vlan 50
interface FastEthernet0/11
 switchport access vlan 50
interface FastEthernet0/12
 switchport access vlan 50
interface FastEthernet0/13
 switchport access vlan 50
interface FastEthernet0/14
 switchport access vlan 50
interface FastEthernet0/14
 switchport access vlan 50
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 shutdown
```

3.2.5.3.5. Configuración de SWITCH_B.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_B
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
switchport access vlan 50
interface FastEthernet0/8
switchport access vlan 50
interface FastEthernet0/9
switchport access vlan 50
interface FastEthernet0/10
switchport access vlan 50
interface FastEthernet0/11
switchport access vlan 50
interface FastEthernet0/12
switchport access vlan 60
interface FastEthernet0/13
switchport access vlan 70
interface FastEthernet0/14
switchport access vlan 70
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
no ip address
shutdown
banner motd ^CBIENVENIDO AL SW_B^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
password 7 0812617C0C100B37475D
login
line vty 0 4
password 7 0812617C0C100B37475D
login
line vty 5 15
login
end
```

3.2.5.3.6. Configuración de SWITCH_B_1.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_B1
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
switchport access vlan 50
interface FastEthernet0/2
switchport access vlan 50
interface FastEthernet0/3
switchport access vlan 50
interface FastEthernet0/4
switchport access vlan 50
interface FastEthernet0/5
switchport access vlan 70
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
switchport mode trunk
interface GigabitEthernet0/2
interface Vlan1
no ip address
shutdowninterface GigabitEthernet0/2
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
no ip address
shutdown
banner motd ^CBIENVENIDO AL SW_B1^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
end
```

3.2.5.3.7. Configuración de SWITCH_B_2.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_B2
enable secret 5
$1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport access vlan 40
interface FastEthernet0/2
 switchport access vlan 40
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
 switchport access vlan 40
interface GigabitEthernet0/2
 switchport mode trunk
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
 no ip address
 shutdown
banner motd ^CBIENVENIDO AL SW  B2^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
en
```

3.2.5.3.8. Configuración de SWITCH_B_3.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_B3
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN PROTOCOLO SPANNING TREE**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
 no ip address
 shutdown
banner motd ^CBIENVENIDO AL SW  B3^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
en
```

3.2.5.3.9. Configuración de SWITCH_C.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_C
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN PROTOCOLO SPANNING TREE**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport access vlan 60
interface FastEthernet0/2
 switchport access vlan 60
interface FastEthernet0/3
 switchport access vlan 50
interface FastEthernet0/4
 switchport access vlan 50
interface FastEthernet0/5
 switchport access vlan 70
interface FastEthernet0/6
 switchport access vlan 70
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
 no ip address
 shutdown
banner motd ^CBIENVENIDO AL SW  C^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
end
```

3.2.5.3.10. Configuración de SWITCH_D.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_D
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport access vlan 60
interface FastEthernet0/2
 switchport access vlan 50
interface FastEthernet0/3
 switchport access vlan 50
interface FastEthernet0/4
 switchport access vlan 50
interface FastEthernet0/5
 switchport access vlan 50
interface FastEthernet0/6
 switchport access vlan 50
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
 switchport access vlan 70
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
 no ip address
 shutdownbanner motd ^CBIENVENIDO AL SW_D^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
end
```

3.2.5.3.11. Configuración de SWITCH_D_1.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_D1
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport access vlan 60
interface FastEthernet0/2
 switchport access vlan 50
interface FastEthernet0/3
 switchport access vlan 50
interface FastEthernet0/4
 switchport access vlan 50
interface FastEthernet0/5
 switchport access vlan 50
interface FastEthernet0/6
 switchport access vlan 50
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
 switchport access vlan 70
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
 no ip address
 shutdownbanner motd ^CBIENVENIDO AL SW_D1^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
en
```

3.2.5.3.12. Configuración de SWITCH_D_2.

- **CONFIGURACIÓN DE ENTRADA**

```
hostname SW_D2
enable secret 5 $1$mERr$FJzd3P0jVeUJMtfU1cFnh0
```

- **CONFIGURACIÓN INTERFACE VLAN**

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport access vlan 50
interface FastEthernet0/2
 switchport access vlan 50
interface FastEthernet0/3
 switchport access vlan 50
interface FastEthernet0/4
 switchport access vlan 50
interface FastEthernet0/5
 switchport access vlan 50
interface FastEthernet0/6
 switchport access vlan 50
interface FastEthernet0/7
 switchport access vlan 50
interface FastEthernet0/8
 switchport access vlan 50
interface FastEthernet0/9
 switchport access vlan 50
interface FastEthernet0/10
 switchport access vlan 50
interface FastEthernet0/11
 switchport access vlan 50
interface FastEthernet0/12
 switchport access vlan 50
interface FastEthernet0/13
 switchport access vlan 70
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
 switchport mode trunk
interface GigabitEthernet0/2
```

- **CONFIGURACIÓN BANNER**

```
interface Vlan1
 no ip address
 shutdownbanner motd ^CBIENVENIDO AL SW_D2^C
```

- **CONFIGURACIÓN CONTRASEÑA**

```
line con 0
 password 7 0812617C0C100B37475D
 login
line vty 0 4
 password 7 0812617C0C100B37475D
 login
line vty 5 15
 login
en
```

3.2.5.4. Gestión de Seguridad.

Como se ha dicho anteriormente, una red en una instalación educativa puede utilizarse para una variedad de fines.

Trataremos de una variedad de aspectos dentro del concepto de seguridad:

- **Seguridad del sistema:** es estable y resistente a la manipulación por parte de usuarios no cualificados, ya sea de forma intencionada o no.
- **Seguridad de contenidos:** Evitar que los alumnos accedan a material inadecuado.
- **Seguridad antivirus:** Ponga en marcha protecciones para evitar que los virus infecten los ordenadores a través de la instalación de software, recibir correos electrónicos o descargar sitios web o archivos
- **Seguridad de intervención remota:** para evitar que otros obtengan acceso a nuestra red.

3.2.5.4.1. Seguridad del sistema.

El principal adversario de la estabilidad de un sistema son sus usuarios. Hay que tener en cuenta la capacidad de los usuarios para alterar la configuración del sistema y del ordenador a la

hora de proponer el desarrollo de una red. Para alcanzar el mayor nivel de seguridad, debemos configurar una red con un programa de servidor que gestiona los perfiles de los usuarios.

La propuesta sería:

- **Administrador:** Responsable del aula. Control total del sistema.
- **Usuario avanzado:** Profesores. Tienen la capacidad de instalar programas que no tienen impacto en el sistema, así como crear grupos de usuarios y configurar los recursos del sistema.
- **Usuario:** alumnado. Sólo debe actuar con total control sobre los archivos del sistema que ha creado.

No se puede estar seguro de que estas medidas mejorarán la seguridad y la integridad del sistema. En consecuencia, las copias de seguridad diarias (basadas en criterios de optimización del proceso) y generar imágenes de los equipos que puedan cargarse a distancia o a través de un CD-ROM.

3.2.5.4.2. Seguridad de contenidos.

Uno de los problemas más preocupantes para los profesores a la hora de utilizar la red es el acceso al contenido de Internet. La mayoría de los navegadores tienen herramientas para controlar el acceso a los contenidos basándose en los sistemas de clasificación. Todas las páginas web no clasificadas pueden bloquearse y se pueden adherir páginas específicas.

Otra alternativa es instalar un software que filtre la información y separe el material potencialmente peligroso del resto de la información e impida que los alumnos lo obtengan.

- NET NANNY
- CYBERSITTER
- CYBER PATROL

Estos programas son al 99 por ciento eficaces, como se afirma en la sección anterior.

3.2.5.4.3. Seguridad antivirus.

Todos los expertos están de acuerdo en que conectar un equipo informático a Internet sin infectarse con un virus es virtualmente imposible. Sin embargo, el riesgo es mucho mayor si no tiene un programa antivirus que se actualice de forma regular.

En consecuencia, es beneficioso tener instalado y actualizado el software antivirus para tener ciertas garantías de que no se infectará con ningún virus.

La configuración de nuestra red determinará cómo se instala este tipo de programa. Podemos sistematizar la actualización del archivo de firma y del propio programa si tenemos un ordenador configurado con un programa de servidor.

Debemos configurar la actualización en cada una de las posiciones si no tenemos este equipo.

Las siguientes son tareas que deben programarse o completarse con un programa antivirus:

• Analizar el correo electrónico (activo) y todo el equipo (semanal)

• Analizar el sector de arranque de C: (al iniciar Windows)

• Actualización del fichero de firmas (diario) y del programa (mensual)

También hay otras formas de evitar que se envíen archivos desordenados por correo electrónico o navegador. Por ejemplo, en un correo electrónico, tendremos que deshabilitar la vista anterior, mientras que necesitaremos limitar la ejecución del control ActiveX, evitar la descarga y establecer un alto nivel de seguridad cuando esté en un navegador.

Por último, hacer particiones en los discos duros de los ordenadores es muy útil para asegurar que no perdemos todos nuestros datos en caso de una infección grave.

3.2.5.4.4. Seguridad ante intrusos.

La infiltración de intrusos en las redes es cada vez más común. Para evitar esta intrusión, necesitaremos instalar un sistema de seguridad. Este elemento de red es esencialmente un sistema (equipo o programa) que puede controlar desde el nivel OSI 3 hasta el nivel OSI 7, puede controlar el acceso de paquetes y aplicaciones a nuestra red.

El cortafuegos de nuestra red sirve como primera línea de protección, permitiéndonos bloquear puertos, prohibir la ejecución de scripts y filtrar datos. Algunos pueden encargarse también del control de acceso. A continuación, se enumeran algunos programas gratuitos:

• Agnitum outpost firewall

• Freedom.

• Tiny.

Hay cortafuegos libres y de paga disponibles, y puedes configurar uno con un pentium y Linux. A fin de cuentas, se trata de gestionar el flujo de información que entra y sale de nuestros dispositivos.

Dado que su funcionamiento está basado en el perímetro, también es posible establecer una serie de restricciones para los usuarios avanzados con el fin de evitar que se instalen determinadas aplicaciones o programas.

Por último, existen herramientas que nos permiten escanear nuestros ordenadores para ver si estamos siendo vigilados, ya que los cortafuegos suelen ofrecer una falsa impresión de protección.

3.3. Fase 3: Diseño físico

3.3.1. Parte 10: Selección de tecnologías y dispositivos de red

3.3.1.1. Cableado UTP – Categoría 7.

- El cable está en conformidad con el estándar de protección contra incendios: UL VW-1, IEC 60332-1.
- Material del forro: LSZH (refractario, de baja emisión de humo, no contiene halógenos).
- 4 pares trenzados 23 AWG dispuestos alrededor del alambre de drenaje.
- Cada par está envuelto en una lámina de aluminio-poliéster (lámina de aluminio por fuera) que cubre el 100% del revestimiento del par trenzado.
- Color de los pares trenzados: Blanco/azul – azul, Blanco/naranja – naranja, Blanco/verde – verde, Blanco/marrón – marrón.
- Cantidad de pares: 4
- Cantidad de hilos: 8
- Aislamiento: SFS PO, 1.43 mm
- Conductor: hilo de cobre desnudo, 23 AWG
- Esfuerzo durante el tendido del cable: 130 N máximo durante la instalación.

Para el cableado estructurado de toda la institución tendrá también algunas especificaciones como: EIA/TIA BULLETIN TSB-36, ISO/IEC DIS 11801, ISO/IEC 754-2, CENELEC EN 50288, CENELEC EN 50173.

3.3.1.2. Patch Cord UTP categoría 7.

- Temperatura de funcionamiento: +75ºC, resistente al fuego.
- Diámetro exterior del cable 5.3±0.2 mm.
- 4 Pares trenzados con forro de PVC (0.4 mm) color de pares.
- Diámetro del hilo 1.03±0.02 mm.
- Aislamiento: polietileno denso, grosor mínimo 0.18 mm
- Conductor: 7 hilos de cobre Ø0.2±0.01 mm, 24 AWG.

Las especificaciones que se cumplen son los estándares UL444/UL1581, TIA/EIA 568B.2-1.

3.3.1.3. Gabinete de Piso 37 RU.

- Tratamiento de la superficie para evitar que la corrosión y otras influencias ambientales causen daños.
- Hoja de acero laminado en frío de excelente calidad. Grosor: 2,0 mm en los bordes de los ángulos, 1,2 a 1,5 mm de espesor en el resto.
- Diseñado para adaptarse a los equipos de montaje en bastidor que cumplen la norma EIA de 19 pulgadas.
- Se incluye un sistema de gestión de cables en la parte superior interior del gabinete.
- El transporte e instalación de la unidad están facilitada por la base de apoyo y ruedas.
- Sólida construcción con materiales de alta calidad, pensados específicamente para la colocación de equipos pesados.
- Cumple con las especificaciones ANSI/EIA RS-310-D, DIN41491: PART1, IEC297-2, DIN41494: PART7 y GB/T3047.92.

3.3.1.4. Gabinete de Pared 6RU.

- Puerta con centro de acrílico polarizado de 3mm.
- Cuenta con 2 rieles, tropicalizado, con perforaciones circulares, normalizados en 19".
- Entrada y salida de cables a través del marco desmontable.
- Ofrece una resistencia cinco veces mayor al óxido y ralladuras.
- Fabricado con acero LAF de 1.2mm
- Diseñado según la norma EIA – 310D.

3.3.1.5. Jack RJ45.

- Cumple con las normas TIA/EIA.
- Ideal para aplicaciones de datos, voz o video con la mínima atenuación.
- Instalables tanto en los Face-Plate (Placa de Pared) como también en los Patch Panel.
- Diseñados para cumplir y exceder los requerimientos del estándar ANSI/TIA-568-C.2.
- Las terminaciones T568A/T568B están codificadas por colores según la norma.
- Jack modulares para 4 pares trenzados
- El empalme de cables horizontales y de cables de conexión se realiza con esta interfaz.

3.3.1.6. Faceplate.

- Los puntos se instalarán en las zonas de trabajo y donde sean necesarios puntos de toma de red.
- Debe cumplir con las normas TIA/EIA.
- Su presentación está disponible en varios tonos, siendo el marfil y el blanco los más frecuentes
- Se requiere soporte para hasta cuatro estándares de conexión para configuraciones personalizadas
- Faceplate con dos puertos de iconos en ángulo de 45 grados para red, teléfono y 4 video Jack modular de pares trenzados
- Contar con dos puertos para conectores UTP.

3.3.1.7. Switch Cisco Catalyst 2960 – 24T.

Tabla 29.

Tabla de características del Switch Cisco Catalyst 2960-24T.

CARACTERÍSTICA	DESCRIPCIÓN
Tasas de reenvío	Entre 16 a 32 Gbps
Números de puertos	24 puertos 100 Mbps – 02 puertos 1000 Mbps
Funciones de LANs avanzadas	- Conmutación multicapa. - QoS. - ACL. -VLANs
Memoria Ram	32 MB
Memoria Flash	16 MB
Protocolo de Gestión de Remota	SNMP 2c, SNMP 3, Telnet, RMON, SNMP 1.
Estándar	10/100/1000 Mbps.
Voltaje de Alimentación	100 – 240 VAC.
Cumplimiento de Normas	IEEE 802.3ab, IEEE 802.1Q, IEEE 802.1D, IEEE 802.3, IEEE 802.3z, IEEE 802.3u.
Dimensiones	1.73 x 17.5 x 9.3 in. (4.4 x 44.5 x 23.6 cm

Fuente: Elaboración Propia

3.3.1.8. Switch Cisco Catalyst 2960 – 48TC.

Tabla 30.

Tabla de características del Switch Cisco Catalyst 2960-48TC

CARACTERÍSTICA	DESCRIPCIÓN
Tasas de reenvío	Entre 32 a 64 Gbps.
Números de puertos	48 puertos 100 Mbps – 02 puertos 1000 Mbps.
Funciones de LANs avanzadas	- Conmutación multicapa.
	- QoS.
	- ACL
	-VLANs.
Memoria Ram	32 MB
Memoria Flash	32 MB
Protocolo de Gestión de Remota	SNMP 2c, SNMP 3, Telnet, RMON, SNMP 1.
Estándar	10/100/1000 Mbps.
Voltaje de Alimentación	100 – 240 VAC.

Fuente: Elaboración propia

3.3.1.9. Router CISCO 2811

Tabla 31.

Tabla de características del Router CISCO 2811

CARACTERÍSTICA	DESCRIPCIÓN
FACTOR DE FORMA	EXTERNO – MODULAR -1U
ANCHURA	43.8 CM, 43.82 CM
PROFUNDIDAD	41.7 CM, 41.66 CM
ALTURA	4.5 CM, 4.45 CM
PESO	6.5 KG
MEMORIA RAM	256 MB (instalados) / 768 MB (máx.) – DDR SDRAM, 256 MB (instalados) / 760 MB (máx.) – DDR SDRAM.
MEMORIA FLASH	64 MB (instalados) / 256 MB (máx.)

PROTOCOLO DE INTERCONEXIÓN DE DATOS	Ethernet, Fast Ethernet
RED / PROTOCOLO DE TRANSPORTE	IPSec
PROTOCOLO DE GESTIÓN REMOTA	SNMP 3
FUNCIONES DE LAN AVANZADAS	- QoS - ACL.
INDICADORES DE ESTADO	Alimentación y actividad de enlace.
Cifrado de 256 bits, filtrado de URL, asistencia técnica VPN, cifrado del hardware, criptografía 128 bits, diseño modular, soporte de MPLS, cifrado del hardware, Protección firewall.	

Fuente: Elaboración Propia

3.3.1.10. Access Point Linksys WRT300N.

Tabla 32.

Tabla de características de Access Point Linksys WRT300N

CARACTERÍSTICA	DESCRIPCIÓN
FACTOR DE FORMA	EXTERNO
DIMENSIONES	18.8 X 17.6 X 4 CM
PESO	0.53 KG
INTERFACES	4 x network - Ethernet 10Base-T/100Base-TX - RJ-45, 1 x network - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)
CARACTERÍSTICAS	MIMO technology, Firmware update, Access Point operational mode, VPN passthrough, 256-bit encryption, MAC address filtering, Stateful Packet Inspection (SPI), auto uplink (auto MDI/MDI-X), auto-negotiation, switch MDI/MDI-X, NAT support, DHCP support, Sensing per device, Porta DMZ, Firewall protection, Full duplex capability.
PROTOCOLO DE TRANSPORTE	PPPoE, IPSec, L2TP, PPTP.
Normas de cumplimiento	IEEE 802.11n (draft), IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Protocolo de conmutación	Ethernet
Protocolo de enrutamiento	Static IP Routing

Banda de frecuencia (GHz)	5.4 GHz y 2.4Ghz.
Interruptor integrado	4 – port Switch
Algoritmo de cifrado	WPA2, WPA, WEP 64 bit, WEP 128 bit

Fuente: Elaboración Propia

3.3.2. Parte 11: Cableado estructurado de la red informática

La Topología a usar en el Cableado Estructurado del Centro Educativo Particular "Santa María Reina" es la Topología Estrella y Protocolo de comunicación TCP/IP.

Para la instalación se utilizará el cable UTP de 8 hilos de categoría 7, que garantiza la transmisión de 10-Gigabit Ethernet (XGbE o 10GbE), que es actualmente el más rápido de los estándares Ethernet, capaz de transmitir una velocidad nominal de 10 Gbit/s.

Algunos elementos que se usaran para el cableado estructurado son:

- **Cuarto de Comunicaciones**

Es el lugar donde se concentran los equipos y las conexiones activas de la red, como el Switch, los Servidores (Aplicaciones, Archivos, etc.) y el Router que enlazará la red con Internet.

- **Área de Trabajo**

La Faceplate se conectará a la estación de trabajo mediante un Patch Cord de categoría 7.

- **Cableado Horizontal**

Constituido por el cable que va desde el área de trabajo hasta el gabinete de dispositivos tendrá una topología en estrella, con un punto por cada salida de los puestos de trabajo, y debe terminar en una caja protegida por su faceplate. El cable no debe discurrir a ras de suelo más de 90 metros lineales, medidos desde la zona de trabajo hasta la sala de comunicaciones. Los Patch cables no deben tener más de 3 metros de longitud. Se ha medido la cantidad de cable y material que hay que emplear desde el gabinete del aparato hasta todos los puestos de trabajo.

- **Gabinete de Dispositivos**

Comprende los gabinetes que albergan los dispositivos de interconexión (Routers, Servidores, Switches) así como las terminaciones de los cables que salen de los terminales de los puestos de trabajo.

3.3.3. Parte 12: Dispositivos de interconexión a usar

Se empleará 2 dispositivos de interconexión entre el router y el switch, el cual deben tener características importantes como los siguientes:

Tabla 33.

Dispositivos de Interconexión a usar.

DISPOSITIVO	CARACTERÍSTICAS
SWITCHES	✓ Dispositivo certificado ✓ Disponibilidad de soporte técnico ✓ Costo bajo ✓ Auto sensibilidad de velocidad ✓ Operaciones a nivel de Capa de Enlace ✓ Cantidad de Puertos ✓ Soporta Tecnología LAN.
ROUTER	✓ Firewall. ✓ Soporte de Listas de Control de Accesos. ✓ Seguridad. ✓ Dispositivo certificado.

Fuente: Elaboración Propia

3.3.4. Parte 13: Planos Propuestos para el Diseño Físico de la Red

Figura 27

Plano Primer Piso

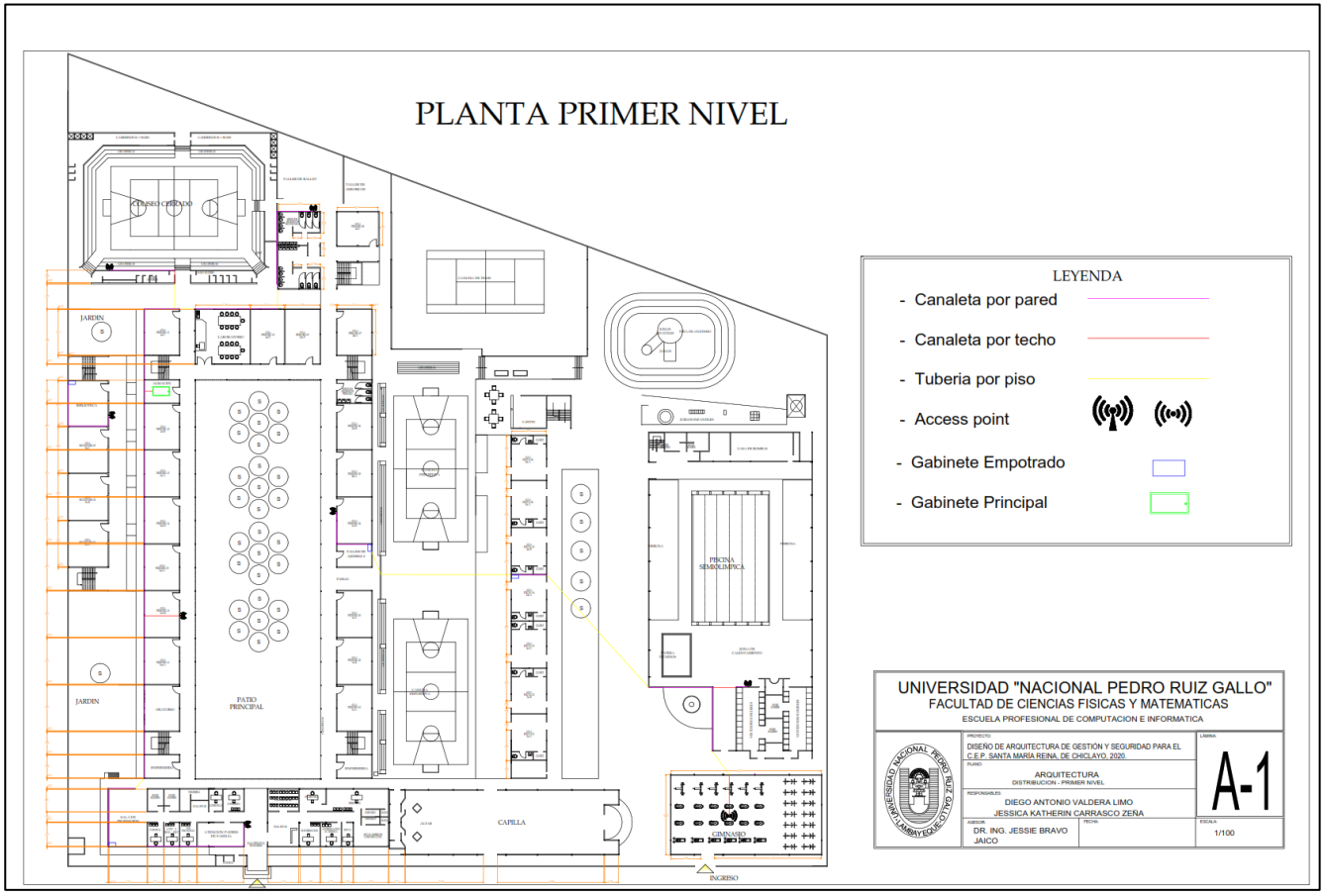


Figura 28

Plano Segundo Piso

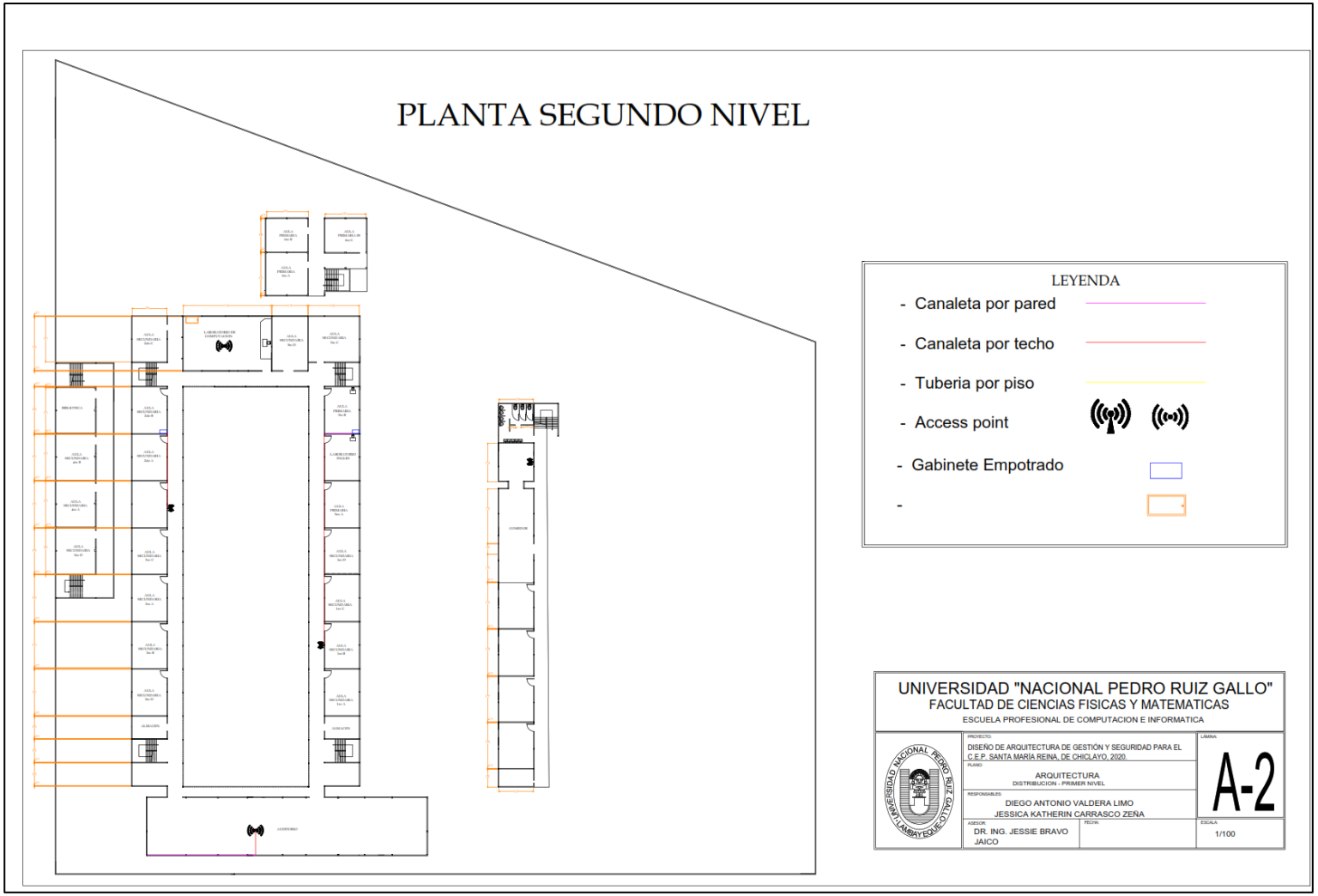
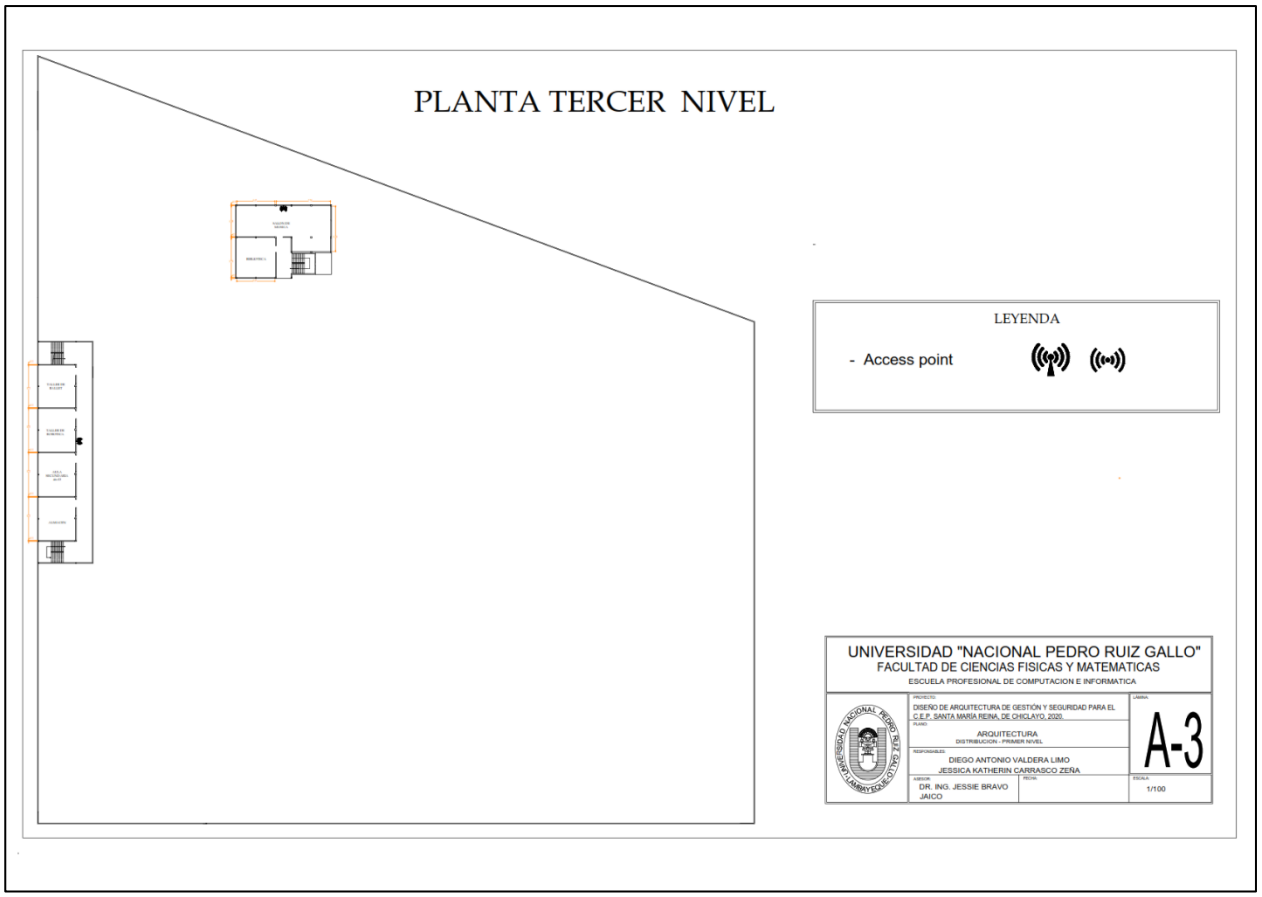


Figura 29

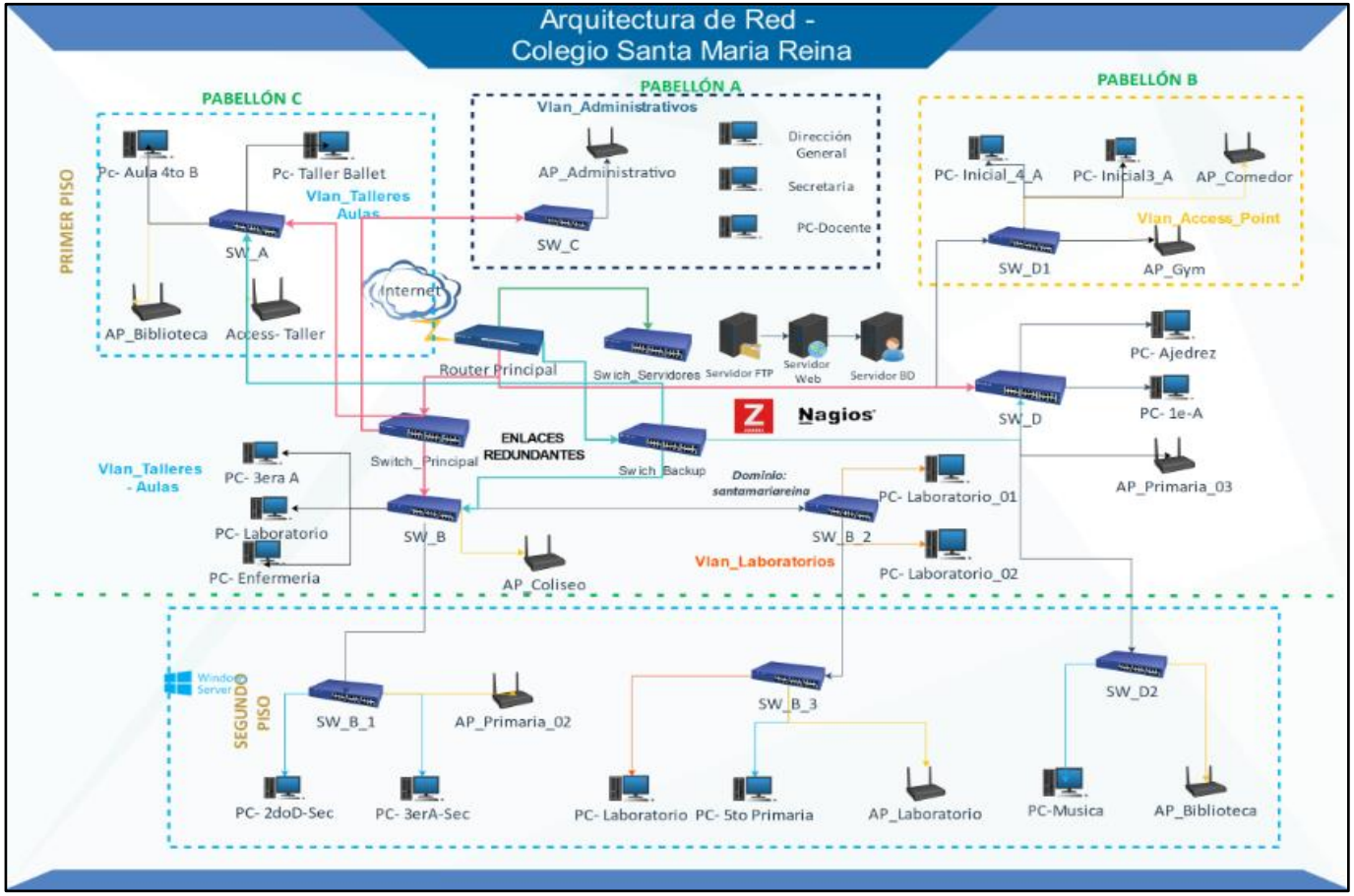
Plano Tercer Piso



3.3.5. Parte 14: Diseño de Arquitectura de Red

Figura 30

Diseño de Arquitectura de Red



3.4. Fase 4: Testeo, optimización y documentación de la red

3.4.1. Parte 15: Testeo

Se procedió a utilizar la herramienta Nagios para el monitoreo de los dispositivos y de la red propuesta para el Colegio Santa Maria Reina. De aquí en adelante, se realizaron las instalaciones de VMware y en CentOS, la configuración del servidor muestra el siguiente usuario: **[root@localhost ~]#.** Ver Figura 31

Figura 31

Usuario y password para ingresar a Nagios

El acceso a Centros se realiza en modo root y se introduce la siguiente contraseña una vez que se ha instalado en la estación de trabajo virtual VMware, a partir de aquí, se comienza a personalizar la configuración de Nagios. A continuación, se muestra la creación de los archivos que necesitamos para el monitoreo de la red del colegio Santa María Reina:

Configuración de grupos de PC's

Se configuran los grupos de PC's utilizadas en las áreas del colegio, por ejemplo, en áreas como Laboratorio, Administrativo, Aulas.

- **Para crear o modificar el archivo de grupos de PC's, digitaremos en Nagios lo siguiente**:

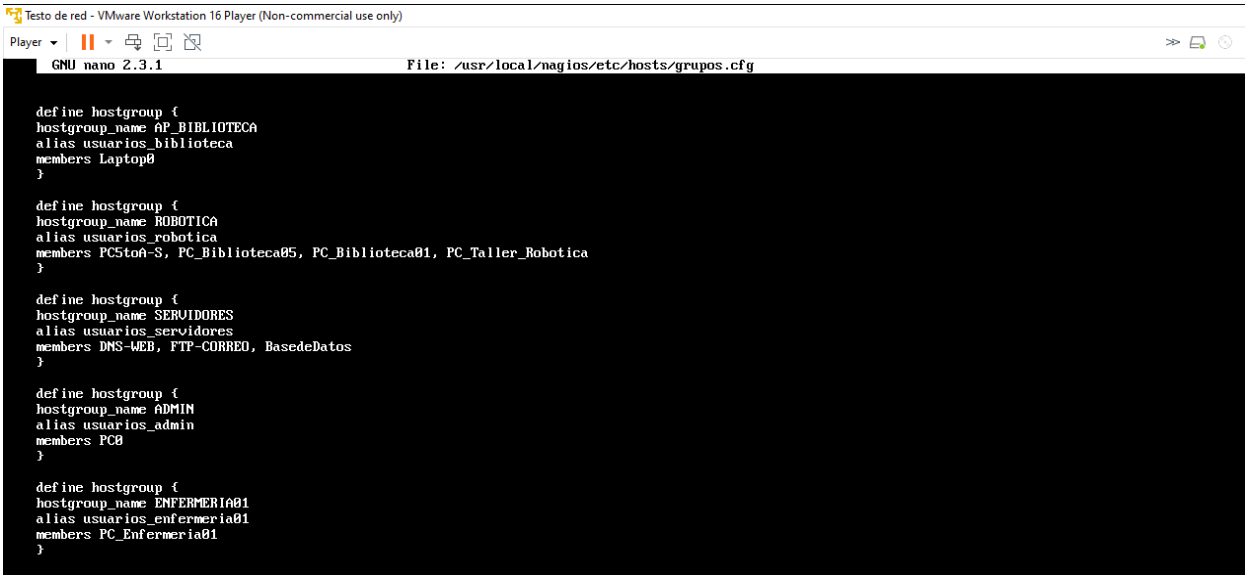
sudo nano /usr/local/nagios/etc/hosts/grupos.cfg

- **Crear el contenido de las PC's, se utilizó**:

define hostgroup {
hostgroup_name Laboratorio (Nombre del área)
alias usuarios_laboratorio
members laptop01, pclab01 (Nombre de las PCs dentro del área)
}

Figura 32

Configuración de grupos de PC's



Configuración de PC's

Se configura todas las PC's, teniendo en cuenta todas las PC's que se definen en members.

- **Para crear o modificar el archivo de PC's, digitamos en Nagios lo siguiente:**

sudo nano /usr/local/nagios/etc/hosts/servidores.cfg

- **Para crear el contenido cada PC, se utilizó:**

```
        define host {
 host_name            laptop01
 alias                laptop01
 address              192.168.1.2
check_command         check-host-alive
max_check_attempts     10
notification_interval    0
notification_period     24x7
notification_options     d,u,r
notifications_enabled    1
contact_groups           contactos_sistemas
```

En contact_groups, se crearon los grupos de contactos que monitorean las redes por ejemplo sistemas.

Figura 33

Configuración de PC's

<u>Configuración de Grupo de Contactos</u>

Se configura el grupo de personas que supervisan la red. Aquí va la definición del grupo que se pone arriba en contact_groups.

- **Para crear o modificar el archivo de grupo de contactos, digitamos lo siguiente:**

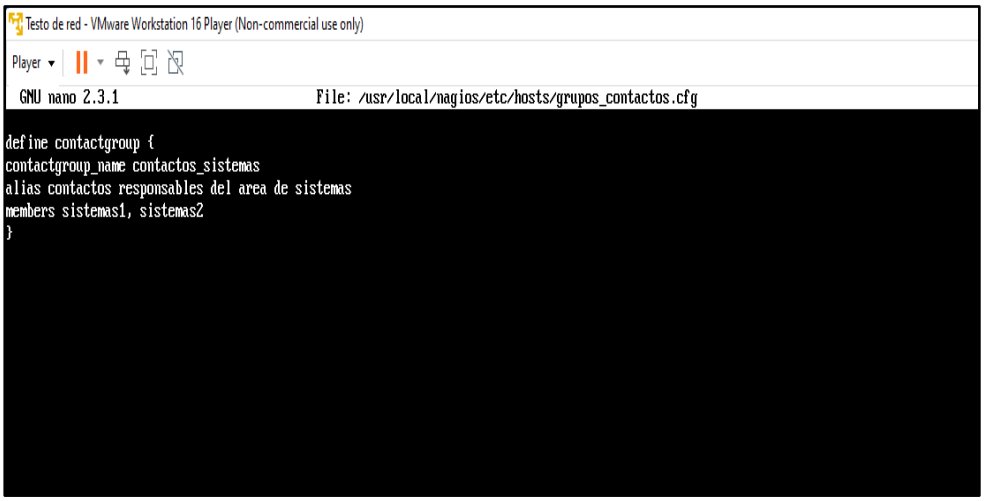
```
sudo nano /usr/local/nagios/etc/hosts/grupos_contactos.cfg
```

- **Para crear el contenido de grupo de contactos, se utilizó:**

```
        define contactgroup {
contactgroup_name     contactos_sistemas (aca va el nombre del grupo de contactos)
   alias                    Contactos responsables del area de sistemas
   members                sistemas1, sistemas2
   }
```

Figura 34

Configuracion de grupo de contactos



Configuración de Contactos

Aquí va la definición del grupo que se pone arriba en contact_groups

- **Para crear o modificar el archivo de PC's, se digitó lo siguiente:**

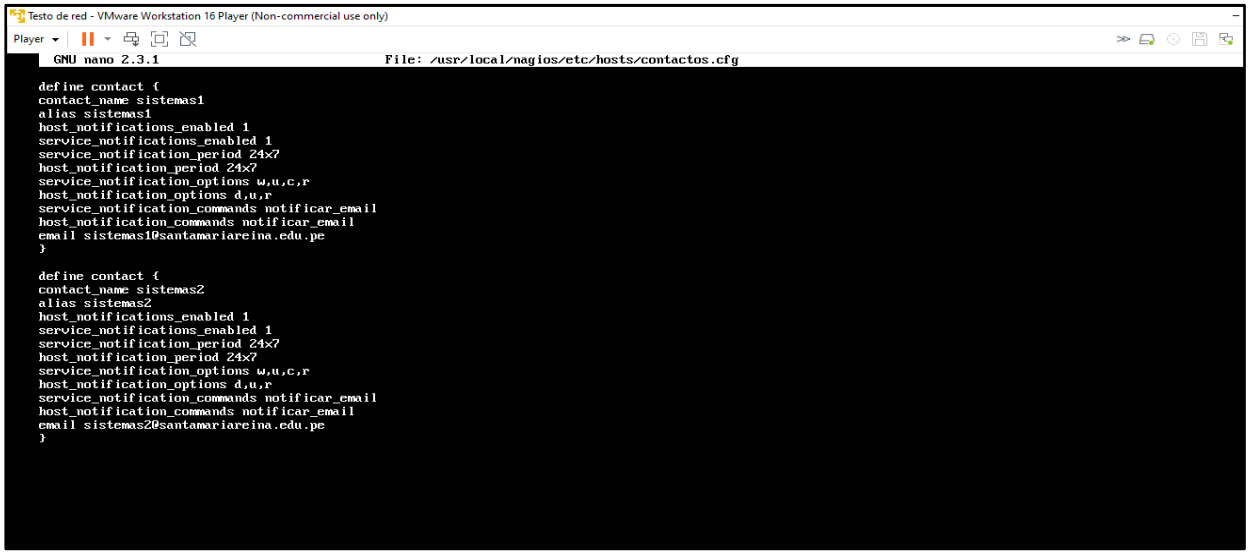
```
sudo nano /usr/local/nagios/etc/hosts/grupos_contactos.cfg
```

- **Para crear el contenido cada contacto se utilizó:**

```
        define contact {
  contact_name                  sistemas1
  alias                         sistemas1
  host_notifications_enabled 1
  service_notifications_enabled 1
  service_notification_period     24x7
  host_notification_period        24x7
  service_notification_options     w,u,c,r
  host_notification_options       d,u,r
  service_notification_commands   notificar_email
  host_notification_commands      notificar_email
  email                           sistemas1@santamariareina.edu.pe (aca va el correo de
sistemas)
  can_submit_commands 1
 }
```

Figura 35

Configuración de contactos



<u>Inicio de sesión en la interfaz web de Nagios</u>

Finalmente, se abre un navegador y hay que colocar el url "http:// IP-address server

/nagios" en este caso http://192.168.0.144/nagiosxi y se coloca el nombre de usuario

"nagiosxi" y la contraseña configurada. Editar el archivo si desea modificar el nombre de usuario y/o la contraseña de acceso a la web:

usr/local/nagios/etc/cgi.cfg sustituya el nombre del usuario por el nombre de usuario deseado en este archivo de configuración.

Figura 36

Interfaz web de Nagios

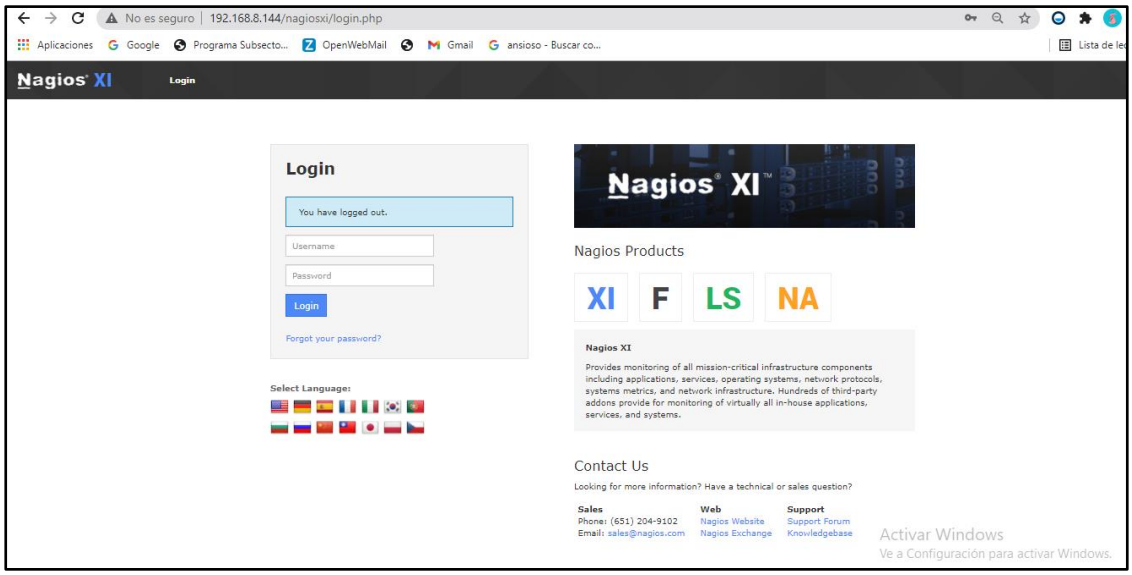


Figura 37

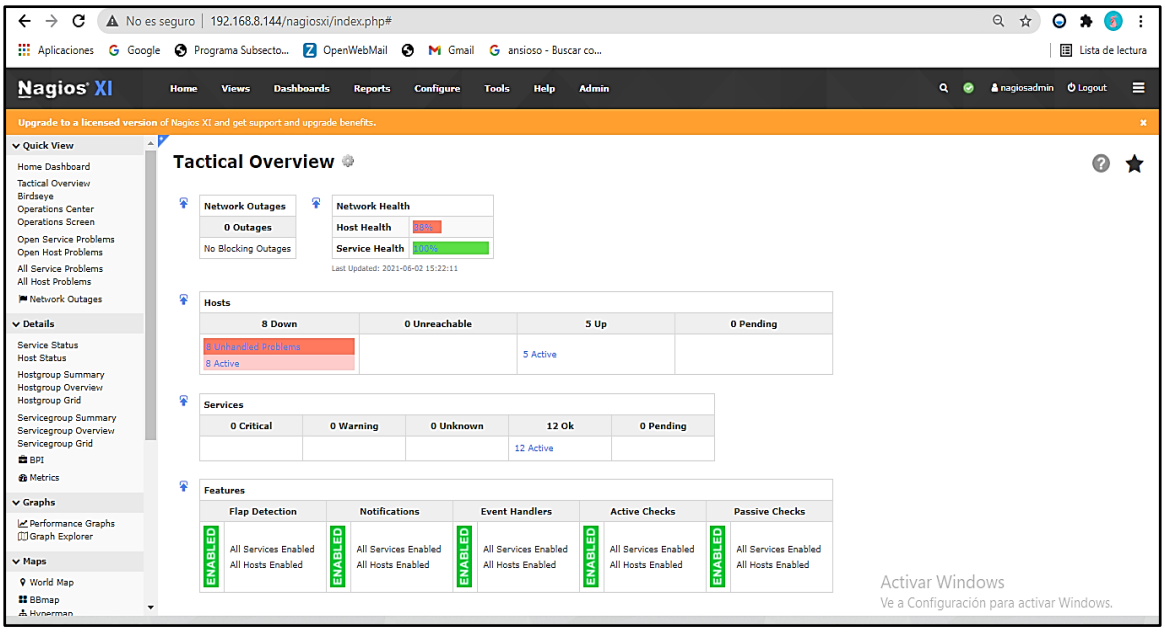
Lista de alertas que percibe el Administrador

ALERTA	SIGNIFICADO
WARNING	El servicio tiene valores superiores al valor percibido como aceptable.
CRITICAL	El servicio tiene valores superiores o iguales valor percibido como crítico.
DOWN	El host en cuestión no tiene conectividad a la red
RECOVERY	El host en cuestión ha recuperado la conectividad a la red
UP	El host en cuestión tiene conectividad a la red

Una vez dentro de la web Nagios, nos dirigimos a Tactical overview, donde podemos observar el estado de los equipos y servicios que se están monitoreando en la red del Colegio Santa Maria Reina.

Figura 38

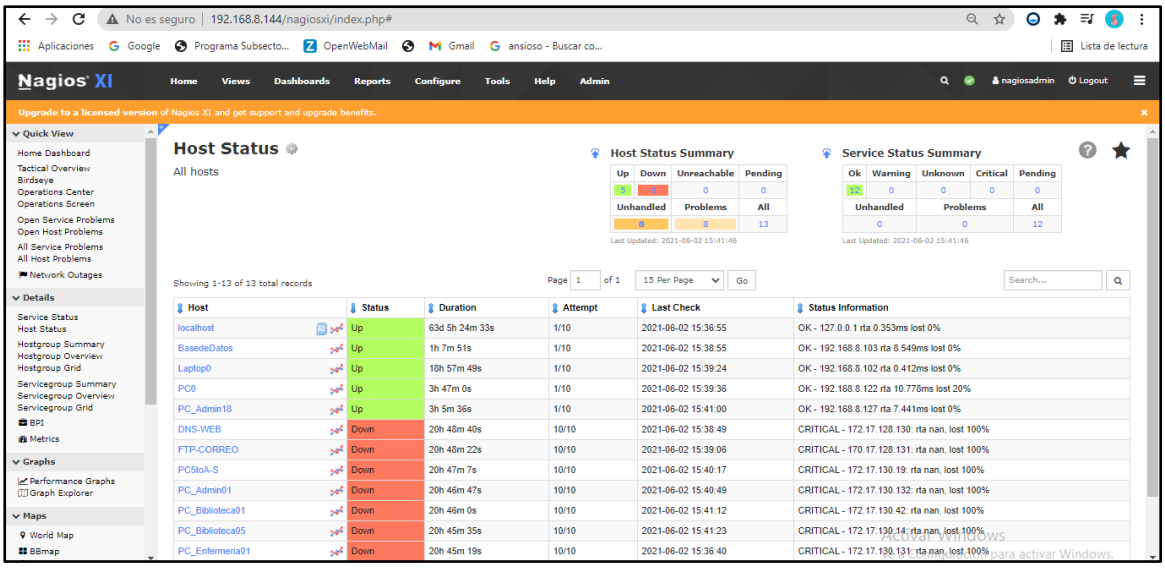
Tactical Overview



Ingresando a Host Status observamos una lista de los equipos de la red, su estado prendido (up)/ apagado (down), el último chequeo realizado, la duración que llevan prendidos y la información de su estado.

Figura 39

Host Status de la red



Ingresando a Service Status observamos una lista de los servicios de la red, que nos muestra el estado del servicio que están funcionando correctamente, su último chequeo y la duración del servicio.

Figura 40

Service Status de la red

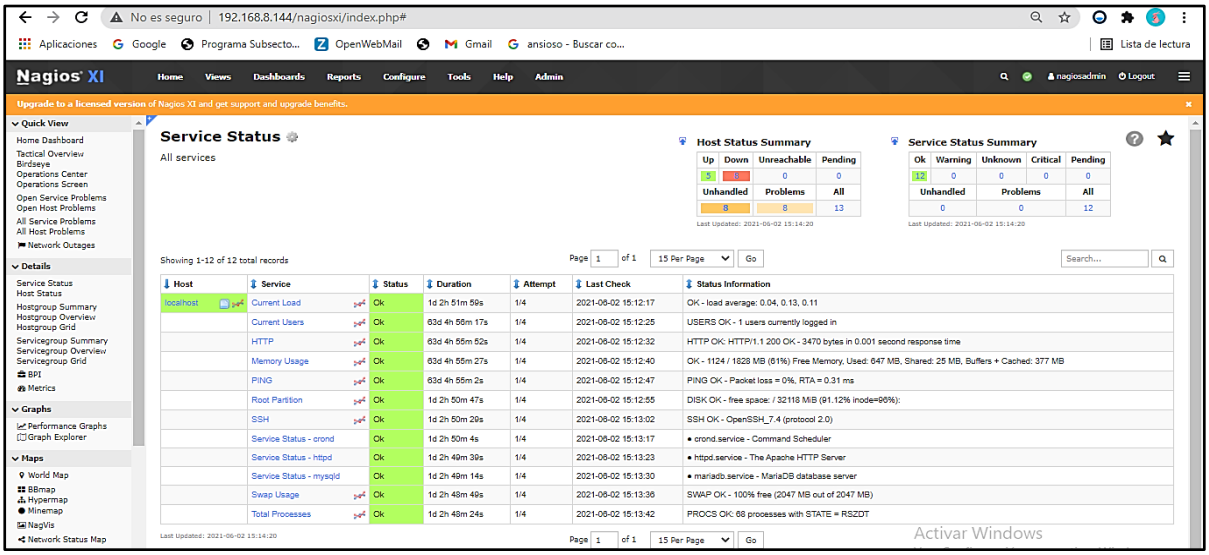
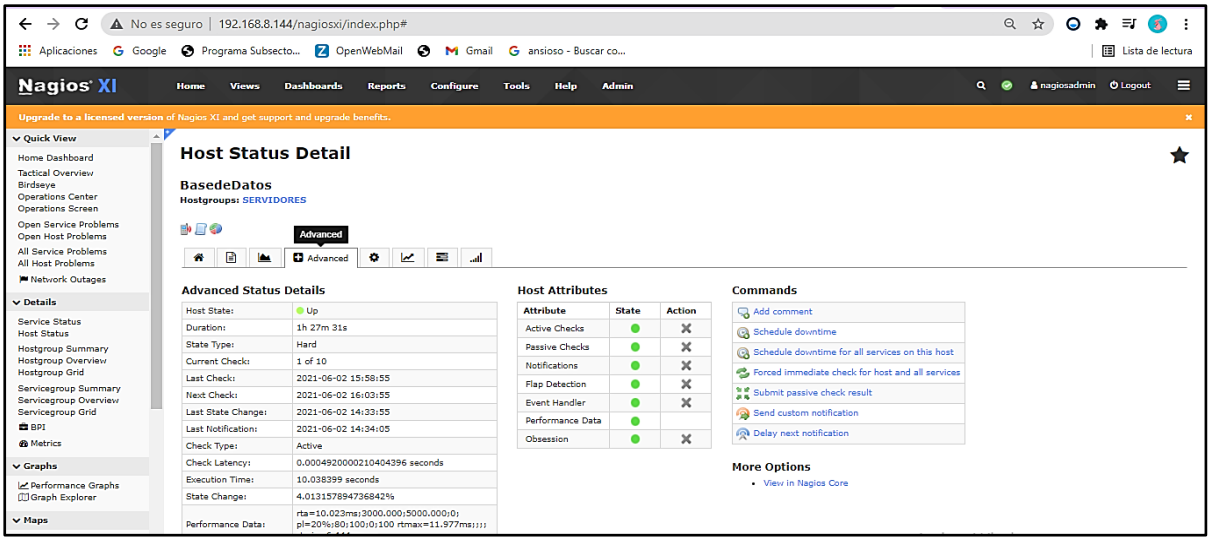


Figura 41

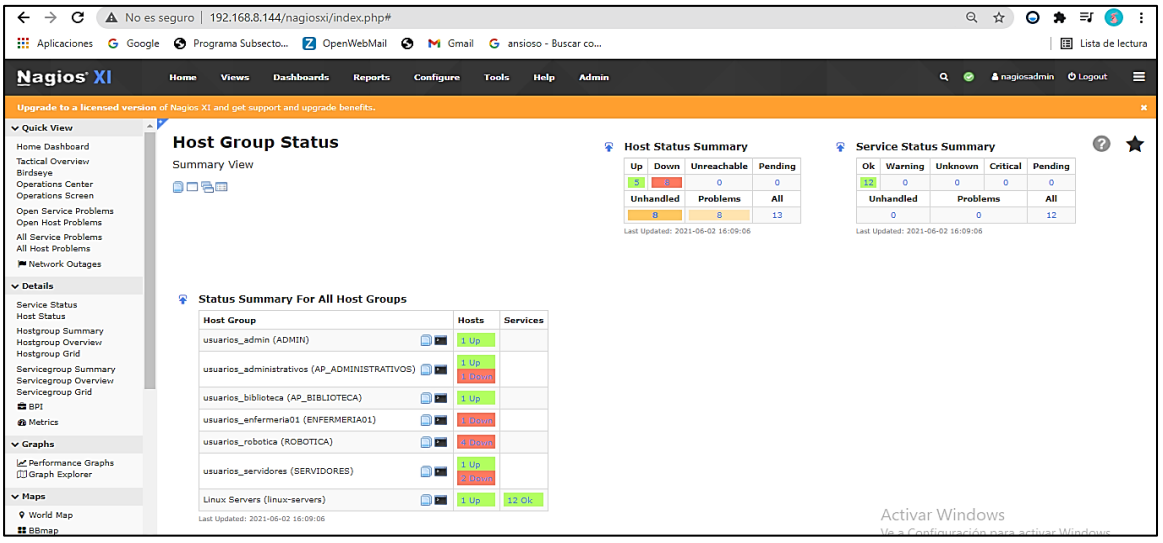
Información del equipo base de datos de la red



En Host Group Status mostramos los grupos creados para organizar los dispositivos que intervienen en la red del colegio Santa Maria Reina.

Figura 42

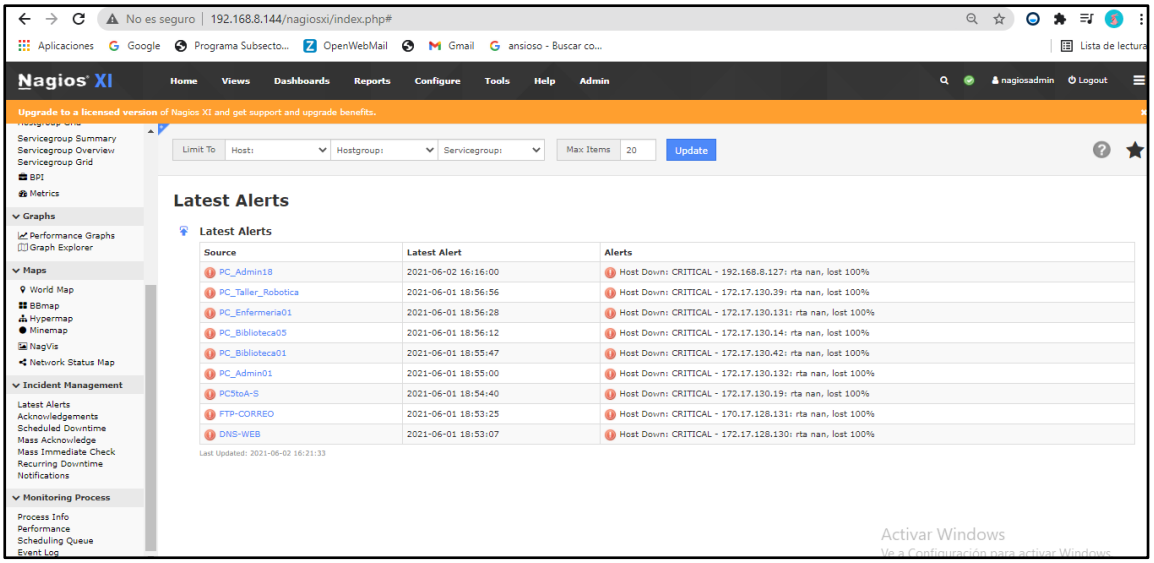
Grupos de host organizados



Finalmente, en latest alterts, podemos observar los host y servicios del colegio Santa Maria Reina que han tenido caídas durante el monitoreo de red.

Figura 43

Grupos de host organizados



Para el testeo realizado a la red encontrada en el colegio Santa Maia Reina se utilizó el programa Packet Tracer, para el testeo de la red propuesta se utilizó la herramienta Nagios.

A continuación, se muestran los testeos realizados:

<u>TESTEO DE LA RED ACTUAL</u>

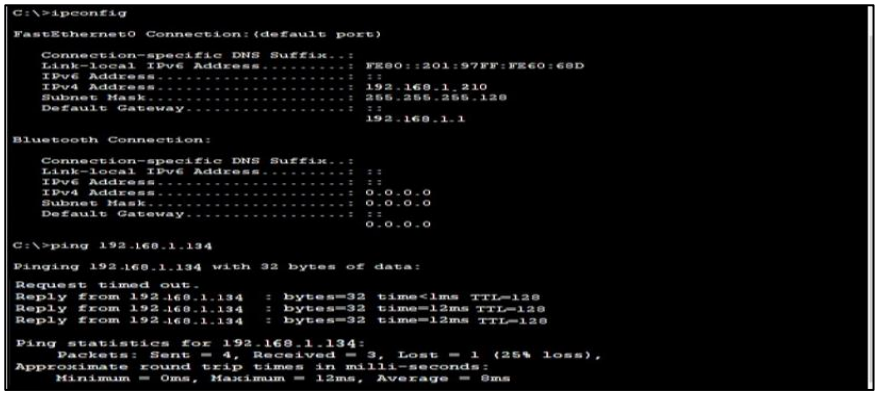
Comunicación entre:

PC_Biblioteca IP: 192.168.1.210

PC1 IP: 192.168.1.134

Figura 44

Testeo de la red actual – PC_Biblioteca



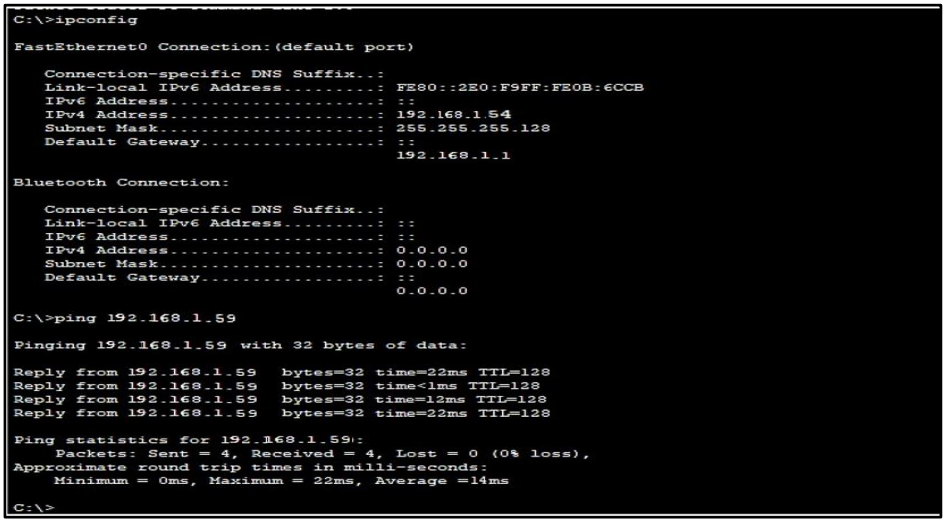
Comunicación entre:

PC_Psicologia IP: 192.168.1.54

PC4 IP: 192.168.1.59

Figura 45

Testeo de la red actual - Psicología



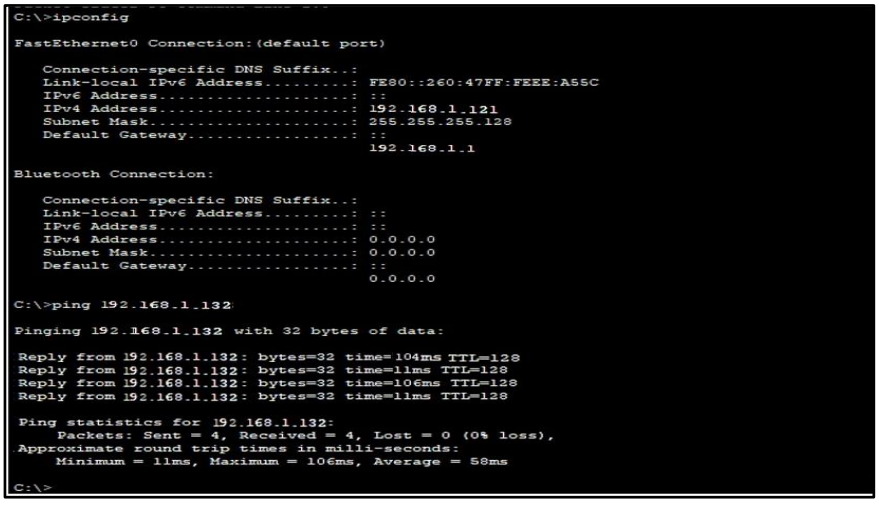
Comunicación entre:

PC_Tesoreria IP: 192.168.1.121

PC_Coordinacion IP: 192.168.1.132

Figura 46

Testeo de la red actual – Tesorería



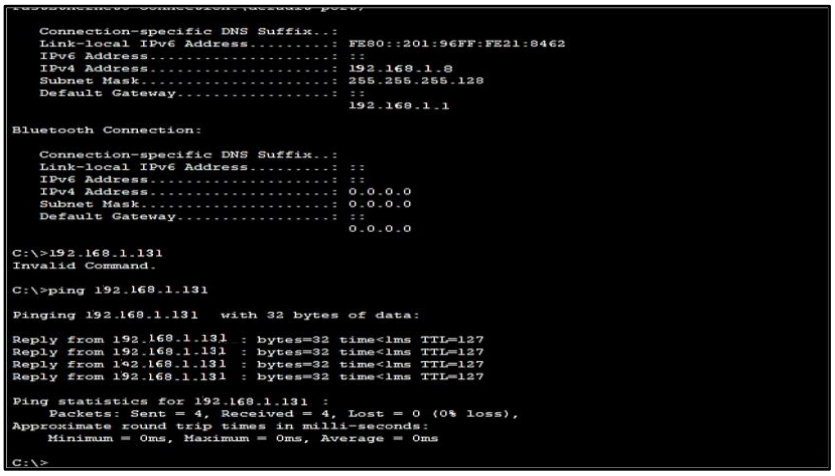
Comunicación entre:

PC2 IP: 192.168.1.8

PC1 IP: 192.168.1.131

Figura 47

Testeo de la red actual – PC2



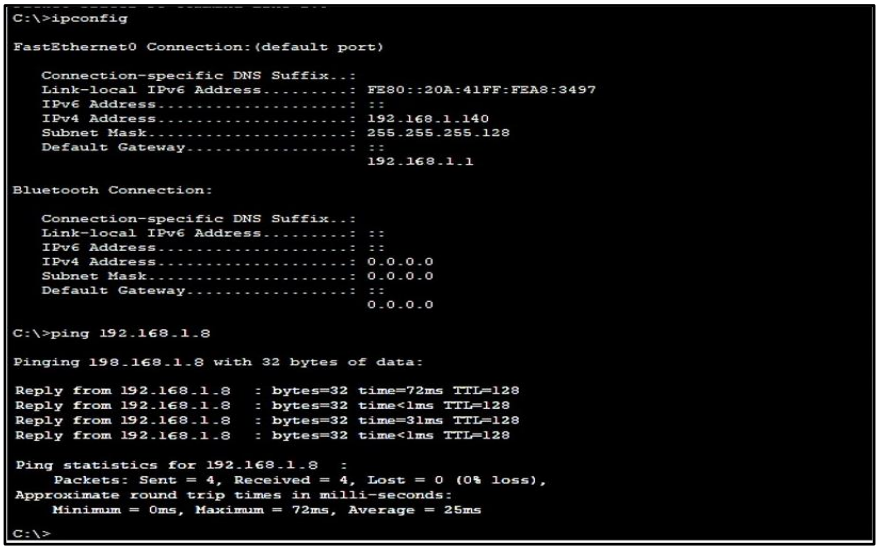
Comunicación entre:

PC3 IP: 192.168.1.140

PC2 IP: 192.168.1.8

Figura 48

Testeo de la red actual – PC3



TESTEO DE LA RED PROPUESTA

A continuación, se muestra el testeo realizado a la red propuesta del Colegio Santa Maria Reina, mediante el uso de Packet Tracer.

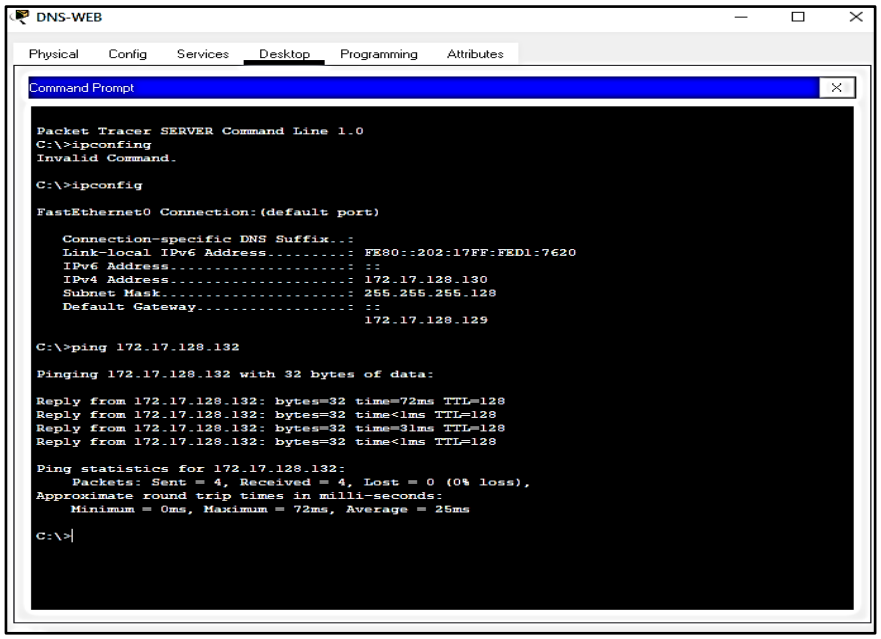
Comunicación entre el servidor web y el servidor de base de datos.

Server – PT DNS WEB IP: 172.17.128.130

Server – PT Base de Datos IP: 172.17.128.132

Figura 49

Testeo de la red propuesta – DNS-WEB



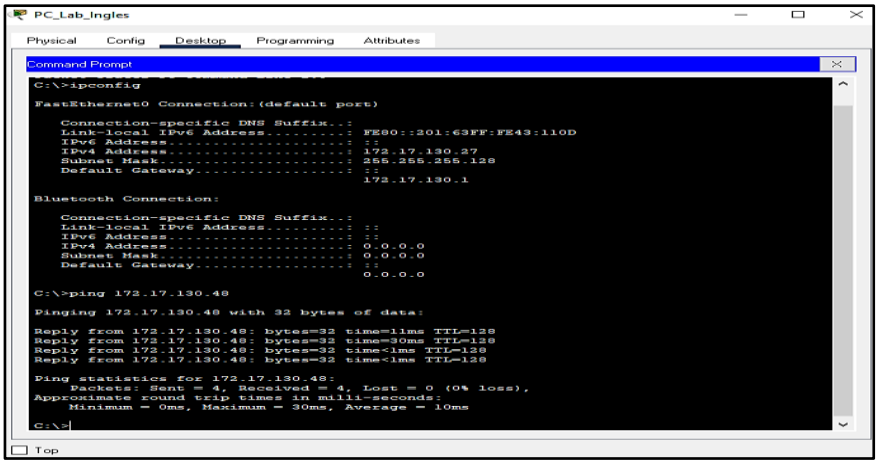
Comunicación entre PC_Lab_Ingles con PC_Salon_Musica

PC – PT PC_Lab_Ingles IP: 172.17.130.27

PC – PT PC_Salon_Musica IP: 172.17.130.48

Figura 50

Testeo de la red propuesta – PC_Lab_Ingles



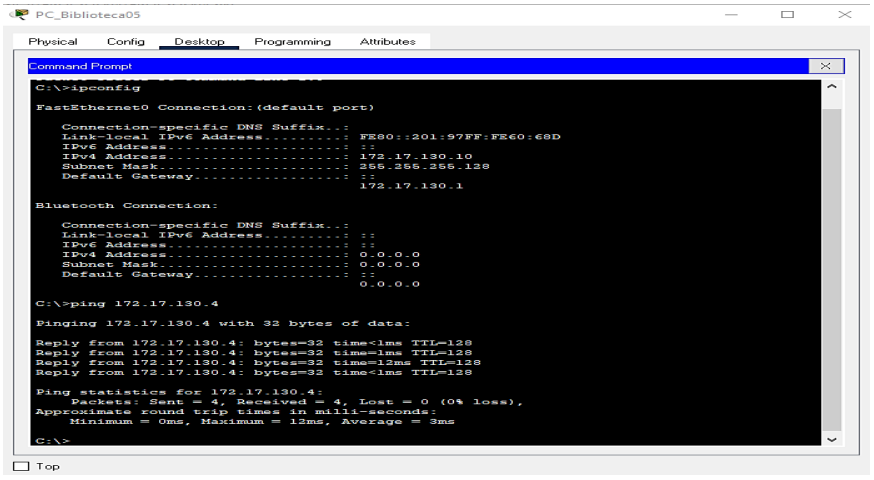
Comunicación entre PC Biblioteca05 y PC 5to.

PC – PT PC Biblioteca05 IP: 172.17.130.10

PC – PT PC5to C-S IP: 172.17.130.4

Figura 51

Testeo de la red propuesta – PC_Biblioteca05



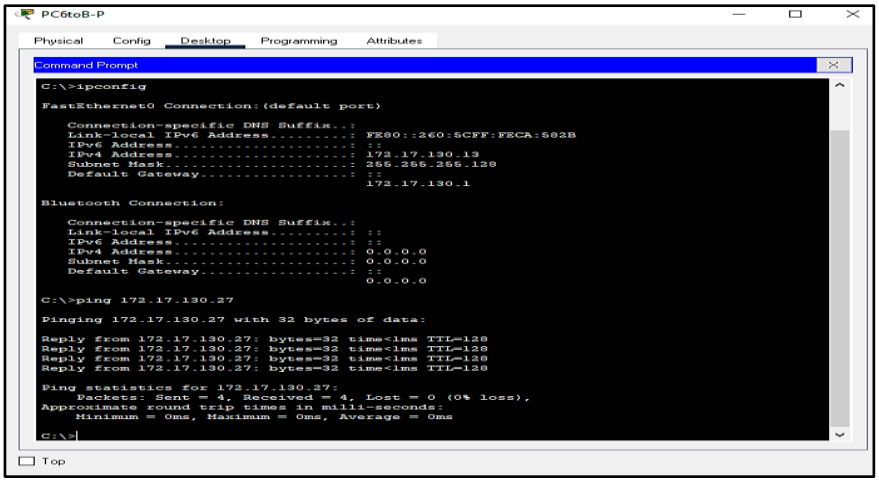
Comunicación entre PC 6toB – P con PC_Lab_Ingles

PC – PT PC 6toB - P IP: 172.17.130.13

PC – PT PC_Lab_Ingles IP: 172.17.130.27

Figura 52

Testeo de la red propuesta – PC 6toB – P



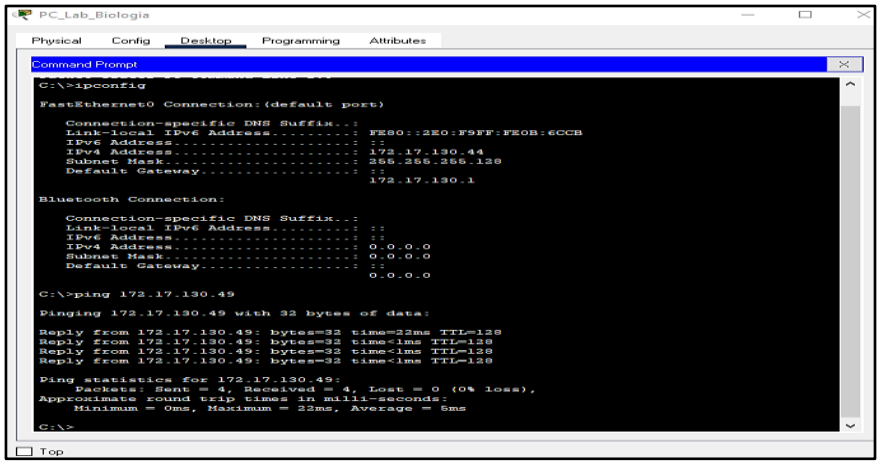
Comunicación entre PC_Lab_Biologia y PC4to A-P

PC – PT PC_Lab_Biologia IP: 172.17.130.44

PC – PT PC4to A-P IP: 172.17.130.49

Figura 53

Testeo de la red propuesta – PC_Lab_Biologia



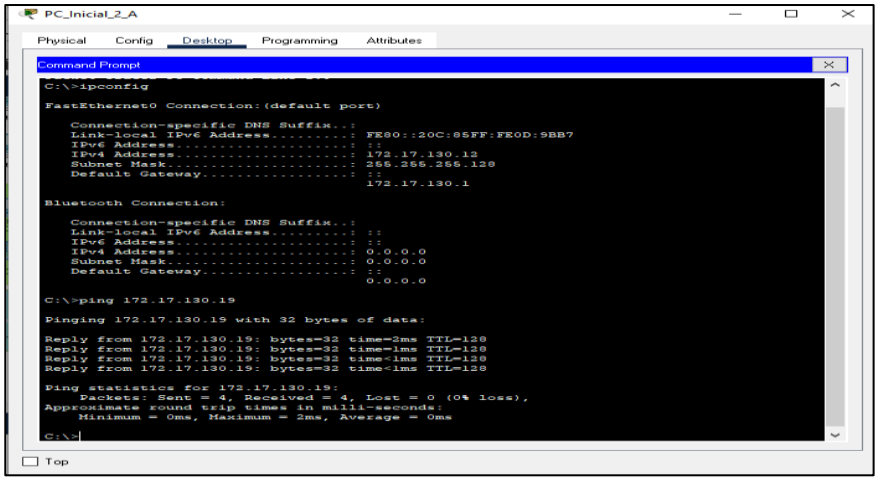
Comunicación entre PC_Inicial_2_A con PC_Inicial_5_B

PC – PT PC_Inicial_2_A IP: 172.17.130.12

PC – PT PC_Inicial_5_B IP: 172.17.130.19

Figura 54

Testeo de la red propuesta – PC_Inicial_2_A



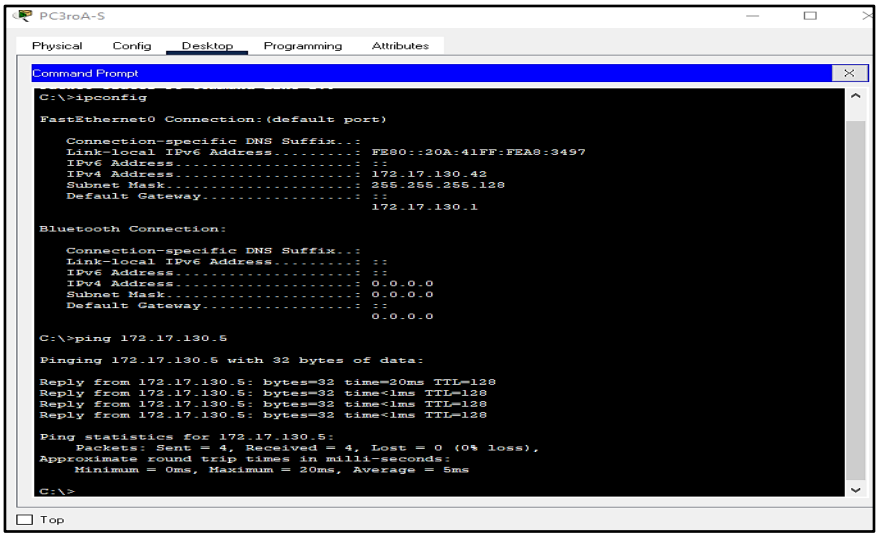
Comunicación entre PC3ro A - S y PC2do A - S

PC – PT PC3ro A - S IP: 172.17.130.42

PC – PT PC2do A - S IP: 172.17.130.5

Figura 55

Testeo de la red propuesta – PC3ro A - S



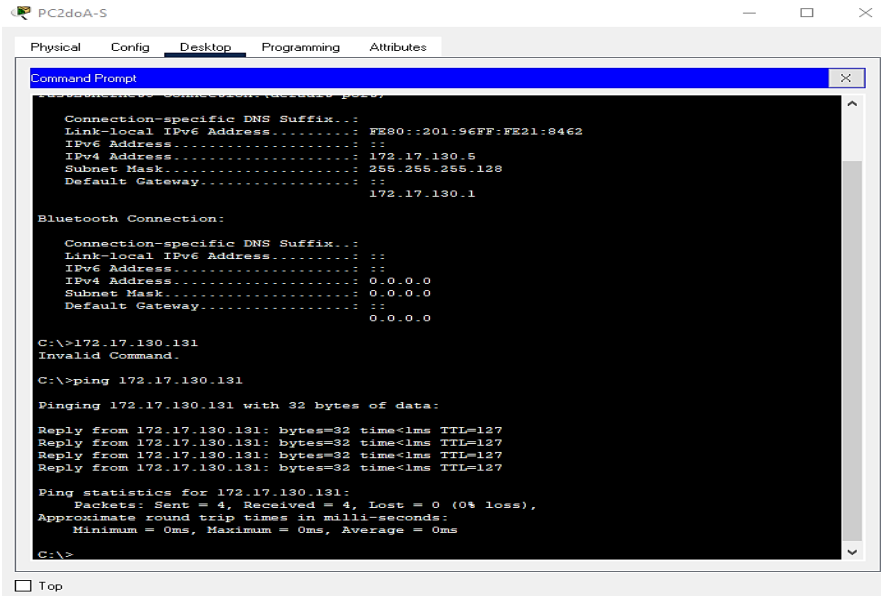
Comunicación entre PC2do A – S con PC_Enfermeria01

PC – PT PC2do A - S IP: 172.17.130.5

PC – PT PC_Enfermeria01 IP: 172.17.130.131

Figura 56

Testeo de la red propuesta – PC2do A – S



Comunicación entre PCLAb50_S con PCLab01_S

PC – PT PCLab50_S IP: 172.17.129.131

PC – PT PCLab01_S IP: 172.17.129.132

Figura 57

Testeo de la red propuesta – PCLAb50_S

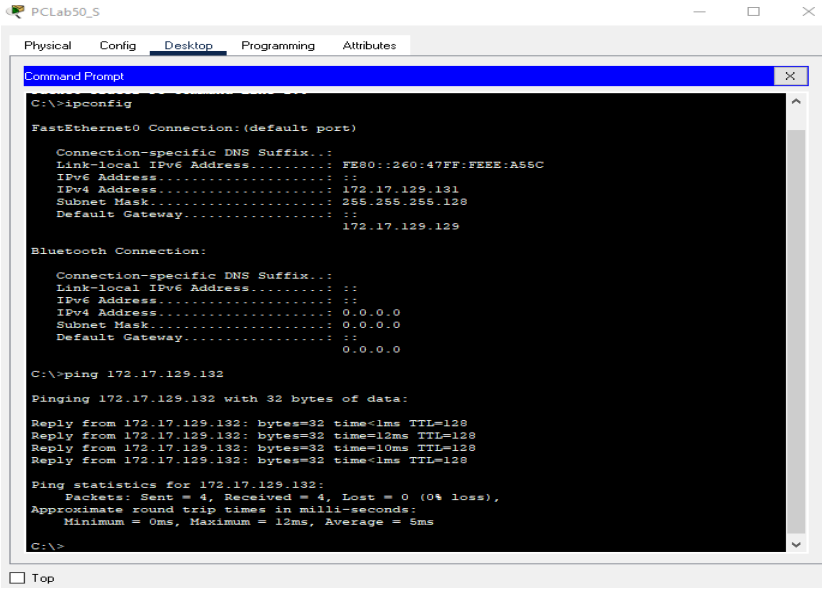


Tabla 34.

Rendimiento de la red actual.

RED ACTUAL							
N°	EQUIPO EMISOR	EQUIPO RECEPTOR	PAQUETES			TIME	
			send	received	lost	max	min
1	PC_Biblioteca IP: 192.168.1.210	PC1 IP: 192.168.1.134	3	3	1	12ms	0ms
2	PC_Psicologia IP: 192.168.1.54	PC4 IP: 192.168.1.59	4	4	0	22ms	0ms
3	PC_Tesoreria IP: 192.168.1.121	PC_Coordinacion IP: 192.168.1.132	4	4	0	106ms	11ms
4	PC2 IP: 192.168.1.8	PC1 IP: 192.168.1.131	4	4	0	0ms	0ms
5	PC3 IP: 192.168.1.140	PC2 IP: 192.168.1.8	4	4	0	72ms	0ms
6	PC4 IP: 192.168.1.59	PC1 [Inicial] IP: 192.168.1.134	4	4	0	106ms	11ms
7	PC5 IP: 192.168.1.13	PC2 IP: 192.168.1.12	4	4	0	254ms	8ms
8	PC6 IP: 192.168.1.36	PC7 IP: 192.168.1.18	4	3	1	12ms	0ms
9	PC7 IP: 192.168.1.18	PC2[Biblioteca] IP: 192.168.1.132	4	4	1	254ms	8ms
10	PC3 IP: 192.168.1.17	PC2[Biblioteca] IP: 192.168.1.131	4	4	0	231ms	11ms

Fuente: Elaboración propia

Tabla 35.

Rendimiento de la red propuesta

RED PROPUESTA						
EQUIPO EMISOR	EQUIPO RECEPTOR	PAQUETES			TIME	
		send	received	lost	max	min
Server – PT DNS WEB IP: 172.17.128.130	Swerver – PT Base de Datos Ip: 172.17.128.132	4	4	0	72ms	0ms
PC – PT PC_Lab_Ingles IP: 172.17.130.27	PC – PT PC_Salon_Musica IP: 172.17.130.48	4	4	0	30ms	0ms
PC – PT PC Biblioteca05 IP: 172.17.130.10	PC – PT PC5to C-S IP: 172.17.130.4	4	4	0	12ms	0ms
PC – PT PC 6toB - P IP: 172.17.130.13	PC – PT PC_Lab_Ingles IP: 172.17.130.27	4	4	0	0ms	0ms
PC – PT PC_Lab_Biologia IP: 172.17.130.44	PC – PT PC4to A-P IP: 172.17.130.49	4	4	0	22ms	0ms
PC – PT PC_Inicial_2_A IP: 172.17.130.12	PC – PT PC_Inicial_5_B IP: 172.17.130.19	4	4	0	2ms	0ms
PC – PT PC3ro A - S IP: 172.17.130.42	PC – PT PC2do A - S IP: 172.17.130.5	4	4	0	20ms	0ms
PC – PT PC2do A - S IP: 172.17.130.5	PC – PT PC_Enfermeria01 IP: 172.17.130.131	4	4	0	0ms	0ms
PC – PT PCLab50_S IP: 172.17.129.131	PC – PT PCLab01_S IP: 172.17.129.132	4	4	0	12ms	0ms
PC – PT PC5toD – P IP: 172.17.130.47	PC – PT PCLab01_S IP: 172.17.129.132	4	4	0	26ms	12ms

Fuente: Elaboración propia

Para revisar la seguridad de la red en el colegio Santa Maria Reina, se plantea el uso de las siguientes herramientas de seguridad (Ver Tabla 36):

Tabla 36.

Herramientas de seguridad

Herramientas de seguridad	
Analizadores de red	**Descripción**
NetTraffic	Se propone el uso de NetTraffic por ser una herramienta gratuita y porque nos permite conocer el tráfico de Internet de los equipos o las conexiones que soporta la red del Colegio Santa Maria Reina, nos ayuda a descubrir si algún intruso se encuentra robando la señal del colegio, pudiendo analizar todos los detalles de los dispositivos conectado a la red del colegio.
Analizadores de seguridad	**Descripción**
OpenVas	Es una herramienta gratuita, y su implementación nos ayudará a detectar errores de configuración, problemas de seguridad, análisis de servidores, de los puertos abiertos y demás vulnerabilidades a las que están expuestas las computadoras del Colegio Santa Maria Reina. También de ser una herramienta compatible con SO Windows y Linux.
Analizadores de paquetes	**Descripción**
Wireshark	Se propone el uso de la herramienta Wireshark en el Colegio Santa Maria Reina, ya que es una herramienta multiplataforma, gratuita y de código abierto. La cual nos permitirá capturar y analizar al detalle todo el tráfico de los paquetes de red que entra y sale de los ordenadores de los laboratorios, administrativos y de las alumnas. De esta manera nos ayudará a verificar que no se acceda a páginas no autorizadas o el uso incorrecto del internet o red.

Fuente: Elaboración Propia

3.4.2. Parte 16: Optimización

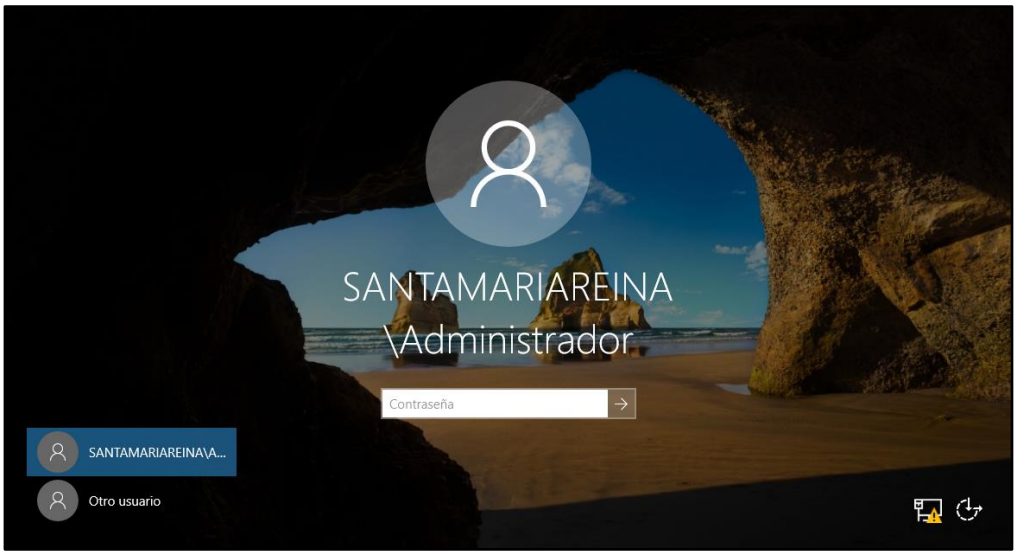
Para mejorar el rendimiento de la red, se procedió a implementar las políticas de seguridad propuestas, y de esta manera optimizar los servicios que brinda el colegio.

A continuación, se muestra el resultado de las políticas implementadas en el colegio Santa Maria Reina.

1. Se pondrá contraseñas a las computadoras para evitar el fácil ingreso a personas no autorizadas, garantizando la disponibilidad e integridad del servicio.
2. Se le otorgará al personal una cuenta con usuario y contraseña, para que accedan a la información que necesiten dentro de la red.

Figura 58

Inicio de sesión en pc administrativas



3. Se bloqueará el acceso a la ejecución de software a personas no autorizadas.

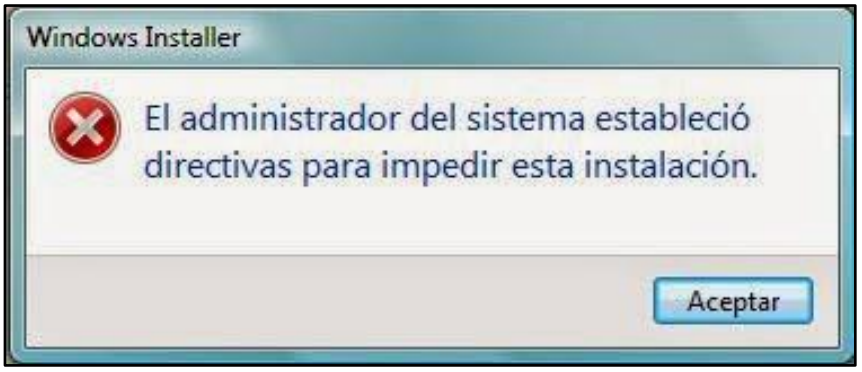
Figura 59

Bloqueo de ejecución de software

4. No se debe permitir que ningún usuario instale equipos de fuera de la institución a la red de datos de la misma.

Figura 60

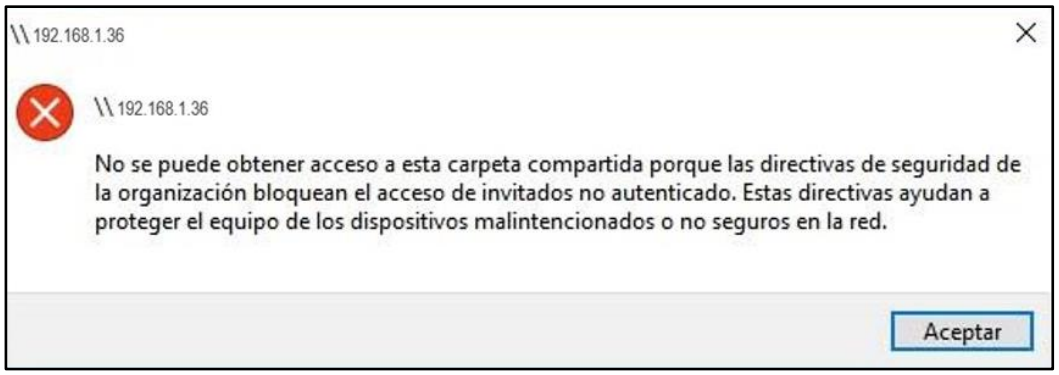
Impedir la instalación de cualquier software



5. Si el usuario no está autorizado, no podrá acceder a los recursos de la red.
6. Denegar que la red de aulas y laboratorios acceda a la red de administrativos.

Figura 61

Acceso no permitido a otra red



7. Se restringe el acceso a internet para evitar las descargas sin control
8. Denegar el tráfico de redes sociales en todas las redes comprendido entre las 8:00am hasta las 4:00pm.

Figura 62

Sitio web restringido

3.4.3. Parte 17: Documentación de la red

Se documentaron los registros de hardware usados en la red.

Tabla 37.

Herramientas de seguridad

Nombre_PC	Dirección IP	Máscara subred	Gateway Predeterminado
Server – PT DNS WEB	172.17.128.130	255.255.255.128	172.17.128.129
Server - PT FPT CORREO	172.17.128.131	255.255.255.128	172.17.128.129
Server – PT Base de Datos	172.17.128.132	255.255.255.128	172.17.128.129
PC – PT PC5to A-S	172.17.130.19	255.255.255.128	172.17.130.1
PC – PT PC5to C-S	172.17.130.4	255.255.255.128	172.17.130.1
PC_Biblioteca05	172.17.130.14	255.255.255.128	172.17.130.1
PC – PT PC4to A-S	172.17.130.16	255.255.255.128	172.17.130.1
PC_Biblioteca01	172.17.130.42	255.255.255.128	172.17.130.1
PC_4toD-S	172.17.130.30	255.255.255.128	172.17.130.1
PC_Taller_Robotica	172.17.130.39	255.255.255.128	172.17.130.1
PC_Taller_Ballet	172.17.130.20	255.255.255.128	172.17.130.1
PC0	172.17.130.130	255.255.255.128	172.17.130.129
PC – PT PC4to A-P	172.17.130.49	255.255.255.128	172.17.130.1
PC – PT PC4to D-P	172.17.130.21	255.255.255.128	172.17.130.1
PC – PT PC3ro A - P	172.17.130.12	255.255.255.128	172.17.130.1
PC – PT PC3ro D - P	172.17.130.46	255.255.255.128	172.17.130.1
PC_Lab_Biologia	172.17.130.22	255.255.255.128	172.17.130.1
PC_Enfermeria01	172.17.130.131	255.255.255.128	172.17.130.129
PC – PT PC3ro A - S	172.17.130.42	255.255.255.128	172.17.130.1
PC – PT PC2do A - S	172.17.130.28	255.255.255.128	172.17.130.1
PC – PT PC3ro D - S	172.17.130.11	255.255.255.128	172.17.130.1
PC – PT PC2do D - S	172.17.130.46	255.255.255.128	172.17.130.1
PCLab01_S	172.17.129.134	255.255.255.128	172.17.129.129
PCLab48_S	172.17.129.135	255.255.255.128	172.17.129.129
PCLab49_S	172.17.129.132	255.255.255.128	172.17.129.129
PCLab50_S	172.17.129.133	255.255.255.128	172.17.129.129
PC5toD-P	172.17.130.48	255.255.255.128	172.17.130.1
PC5toC-P	172.17.130.32	255.255.255.128	172.17.130.1
PC_Admin01	172.17.130.132	255.255.255.128	172.17.130.129
PC_Admin18	172.17.130.149	255.255.255.128	172.17.130.129
PC_Autorio02	172.17.130.5	255.255.255.128	172.17.130.1
PC_Autorio01	172.17.130.18	255.255.255.128	172.17.130.1
PC-Lab01	172.17.129.2	255.255.255.128	172.17.129.1
PC-Lab015	172.17.129.3	255.255.255.128	172.17.129.1
PC_Enfermeria02	172.17.130.150	255.255.255.128	172.17.130.129
PC_Ajedrez	172.17.130.27	255.255.255.128	172.17.130.1
PC1eroA-P	172.17.130.34	255.255.255.128	172.17.130.1
PC2doA-P	172.17.130.23	255.255.255.128	172.17.130.1
PC1roD-P	172.17.130.9	255.255.255.128	172.17.130.1
PC2doD-P	172.17.130.26	255.255.255.128	172.17.130.1

Fuente: Elaboración Propia

3.4.3.1. Plan de implementación de la red informática.

3.4.3.1.1. Directivas para instalación y configuración de AD.

- Tipo de controlador de dominio: dominio nuevo.
- Tipo de dominio a crear: dominio en un nuevo bosque.
- Nombre DNS para el nuevo dominio: santamariareina.edu.pe
- Nombre NetBios: santamariareina
- Tipos de permisos para usuarios y objetos: compatible con Windows Server 2016.
- Se establece contraseña de Administrador de manera remota.

3.4.3.1.2. Directivas para instalación y configuración de DNS.

- Nombre del DNS: santamariareina.edu.pe
- Zona de búsqueda: inversa o directa.
- IP del Servidor DNS: 192.168.1.3
- Tipo de Servidor: Primario.
- Integrado al AD: Si.

3.4.3.1.3. Directivas para las políticas de seguridad en el dominio.

En la arquitectura de red, las políticas de grupo se pueden aplicar en varios niveles equipo local, sitio, dominio y unidad organizativa. Nuestra propuesta estará orientada aplicar a nivel de dominio ya que se espera aplicar las directivas a todos los equipos y/o usuarios del dominio santamariareina.edu.pe

Entre las políticas de seguridad, se debe agregar:

- **Directiva de bloqueo de cuentas de usuario.**

Tabla 38.

Directivas de bloqueo de cuentas de usuario.

DIRECTIVA	CONFIGURACIÓN
Bloqueo de cuenta, duración	15 minutos
Cuenta de usuario, restablecimiento	15 minutos
Intentos de bloqueo de cuenta	3 intentos

Fuente: Elaboración Propia

- **Directivas de contraseñas.**

Tabla 39.

Directivas de contraseña

DIRECTIVA	CONFIGURACIÓN
Requisito de complejidad	Si
Longitud mínima	8 caracteres
Vigencia máxima	90 días
Vigencia mínima	3 días

Fuente: Elaboración Propia

- **Directivas de grupos de usuarios.**

Tabla 40.

Directivas de grupos de usuario.

DIRECTIVA	CONFIGURACIÓN
Restringir el acceso al panel de control y Configuración	SI
Bloquear acceso al símbolo del sistema	SI
Impedir la instalación de software	SI
Desactivar las actualizaciones automáticas de controladores.	SI

Fuente: Elaboración Propia

3.4.3.1.4. Directivas de auditoría.

Tabla 41.

Directivas de auditoria

DIRECTIVA	FRECUENCIA	CONFIGURACIÓN
AUDITAR EL ACCESO A OBJETOS: Esta auditoria nos brinda un reporte sobre el uso que se está haciendo de los recursos del colegio Santa Maria Reina, es decir, obtenemos información De los intentos de los usuarios para acceder a archivos no asociados a su área o labor, impresoras, computadoras, el borrado o modificado de ficheros y los problemas de seguridad que deben ser reforzados.	Mensual	Erróneo
AUDITAR EL CAMBIO DE DIRECTIVAS: Esta auditoría nos permite hacer un seguimiento de las políticas de seguridad críticas en el sistema o la red local del colegio Santa Maria Reina. Ya que la supervisión de las modificaciones o los esfuerzos por modificar las políticas, que suelen establecer directivas para ayudar a proteger los recursos de la red, puede ser un componente esencial de la gestión de la seguridad de una red de colegio.	Mensual	Correcto, erróneo
AUDITAR EL USO DE PRIVILEGIOS: Al realizar esta auditoría, se tiene un reporte de los permisos concedidos en la red del colegio Santa Maria Reina con el fin de permitir que el personal o los alumnos completen solo tareas específicas.	Quincenal	Erróneo
AUDITAR EL INICIO DE CUENTA DE SESIÓN:		

Los intentos de autentificar los datos de la cuenta desde el controlador de dominio o el administrador de cuentas de seguridad (SAM) local del Colegio Santa María Reina pueden ser documentados utilizando esta auditoría, del mismo modo se puede identificar cada vez que un usuario del colegio Santa Maria Reina inicia o cierra una sesión desde otro equipo. **AUDITAR EVENTOS DE SISTEMA:** El auditar eventos del sistema nos permite hacer un seguimiento a eventos de errores, reinicio o cierre de un equipo realizado por un usuario del colegio Santa Maria Reina y podemos determinar sucesos que afecten a la seguridad del sistema del colegio.	Mensual Mensual	Erróneo Erróneo

Fuente: Elaboración Propia

3.4.3.1.5. Directivas para instalación y configuración DHCP.

La configuración del DHCP se realizará a través del switch core de la red del colegio Santa María Reina.

3.4.3.1.6. Directivas de instalación y configuración de servicio de correo.

Para el uso del correo usaremos POP3.

SERVIDOR:

- Nombre del servidor: Server_Correo_FTP
- Tipo de Servidor: integrado a Active Directory.
- Dominio de trabajo con POP3: server2.santamariareina.edu.pe

CLIENTES:

- Usuario: administrador
- Correo electrónico: administrador@server2.santamariareina.edu.pe

- Servidor entrante: servidor2
- Servidor saliente: servidor2

SERVIDOR WEB

Al usar como sistema operativo Windows Server 2016, por lo tanto, usaremos el servicio IIS (Internet Information Server) para nuestro servidor Web:

- Sitio web: santamariareina.edu.pe
- Dirección IP: 192.168.1.3
- Puerto a usar: 80
- Directorio del sitio web: C:\Inetpub\wwwrot\Santamariareina
- Acceso: leer.

3.4.3.1.7. Directivas para la instalación y configuración del firewall.

En esta ocasión usaremos como firewall a nuestro router cisco, el cual se configurarán listas de control de acceso para permitir o denegar entradas o salidas.

3.4.3.1.8. Directivas para la instalación y configuración de servicios de FTP.

Servidor que tendrá la función para compartir documentos, archivos y datos a nivel de red. Por lo tanto, se aplicará algunas políticas:

- Cantidad de espacio por usuario: 3 GB.
- Cantidad de espacio para el sistema operativo: 80 GB.
- Cantidad de espacio para aplicaciones: 100 GB.

CAPÍTULO IV

4. DISCUSIÓN

Para el diseño y arquitectura de gestión y seguridad propuesta en esta investigación se han tomado un análisis de los objetivos y limitaciones de la institución educativa donde facilite a sus colaboradores y estudiantes tener una tecnología colaborativa y efectiva.

Rendimiento

Según Aguado (2018, p. 834), indica que toda red es medible, debido a que la velocidad de transferencia es la que permite determinar si este está funcionando o no de manera óptima, sin embargo, las interferencias que pueden impedir el correcto funcionamiento de esta red son, la poca cobertura que pueda tener esa zona. Por otro lado, en el artículo científico de Franciosi y Vidarte (2021), quienes indicaron que su propuesta de implementación de red informática tuvo un tiempo de respuesta menor, debido a que el tiempo que llega un nodo a otro es 10% más rápido de lo inicial. A su vez, se asemeja en los resultados del artículo científico de Zapata y Grisales (2020) quienes lograron determinar que el rendimiento de la red propuesta aumentó en un 8.7% en el tiempo de velocidad de un nodo a otro, trayendo grandes beneficios a los usuarios finales. En la presente investigación, la arquitectura de red que se propone es que exista un tiempo de repuesta menor y que llegue correctamente de un nodo de la red a otro, por consiguiente con la ayuda del indicador de rendimiento de ping en la red propuesta se obtiene una reducción considerable por muy debajo de los 2 ms el cual evita la perdida de paquetes de datos y la variación del tiempo de llegada causadas por la congestión de la red, finalmente se demostró que la red propuesta es 10% más rápida que la inicial.

Escalabilidad

Alea (2018, p. 25) indica que una red es escalable si esta permite soportar el número de usuarios que aumente en un futuro, asimismo, la red debe ser tolerante a fallas por lo que el autor propone equipos routers o Switches multicapas para limitar las transmisiones y crear una estrategia de direcciones IPv4 el autor propone un estilo jerárquico. Por otro lado, en el artículo de científico de Céspedes y Martínez (2020) quienes lograron determinar que después de aplicar la gestión y seguridad en una institución educativa, donde la escalabilidad era para un total 100 alumnos, pero se pudo expandir a un total de 180 alumnos, teniendo de esa manera una ampliación alta para todos alumnos que pudieron ingresar en dicha institución. En la arquitectura de red que se propone existe una mejora ya que al inicio se tenía un número de usuarios entre administrativos y alumnado un total de 12 usuarios conectados a la red, pero con nuestra propuesta de red se obtiene un total de 161 usuarios conectados a la red ofreciendo dispositivos de distribución escalables es decir permitirá incrementar la cantidad de puertos, esto permitirá soportar futuros aumentos.

Disponibilidad

Ortega (2017, p. 23) menciona que cuando el hardware, las aplicaciones y/o los sistemas operativos fallen, los usuarios podrán seguir accediendo a las aplicaciones y/o servicios, usando enlaces redundantes de esta forma no habrá variaciones en la productividad de la empresa. Por otro lado, Flores (2018) en su artículo científico demuestra que, tras la realización de la prueba a personas de las 3 unidades de la DTI, se estimó que el primer porcentaje de cumplimiento de los 11 dominios de seguridad de la norma ISO 27002 fue del 52%, siendo este valor de cumplimiento “bajo”, dado que la norma está destinada a cualquier tipo de organización privada o pública, grande, mediana o pequeña. En nuestra propuesta de red al utilizar enlaces redundantes proporciona protección contra el tiempo de inactividad de la red, logrando una tasa de disponibilidad alta (TD = 99.90%) esto significa que la red de datos funcionará correctamente. Asimismo, nuestros dispositivos tecnológicos estarán a disposición de los usuarios si ocurre un corte de fluido eléctrico o fallas, implementaremos varios caminos ya que, si una ruta falla, tengamos más rutas alternativas y el mensaje siempre llegue a su destinatario las 24 horas del día.

Performance

En las teorías de Atienza (2018) donde se indica que la colocación de UPS's en la empresa para asegurar los discos de los servidores como plan de contingencia ante posibles fallos de red o eléctricos. A su vez se asemeja en los resultados de Franciosi y Vidarte (2021), quienes pudieron determinar que mediante el uso de una metodología sistemática de riesgos informáticos como Magerit, fue posible clasificar la información y determinar el nivel de riesgo de cada uno de ellos, identificando así los activos más críticos que requieren mayor atención y controles de seguridad por el alto impacto que tienen en la prestación de servicios y el óptimo funcionamiento de los procesos de la institución

Traducción realizada con la versión gratuita del traductor www.DeepL.com/Translator. En la presente investigación se logró mejorar la performance de la red informática puesto que se está ofreciendo una arquitectura de red que soportará fallas; como son las sobrecargas de voltajes que pueden originarse, así como también de una serie de técnicas y estudios, mediante mediciones de tráfico y un minucioso análisis del comportamiento de la red, para ello proponemos un plan en cuanto a posibles caídas de la red que irían desde instalar UPS´s para el problema de voltaje hasta poder realizar una serie monitoreo y análisis de comportamiento de la red mediante la plataforma nagios donde el personal encargado podrá documentar futuras caídas o vulnerabilidades, de esta forma cumplimos con lo propuesto.

Seguridad

Según lo señalado en las teorías de Álvarez y Enrico (2017, p. 34) donde asegura que implementar una red con VLAN'S permite desarrollar un alto nivel de seguridad ya que no permite que la información salga del mismo grupo del trabajo agregado a ello el investigador plantea políticas donde resalta el registro o destrucción no autorizados, modificación, uso, la protección de la información y los sistemas de información de un acceso. A su vez se asemeja en los resultados hallados por Flores (2018) quien halló que la implantación de un servidor radius con certificados digitales reducirá el peligro de robo de información y de asalto a la red, mejorando así la seguridad y el control de las redes inalámbricas de UNSM-T. En

nuestra red propuesta se logró mejorar la seguridad de la red informática principalmente porque se ha implementado una red con 7 VLAN'S distribuidas en todo el campus educativo permitiendo desarrollar un nivel de seguridad más alto garantizando el funcionamiento de todos los equipos de una manera segura. Por otro lado, los usuarios tendrán los permisos asignados y los equipos estarán conectados al servidor de antivirus donde ofrecerá un monitoreo y protección ante cualquier amenaza de la red, asimismo, se está adoptando un conjunto de normas de seguridad para notificar al personal técnico, administradores y usuarios de sus responsabilidades en la protección de los activos de información. Asimismo, si deseamos prevenir y proteger nuestra red privada de cualquier ataque de intrusos, bloqueando el acceso ofrecemos el firewall SolarWinds todo ellos a costos que puedan ser accesibles para la institución educativa.

Adaptabilidad

No cabe duda de que estas redes, que se expanden a un ritmo acelerado a lo largo del tiempo, son las que nos mantienen unidos, entre otras muchas cosas. Según Books (2017, p. 65) señala que si se forma un diseño de entorno de red estructurado, se adquieran software y hardware informáticos capaces de adaptarse a futuras ampliaciones de la red. A su vez se asemeja en los resultados de Pérez (2019) quien halló que, el Plan de Tratamiento de Riesgos redujo los niveles de riesgo en los activos de información de la institución, consideró las amenazas y las vulnerabilidades, en consecuencia, se desarrolló una estrategia eficaz de seguridad de la información para hacer frente a estas amenazas, con procesos preventivos y correctivos, así como las acciones esenciales para limitar los riesgos. En nuestra investigación se logró mejorar la adaptabilidad de la red informática según el testeo realizado en el software nagios en el Service Status observamos una lista de los servicios de la red, que nos muestra los equipos están funcionando correctamente, su último chequeo y la duración del servicio nos muestra que los dispositivos se encuentran 100% activos donde permite a los usuarios estar conectado en cualquier parte del colegio e incluso al personal administrativo poder realizar un trabajo remoto seguro. Asimismo, los equipos que proponemos son de la marca Cisco System, TP-Link, Lenovo que han demostrado ser marcas de innovación brindando un buen soporte y ventaja tecnológica de punta, a fin de obtener una mejor experiencia con el usuario.

5. CONCLUSIONES

1. Se analizó el estado actual del Colegio Santa María Reina, permitiendo identificar la problemática para proponer herramientas tecnológicas que cumplan con la red propuesta para el colegio, dando como resultado una tasa de disponibilidad en la red del 90% de equipos tecnológicos concluyendo que la red de datos funcionará correctamente.
2. La implementación de la metodología cisco (top-down network design) permitió lograr una arquitectura de red eficiente, superando el reto de la seguridad de la información y la velocidad de transferencia entre sus distintas áreas, servicios y aulas.
3. Se diseñó una topología de red jerárquica en tres capas con la finalidad de dar solución en mejorar el rendimiento de la red del Colegio Santa María Reina, cuyo estudio y de acuerdo a las necesidades se realizó una segmentación adecuada para el diseño. Asimismo, se planteó la solución con el apoyo del software Packet Trasert pudiendo distribuir las diferentes áreas y nivel de educación en VLAN's para identificar los puntos de interconexión y el alcance de red.
4. Se identificaron las vulnerabilidades de seguridad informática del Colegio Santa María Reina encontradas bajo la norma ISO 2700, de esta forma permitió proponer y documentar políticas de seguridad que deberá cumplir el colegio para el uso de la red propuesta.
5. Se identificó la demanda de servidores y equipos de comunicación que necesita el Colegió Santa Maria Reina, gracias al diseño lógico de la red propuesto, logrando una red altamente estable con equipos que permitan una red segura y confiable.
6. El diseño de red propuesto despliega resultados que evidencian un mejor funcionamiento de las aplicaciones y servicios, además de ser una solución sostenible por la garantía de marca CISCO y LINKSYS, permitiendo ser rentable para el Colegio Santa María Reina.
7. Mediante el diseño propuesto de red informática se logró probar el rendimiento, la disponibilidad del colegio Santa Maria Reina utilizando la herramienta Nagios y proponiendo sistemas redundantes en la red logrando un buen performance, nivel de seguridad y rendimiento entre sus diversas aulas, áreas, departamentos, y servicios.

6. RECOMENDACIONES

1. Se recomienda llevar a cabo la implementación planteada en nuestra propuesta de investigación para mejorar el rendimiento de la red informática y satisfacer las necesidades de los alumnos, docentes y personal administrativo del Colegio Santa María Reina.

2. Se recomienda al Colegio, realizar un plan de mantenimiento preventivo y correctivo a los equipos tecnológicos asegurando una larga vida y mejorando la productividad en la red, así como también el nivel de seguridad.

3. Se recomienda realizar capacitaciones periódicas al personal del Colegio Santa María Reina con la finalidad de fomentar la práctica de las políticas de seguridad y las directivas propuestas, para evitar incidencias de seguridad garantizando el rendimiento y el óptimo funcionamiento de la red.

4. Dado que el Colegio Santa Maria Reina no cuenta con informes de la red existente, se recomienda realizar un inventario de los equipos y las configuraciones desarrolladas con la finalidad de documentar la información de los cambios de equipos y usuarios permitiendo un mejor control y seguimiento de la red informática.

5. Se recomienda al área de informática gestionar con la dirección general, realizar el requerimiento que ayuden a brindar el financiamiento en la mejora tecnológica constante para el beneficio de las estudiantes, ofreciendo una mejora educativa con el apoyo de herramientas tecnológicas que permita dar un mejor alcance educativo.

REFERENCIAS BIBLIOGRÁFICAS

a. Aguado, J. Gestión de Seguridad para aumentar el rendimiento de la red informática. Madrid: Ediciones Díaz de Santo, 2018, 800-912 pp. ISBN: 9788499698021

b. Fuentes, R. (2020). Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca [Tesis pregrado, Universidad Nacional Pedro Ruiz Gallo]. Recuperado https://repositorio.unprg.edu.pe/handle/20.500.12893/9097

c. Alea, V. Gestión de riesgos en una red informática. Barcelona: Universidad de Barcelona, 2018, pp. 1-316. ISBN: 8483382571

d. Álvarez; E y Enrico; S. Gestión y evaluación del riesgo informático. Editorial Factors Humans. Barcelona, 2017. ISBN: 978-84-615-6340-1

e. Atienza, M. 2018. Políticas de seguridad pública y privada. Español; Castellano: Ediciones Experiencia, 2018. ISBN 978-842833-267-5

f. Barbosa, R. (2016). VLAN: Revelando los misterios de las VLAN. Obtenido de CCNA Route & Switch: http://www.seaccna.com/vlan/#

g. Blas, J. (2017). Seguridad y control del acceso a las redes inalámbricas en la UNSM-T mediante servidores de autentificación RADIUS con el uso de certificados digitales. [Tesis pregrado, UNMSM, Lima]. Recuperado de http://repositorio.unsm.edu.pe/handle/11458/2206

h. Books, M. 2017. Manual de seguridad en el trabajo. Español; Castellano: Marge Books, 2017. ISBN: 1794-2470

i. CISCO CCNA2. (s.f.). VLAN CAPITULO 6. Obtenido de CISCO CCNA2: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6.2

j. Yañez, N. (2017). Sistema de gestión de seguridad de la información para la subsecretaria de Economía y empresas de menor tamaño [Tesis post-grado, Universidad Nacional de Chile]. Recuperado https://repositorio.uchile.cl/handle/2250/147976

k. Flores, D. (2017). Atacar un Switch Cisco. Obtenido de TARINGA: https://www.taringa.net/posts/info/19885285/Atacar-un-Switch-Cisco---Parte-1-Mac-Flooding-Attack.html

l. EcuRed. (2016). VLAN. Obtenido de EcuRed: https://www.ecured.cu/VLAN

m. Franciosi, M y Vidarte, M. (2021). Importancia de la cultura de gestión de riesgos en el Perú. Revista Accounting Power for Business 1(1), 73 – 90. DOI: https://revistas.upeu.edu.pe/index.php/ri_apfb/article/view/898

n. Florez, P. (2018). Análisis de la normatividad en seguridad y salud ocupacional en la informática privada Revista Derecho & Sociedad, 1(43), 151-167. DOI: http://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/12567/13125 ISSN: 2019-3634

o. Huerta, M. (s.f). METODOLOGIA DE DISEÑO DE RED TOP DOWN. En M. Huerta, Metodología Top Down (pág. 19).

p. Irastorza, J. (2016). Arquitectura de Gestión Distribuida para Redes Malladas Inalámbricas: Aplicación en el Entorno de la Red Personal. Universidad de Cantabria. España.

q. Juan, G. (2019) FPB - Instalación y mantenimiento de redes para transmisión de datos https://books.google.com.pe/books?id=pY2XDwAAQBAJ&pg=PA82&dq=sistema+de+cableado+estructurado&hl=es&sa=X&ved=2ahUKEwi53-aKoc7uAhVLGLkGHUHUB-gQ6AEwAnoECAQQAg#v=onepage&q=sistema%20de%20cableado%20estructurado&f=false

r. David B. (2019) Administración de redes telemáticas https://es.scribd.com/book/409472879/Administracion-de-redes-telematicas

s. Marco N. (2019) Cableado Estructurado – Instituto Tecnológico Superior del el Mante https://es.scribd.com/document/409241907/Cableado-Estructurado

t. José C. (2019) Wi-Fi. Instalación, Seguridad y Aplicaciones: Redes y aplicaciones WAP (del protocolo para aplicaciones inalámbricas). https://es.scribd.com/book/409464435/Wi-Fi-

Instalacion-Seguridad-y-Aplicaciones-Redes-y-aplicaciones-WAP-del-protocolo-para-aplicaciones-inalambricas.

u. Rafael C (2012) Redes Locales, https://www.buscalibre.pe/libro-redes-locales-2012-sistemas-microinformaticos-y-redes/9788415426479/p/8317762

v. MILAGRITOS. (2013). METODOLOGIAS DE REDES. Obtenido de METODOLOGIAS PARA IMPLEMENTAR PROYECTOS DE REDES: http://metodologiaspararedes.blogspot.com/

w. Montes, J. (2016). Diseño de arquitectura de seguridad perimetral para una empresa dedicada a la actividad inmobiliaria. [Tesis pregrado, Universidad Ricardo Palma, Lima] Recuperado de http://cybertesis.urp.edu.pe/handle/urp/1285

x. Muñoz, J. (2016). Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la Universidad de Cuenca. Recuperado de http://dspace.ucuenca.edu.ec/handle/123456789/25646

y. Oppenheimer, P. (2011). Top-Down Network Design. 3° Edition. EE.UU. Recuperado de http://www.teraits.com/pitagoras/marcio/gpi/b_POppenheimer_TopDownNetworkDesign_3rd_ed.pdf

z. Pérez, C. (2019). Métodos de control en seguridad informática. Universidad y Sociedad, 9(2), 219-224. DOI: http://scielo.sld.cu/pdf/rus/v9n3/rus34317.pdf

aa. ARIGANELLO, Ernesto y BARRIENTOS, [en línea] Enrique. Redes Cisco CCNP a Fondo, Guía de estudio para profesionales. Madrid, 2015. [fecha de consulta: 08 de febrero de 2021]. Disponible en https://books.google.com.pe/books?id=Zo-fDwAAQBAJ&pg=PA335&dq=vtp&hl=es&sa=X&ved=2ahUKEwj08Kz83NruAhVIGbkGHeXPDJUQ6AEwAnoECAQQAg#v=onepage&q=vtp&f=false

bb. LEDERKREMER, Miguel. Redes Informáticas 1era ed. Ciudad Autónoma de Buenos Aires,2019 pp. 126-130

cc. Chambergo, G. (2015). Rediseño de la red de transmisión de datos para mejorar la gestión del rendimiento de red de la Corte Superior de Justicia de Junín - sede central. [Tesis pregrado, UNCP Huancayo]. Recuperado http://hdl.handle.net/20.500.12894/6111

dd. Horna, P. (2021). Propuesta de Reingeniería de la Red LAN de la Red de Salud Pacifico Sur - Nuevo Chimbote; 2021. [Tesis pregrado, Universidad Católica Los Ángeles Chimbote]. Recuperado de http://repositorio.uladech.edu.pe/handle/123456789/21771

ee. Yacila, R. (2021). Propuesta de Implementación de una Red LAN para la Municipalidad Distrital de Corrales Tumbes; 2021. [Tesis pregrado, Universidad Católica Los Ángeles Chimbote]. Recuperado de http://repositorio.uladech.edu.pe/handle/123456789/23074

ff. Sanchez, I. (2017). Diseño e implementación de una red informática LAN y el servicio de internet en alta velocidad utilizando la metodología Top-Down para la comunicación de los equipos informáticos de la Municipalidad Distrital de José Sabogal en la Provincia de San Marcos departamento de Cajamarca, Perú. [Tesis pregrado, Universidad Peruana Unión]. Recuperado de http://hdl.handle.net/20.500.12840/1504

gg. Barbacho – Benjumea et al. (2018). Redes Locales. https://books.google.com.pe/books?id=zpzODwAAQBAJ&lpg=PP1&dq=Barbacho%20%E2%80%93%20Benjumea&hl=es&pg=PP1#v=onepage&q=Barbacho%20%E2%80%93%20Benjumea&f=false

hh. Zapata, H y Grisales, T. (2020). Importancia de la formación para la prevención de riesgos en la informática. Revista Accounting Power for Business 1(2), 59 – 69. DOI: https://revistas.upeu.edu.pe/index.php/ri_apfb/article/view/889

ANEXOS

Anexo 01:

Instrumento de Recolección de Datos – Encuesta a las estudiantes.

DATOS GENERALES:

Nivel: ……Grado:……

Edad: [ ] Sexo: Femenino [ ] Masculino [ ]

Se ha diseñado el presente cuestionario para analizar la situación actual problemática del Colegio Santa Maria en que cuanto tecnología e infraestructura por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

PREGUNTAS		**SIEMPRE**	**A VECES**	**NUNCA**	**TOTAL**
Fase 1: Análisis de Negocios Objetivos y limitaciones					
1.-	¿Cree usted que la red de las aulas o laboratorios se encuentra debidamente organizada?				
2.-	¿El servicio de internet en la institución es rápido?				
3.-	¿Existe internet inalámbrico (WIFI) en sus aulas o laboratorios?				
4.-	¿Las computadoras con las que trabajan son rápidas?				
Fase 2: Diseño Lógico					
5.-	¿Se encuentra en buen estado las instalaciones del cableado en la institución?				
6.-	¿Sabe los cables de internet en el laboratorio están cubierto por canaletas o empotrados?				

7.-	¿Para tener internet es necesario darle algún movimiento al cable en el Laboratorio?				
8.-	¿El servicio de internet en la institución es rápido?				
Fase 3: Diseño Físico					
9.-	¿Son adecuados los equipos que utiliza en los laboratorios?				
10.-	¿Puede realizar comparticiones de archivos con otro computador en la red de la institución? Sin usar USB, ni otro medio				
11.-	¿Considera que los equipos tecnológicos que dispone la Institución Educativa son suficientes para todo el alumnado?				
12.-	¿Existen impresoras disponibles en red para imprimir tus archivos en la institución Educativa?				
Fase 4: Pruebas, Optimización y Documentación de la red.					
13.-	¿Se realizan talleres en la institución que abarquen temas informáticos?				
14.-	¿Existen políticas de seguridad para el acceso a internet?				
15.-	¿Se han restringido algunas páginas inseguras de la web?				
16.-	¿Lo han instruido sobre medidas de como tener los equipos informáticos en su área y el uso que se le debe dar?				
Fase 4: Gestión de Redes					
17.-	¿Sabe usted si se realiza mantenimiento periódico de la red de la Institución Educativa?				

- 18.	¿Cuenta usted con los programas y aplicaciones necesarias para el desarrollo de sus actividades en los laboratorios?				
- 19.	¿La computadora de los laboratorios cuenta con contraseñas?				
- 20.	¿Existe un personal o software encargado de dar solución en caso su PC presente problemas en plena clase de laboratorio?				

Anexo 02:

Instrumento de Recolección de Datos – Encuesta a los profesores.

DATOS GENERALES:

Nivel: …… Grado: ……..

Edad: [ ] Sexo: Femenino [ ] Masculino [ ]

Se ha diseñado el presente cuestionario para analizar la situación actual problemática del Colegio Santa Maria en que cuanto tecnología e infraestructura por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

	PREGUNTAS	**SIEMPRE**	**A VECES**	**NUNCA**	**TOTAL**
Fase 1: Análisis de Negocios Objetivos y limitaciones					
1.-	¿Cree usted que la red de las aulas o laboratorios se encuentra debidamente organizada?				
2.-	¿El servicio de internet en la institución es rápido?				
3.-	¿Existe internet inalámbrico (WIFI) en sus aulas o laboratorios?				
4.-	¿Las computadoras con las que trabajan son rápidas?				
Fase 2: Diseño Lógico					
5.-	¿Se encuentra en buen estado las instalaciones del cableado en la institución?				
6.-	¿Sabe los cables de internet en el laboratorio están cubierto por canaletas o empotrados?				
7.-	¿Para tener internet es necesario darle algún movimiento al cable en el Laboratorio?				
8.-	¿El servicio de internet en la institución es rápido?				
Fase 3: Diseño Físico					
9.-	¿Son adecuados los equipos que utiliza en los laboratorios?				

10.-	¿Puede realizar comparticiones de archivos con otro computador en la red de la institución? Sin usar USB, ni otro medio				
11.-	¿Considera que los equipos tecnológicos que dispone la Institución Educativa son suficientes para todo el alumnado?				
12.-	¿Existen impresoras disponibles en red para imprimir tus archivos en la institución Educativa?				
Fase 4: Pruebas, Optimización y Documentación de la red.					
13.-	¿Se realizan talleres en la institución que abarquen temas informáticos?				
14.-	¿Existen políticas de seguridad para el acceso a internet?				
15.-	¿Se han restringido algunas páginas inseguras de la web?				
16.-	¿Lo han instruido sobre medidas de como tener los equipos informáticos en su área y el uso que se le debe dar?				
Fase 4: Gestión de Redes					
17.-	¿Sabe usted si se realiza mantenimiento periódico de la red de la Institución Educativa?				
18.-	¿Cuenta usted con los programas y aplicaciones necesarias para el desarrollo de sus actividades en los laboratorios?				
19.-	¿La computadora de los laboratorios cuenta con contraseñas?				
20.-	¿Existe un personal o software encargado de dar solución a un problema TIC?				

Anexo 03:

Instrumento de Recolección de Datos – Encuesta al personal administrativo.

DATOS GENERALES:

Cargo: …….

Área: …….

Edad: [ ] Sexo: Femenino [ ] Masculino [ ]

Se ha diseñado el presente cuestionario para analizar la situación actual problemática del Colegio Santa Maria en que cuanto tecnología e infraestructura por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

	PREGUNTAS	SIEMPRE	A VECES	NUNCA	TOTAL
Fase 1: Análisis de Negocios Objetivos y limitaciones					
1.-	¿Cree usted que la red de las aulas o laboratorios se encuentra debidamente organizada?				
2.-	¿El servicio de internet en la institución es rápido?				
3.-	¿Existe internet inalámbrico (WIFI) en sus aulas o laboratorios?				
4.-	¿Las computadoras con las que trabajan son rápidas?				
Fase 2: Diseño Lógico					
5.-	¿Se encuentra en buen estado las instalaciones del cableado en la institución?				
6.-	¿Sabe los cables de internet en el laboratorio están cubierto por canaletas o empotrados?				
7.-	¿Para tener internet es necesario darle algún movimiento al cable en el Laboratorio?				
8.-	¿El servicio de internet en la institución es rápido?				
Fase 3: Diseño Físico					
9.-	¿Son adecuados los equipos que utiliza en los laboratorios?				

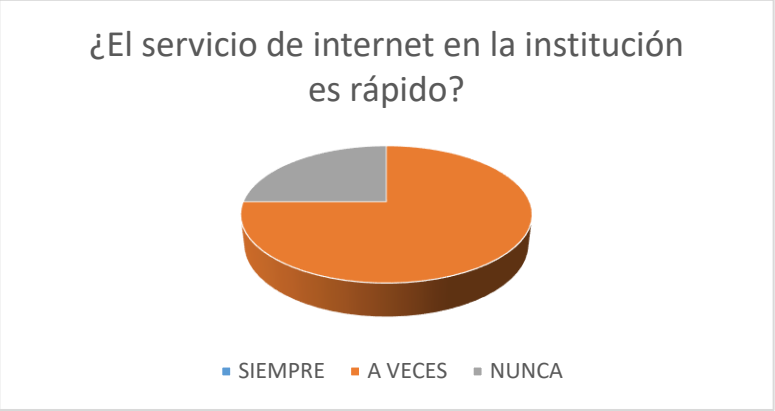
10.-	¿Puede realizar comparticiones de archivos con otro computador en la red de la institución? Sin usar USB, ni otro medio				
11.-	¿Considera que los equipos tecnológicos que dispone la Institución Educativa son suficientes para todo el alumnado?				
12.-	¿Existen impresoras disponibles en red para imprimir tus archivos en la institución Educativa?				
Fase 4: Pruebas, Optimización y Documentación de la red.					
13.-	¿Se realizan talleres en la institución que abarquen temas informáticos?				
14.-	¿Existen políticas de seguridad para el acceso a internet?				
15.-	¿Se han restringido algunas páginas inseguras de la web?				
16.-	¿Lo han instruido sobre medidas de como tener los equipos informáticos en su área y el uso que se le debe dar?				
Fase 4: Gestión de Redes					
17.-	¿Sabe usted si se realiza mantenimiento periódico de la red de la Institución Educativa?				
18.-	¿Cuenta usted con los programas y aplicaciones necesarias para el desarrollo de sus actividades en los laboratorios?				
19.-	¿La computadora de los laboratorios cuenta con contraseñas?				
20.-	¿Existe un personal o software encargado de dar solución en caso su PC presente problemas en plena clase de laboratorio?				

Anexo 04:

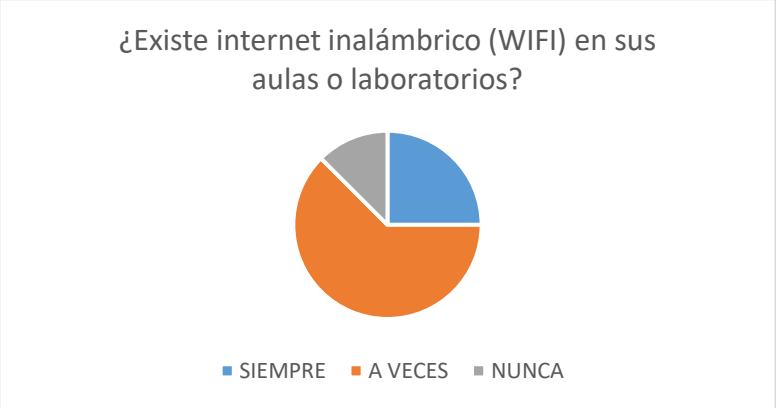
Resultado de encuesta aplicado a las estudiantes.

1. ¿Cree usted que la red de las aulas o laboratorios se encuentra debidamente organizada?

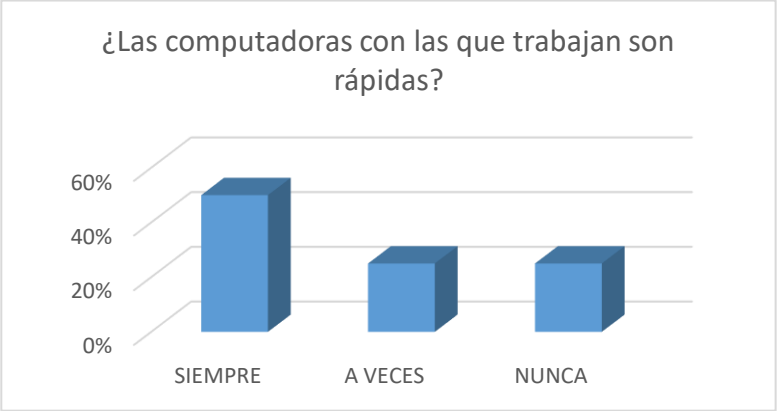
2. ¿El servicio de internet en la institución es rápido?



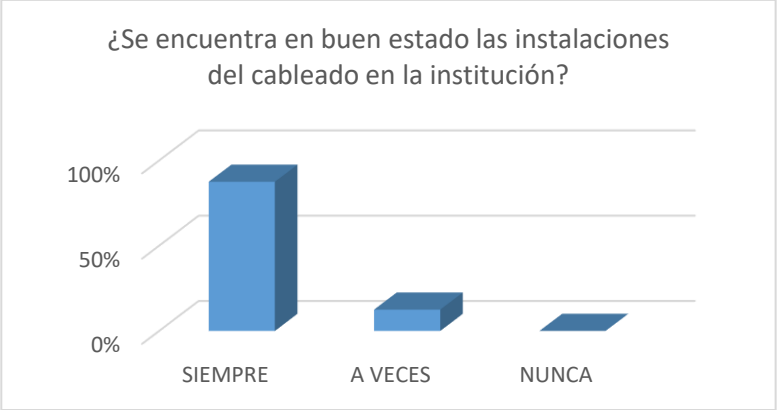
3. ¿Existe internet inalámbrico (WIFI) en sus aulas o laboratorios?



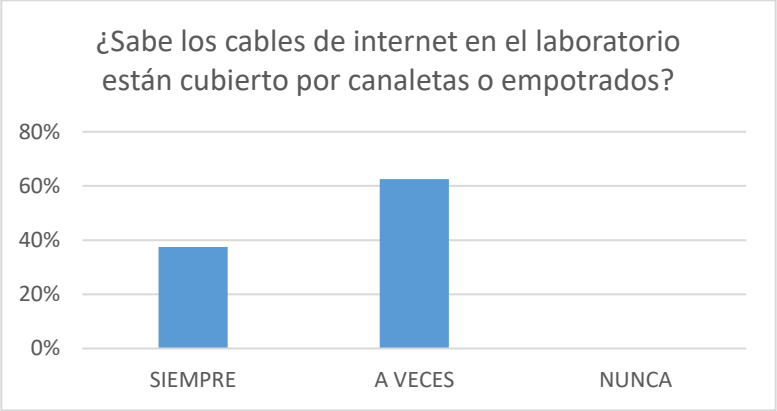
4. ¿Las computadoras con las que trabajan son rápidas?



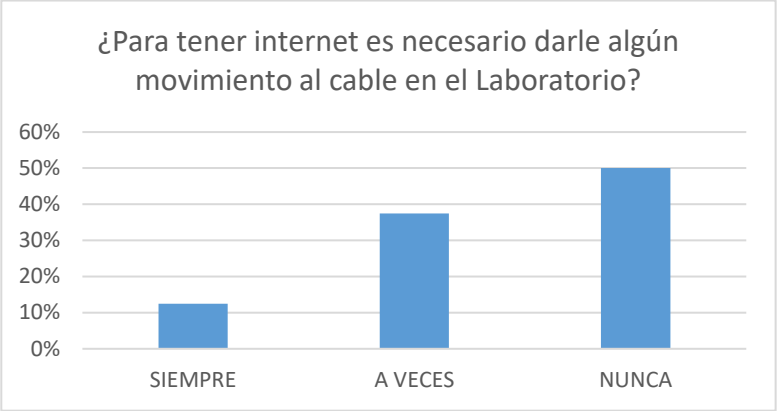
5. ¿Se encuentra en buen estado las instalaciones del cableado en la institución?



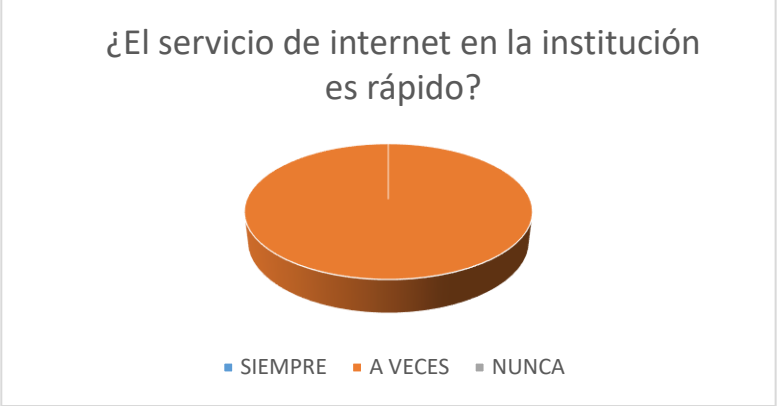
6. ¿Sabe los cables de internet en el laboratorio están cubierto por canaletas o empotrados?



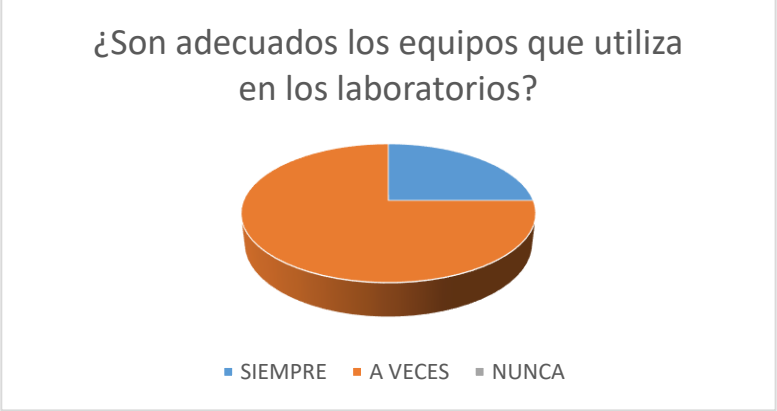
7. ¿Para tener internet es necesario darle algún movimiento al cable en el Laboratorio?



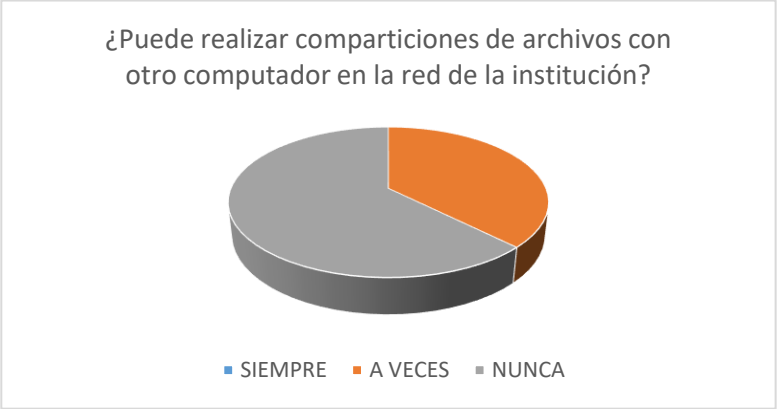
8. ¿El servicio de internet en la institución es rápido?



9. ¿Son adecuados los equipos que utiliza en los laboratorios?

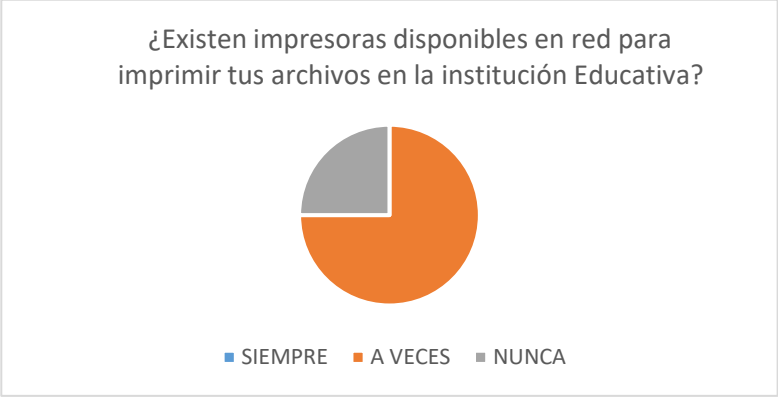


10.¿Puede realizar comparticiones de archivos con otro computador en la red de la institución?

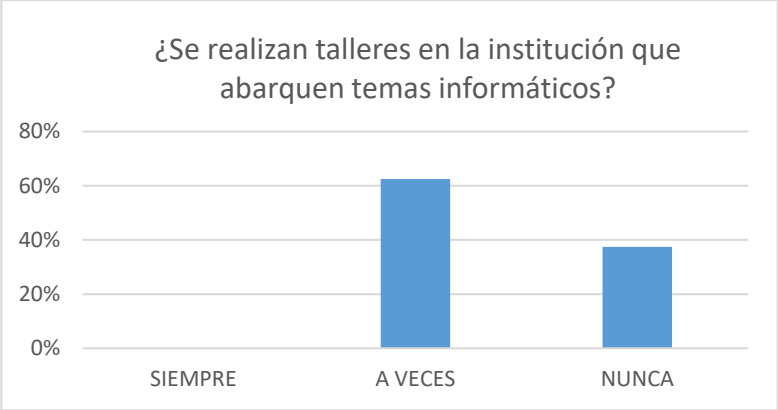


11.¿Considera que los equipos tecnológicos que dispone la Institución Educativa son suficientes para todo el alumnado?

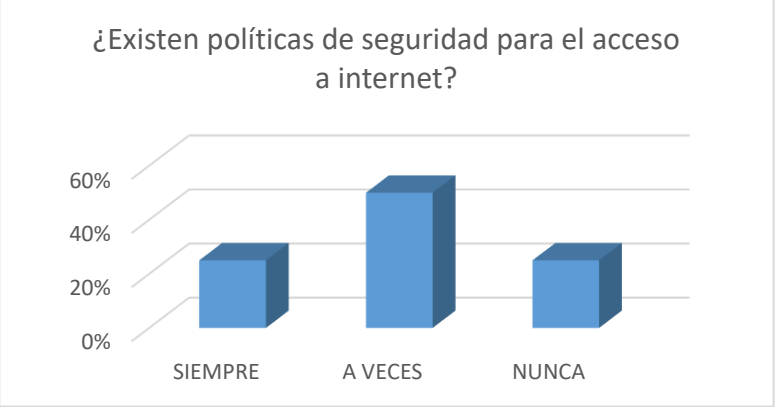
12.¿Existen impresoras disponibles en red para imprimir tus archivos en la institución Educativa?



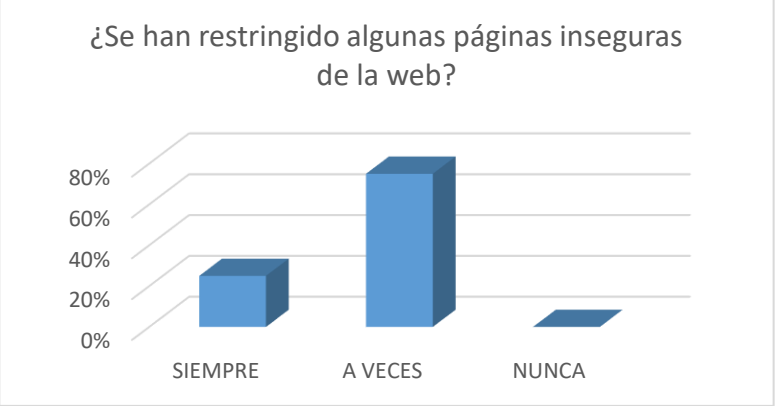
13.¿Se realizan talleres en la institución que abarquen temas informáticos?



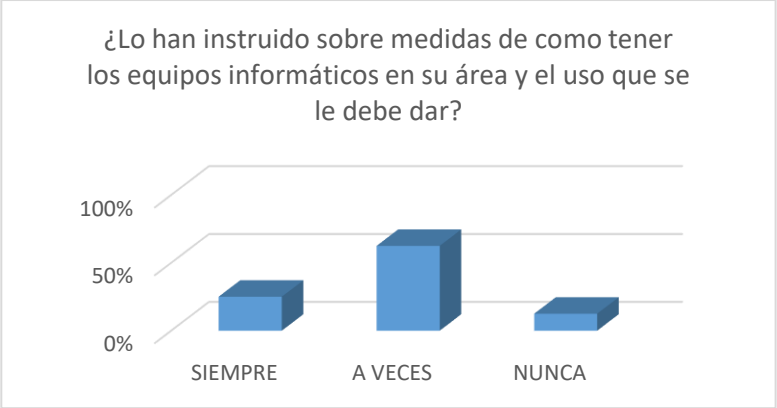
14.¿Existen políticas de seguridad para el acceso a internet?



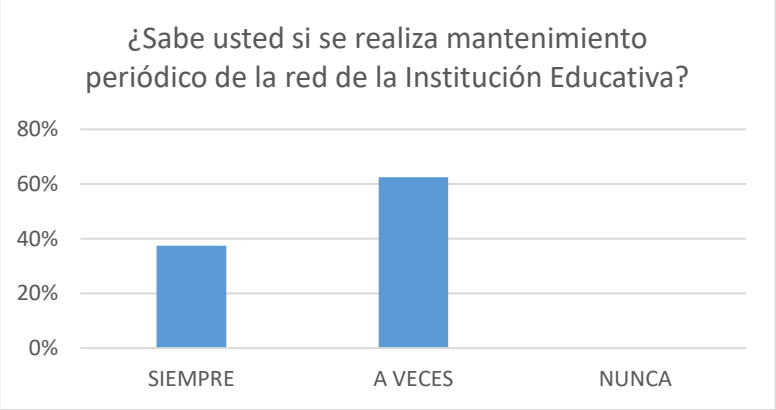
15.¿Se han restringido algunas páginas inseguras de la web?



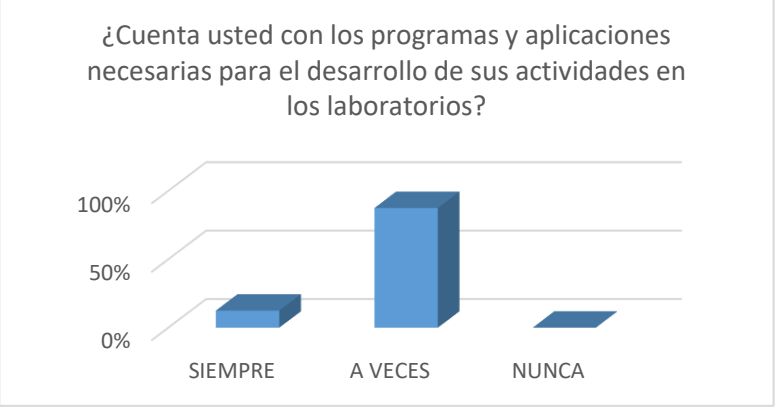
16.¿Lo han instruido sobre medidas de como tener los equipos informáticos en su área y el uso que se le debe dar?



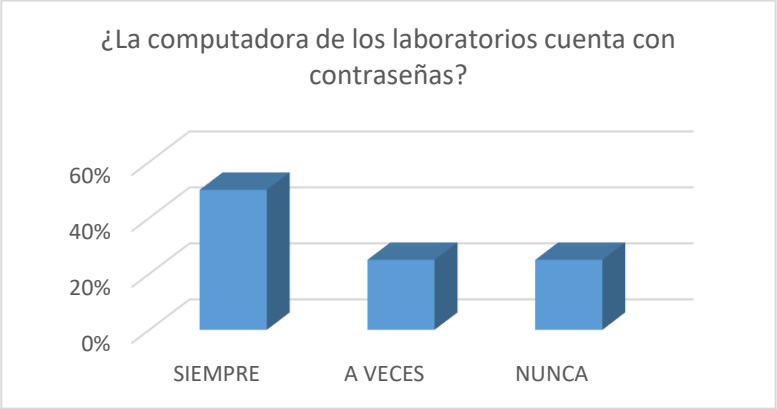
17.¿Sabe usted si se realiza mantenimiento periódico de la red de la Institución Educativa?



18.¿Cuenta usted con los programas y aplicaciones necesarias para el desarrollo de sus actividades en los laboratorios?



19.¿La computadora de los laboratorios cuenta con contraseñas?



20.¿Existe un personal o software encargado de dar solución en caso su PC presente problemas en plena clase de laboratorio?