UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS:

IMPLEMENTACIÓN DE INFRAESTRUCTURA DE REDES PARA MEJORAR LA COMUNICACIÓN Y SEGURIDAD DE DATOS EN LA UGEL 312 HUANCA SANCOS – AYACUCHO

PARA OPTAR: EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

Autor : **Bach. Ronald Apaico Mendoza**

Asesores : **Ing. Jowel Sigfrido Cabrera Padilla**

Ing. Rafael Edwin Gordillo Flores

Línea de Investigación : **Ingeniería e Infraestructura**

Huancayo – Perú

2023

ASESOR METODOLÓGICO
Ing. Jowel Sigfrido Cabrera Padilla

ASESOR TEMÁTICO
Ing. Rafael Edwin Gordillo Flores

DEDICATORIA

A Dios todo poderoso, también a mis padres Alejandrino y Trinidad, quienes siempre han confiado en mí y me han dado su apoyo incondicional, a su vez me enseñaron a ser cada vez mejor en esta vida.

Bach. Ronald Apaico Mendoza

AGRADECIMIENTO

A la Universidad Peruana Los Andes en especial a mis asesores el Ing. Jowel y Rafael por sus paciencia y profesionalismo.

Bach. Ronald Apaico Mendoza

CONSTANCIA 135

DE SIMILITUD DE TRABAJOS DE INVESTIGACIÓN POR EL SOFTWARE DE PREVENCIÓN DE PLAGIO TURNITIN

La Dirección de Unidad de Investigación de la Facultad de Ingeniería, hace constar por la presente, que el informe final de tesis titulado:

"IMPLEMENTACIÓN DE INFRAESTRUCTURA DE REDES PARA MEJORAR LA COMUNICACIÓN Y SEGURIDAD DE DATOS EN LA UGEL 312 HUANCA SANCOS – AYACUCHO"

Cuyo autor (a) : Ronald Apaico Mendoza.

Facultad : Ingeniería

Escuela Profesional : Ingeniería de Sistemas y Computación.

Asesor (a) (es) : Ing. Jowel Sigfrido Cabrera Padilla.

: Ing. Rafael Edwin Gordillo Flores

Que, fue presentado con fecha 06.03.2023 y después de realizado el análisis correspondiente en el software de prevención de plagio Turnitin con fecha 07.03.2023; con la siguiente configuración de software de prevención de plagio Turnitin:

Excluye bibliografía.

[X] Excluye citas.

[X] Excluye cadenas menores de a 20 palabras.

[ ] Otro criterio (especificar)

Dicho documento presenta un porcentaje de similitud de **20%**. En tal sentido, de acuerdo a los criterios de porcentajes establecidos en el artículo N°11 del Reglamento de uso de software de prevención de plagio, el cual indica que no se debe superar el **30%**. Se declara, que el trabajo de investigación: si contiene un porcentaje aceptable de similitud. Observaciones: Trabajo de Suficiencia Profesional.

En señal de conformidad y verificación se firma y sella la presenta constancia.

Huancayo 08 de Marzo del 2023

UNIVERSIDAD PERUANA LOS ANDES
DIRECCIÓN DE LA UNIDAD DE INVESTIGACIÓN
FACULTAD DE INGENIERÍA

Dr. Santiago Zevallos Salinas
Director de la Unidad de Investigación

HOJA DE CONFORMIDAD DE JURADOS

_____

Presidente

_____

Jurado

_____

Jurado

_____

Jurado

_____

Secretario Docente

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La presente tesis titulada “Implementación de infraestructura de redes para mejorar la comunicación y seguridad de datos en la UGEL 312 Huanca Sancos – Ayacucho” aborda la problemática de la infraestructura inadecuada y la seguridad los datos en los ambientes donde se ubican los equipos de comunicación de la red de datos mediante las conexiones de internet para uso de los sistemas de información y transferencia de datos. Por lo que se planteó como objetivo, determinar la implementación de infraestructura de redes para mejorar la comunicación y seguridad de datos.

Se realizó la implementación mediante un diseño de red convergente a medida de la UGEL Huanca Sancos para la comunicación y seguridad. Basándonos en la metodología de diseño de CISCO con el fin de optimizar el funcionamiento del ciclo de vida de la red: PPDIOO (acrónimo de sus fases en inglés; Prepare, Plan, Design, Implement, Operate y Optimize). Esta metodología se utiliza para planificar e implementar una infraestructura de red eficiente y sostenible en términos de rendimiento, escalabilidad y disponibilidad. Obteniendo como resultado un buen diseño de redes y el mejoramiento de atención a los usuarios y trabajo administrativo en la UGEL Huanca Sancos.

Los resultados mostraron que se pudo reducir el nivel de latencia de 74.17 ms (100%) a 28.07 ms (37.84%). Esto dio lugar a una reducción del nivel de latencia de 46.10 ms (62.15%). Del mismo modo en cuanto al nivel de Jitter, se redujo de 35.53 ms (100%) a 17.31 ms (48.71%). Esto dio lugar a una reducción del nivel de latencia de 18.22 ms (51.28%), logrando la meta de nuestro estudio.

El índice de detección de intrusiones se redujo de 78.17% al 44.03% Esto dio como resultado una reducción del índice de detección de intrusiones de 34.14% logrando para nuestro indicador mencionado, el porcentaje de 43.67%.

Validando de esta forma que la implementación de una infraestructura correcta de red reduce el nivel de latencia y nivel de Jitter en la UGEL Huanca Sancos.

Palabras claves: infraestructura de red, seguridad de datos, metodología PDIOO

ABSTRACT

This thesis entitled "Implementation of network infrastructure to improve communication and data security at UGEL 312 Huanca Sancos - Ayacucho" addresses the problem of inadequate infrastructure and data security in the environments where the communication equipment of the data network through internet connections for the use of information systems and data transfer. Therefore, the objective was to determine the implementation of network infrastructure to improve communication and data security.

The implementation was carried out through a convergent network design tailored to the UGEL Huanca Sancos for communication and security. Based on the CISCO design methodology in order to optimize the operation of the network life cycle: PPDIOO (acronym for its phases in English; Prepare, Plan, Design, Implement, Operate and Optimize). This methodology is used to plan and implement an efficient and sustainable network infrastructure in terms of performance, scalability and availability. Obtaining as a result a good design of networks and the improvement of attention to users and administrative work in the UGEL Huanca Sancos.

The results showed that the latency level could be reduced from 74.17 ms (100%) to 28.07 ms (37.84%). This resulted in a latency level reduction of 46.10 ms (62.15%). In the same way regarding the Jitter level, it was reduced from 35.53 ms (100%) to 17.31 ms (48.71%). This resulted in a latency level reduction of 18.22 ms (51.28%), achieving the goal of our study.

The intrusion detection rate was reduced from 78.17% to 44.03% This resulted in a reduction of the intrusion detection rate of 34.14%. Achieving for our mentioned indicator, the percentage of 43.67%.

Validating in this way that the implementation of a correct network infrastructure reduces the level of latency and level of Jitter in the UGEL Huanca Sancos.

Keywords: network infrastructure, data security, PDIOO methodology

INTRODUCCIÓN

Esta investigación tiene como objetivo principal: Determinar cómo la implementación de infraestructura de redes mejora la comunicación y seguridad de datos en la UGEL Huanca Sancos. Por lo que se ha procedido al desarrollo de la tesis guiado por dicho objetivo en cinco capítulos de la siguiente manera:

En el primer capítulo, se realiza la formulación del problema, la problemática, la justificación como a las delimitaciones, las limitaciones y los objetivos de la investigación.

En el segundo capítulo, se desarrolla el Marco teórico iniciando por los antecedentes, seguido por las bases teóricas, el Marco conceptual, la definición de las hipótesis y terminando con la definición de las variables.

En el tercer capítulo, se aborda la metodología por la cual se ha dado la solución a la problemática.

En el cuarto capítulo, se desarrolla en los resultados, en donde se realizó el desarrollo de la metodología y el ciclo de vida del proyecto desde su planificación hasta su implementación, Además el análisis de resultados iniciando por el análisis descriptivo, la prueba de normalidad y finalizando con la prueba de hipótesis, en donde se pudo concluir que se rechazaron las hipótesis nulas y se aceptaron las alternas.

El quinto capítulo, se realiza la discusión de los resultados de la implementación de la solución.

Finalmente, se esbozan las conclusiones y recomendaciones de la investigación.

CAPITULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

La presente investigación se realizó en la Unidad de Gestión Educativa Local de Huanca Sancos, es una instancia de ejecución descentralizada de la Dirección Regional de Educación, del Gobierno Regional de Ayacucho, con autonomía en el ámbito de su competencia, Responsables de promover, coordinar y evaluar el servicio educativo que ofrecen las Instituciones y Programas Educativas en su ámbito jurisdiccional y presupuestalmente como Unidad Ejecutora depende del Gobierno Regional Ayacucho.

La función principal de esta Unidad, es brindar asistencia técnica al trabajo educativo que desarrolla, a su vez se encargan de difundir, orientar y supervisar la aplicación de la política normatividad educativa nacional o regional en materia de gestión institucional, pero también se encargan de evaluar los resultados de las instituciones y programas bajo el ámbito de la UGEL Huanca Sancos para el bien de la población, directivos, docentes, administrativos y estudiantes de las Instituciones Educativas en el ámbito de la UGEL Huanca Sancos, se tiene los aplicativos y sistemas informáticos interconectados con el Ministerio de Educación, Gobierno Regional de Ayacucho y la Dirección Regional Educación Ayacucho son permanentes, los cuales tiene que tener un buen ancho de banda y velocidad de transferencia de datos, tanto para procesamiento de navegación on-line y off-line en los procesos administrativo; así como también la buena comunicación con los servidores interconectados para el uso de los diferentes sistemas de información, aplicativos web y entornos virtuales.

Los problemas más comunes detectados en la actualidad, se mencionan a continuación:

a) Las áreas no cuentan con ambientes propios en la que estuvo funcionando inadecuadamente, los equipos de red se encuentran ubicados a una distancia de 1 metro y el cableado están mal ubicados la cual la transferencia de datos y manejo de los sistemas informáticos no respondían de forma rápida y con averías de conectividad constantes.
b) Los servidores se encontraban en ambientes inadecuados sin ventilación donde no se garantiza su conservación y funcionamiento correcto como se muestra en la figura 1.1.

Figura 1.1: Evidencia del servidor con problemas

c) Algunos usuarios con conocimiento de informática vulneraron la conectividad del acceso a internet, como se muestra en la figura 1.2, el cambio de los protocolos de internet (IP) y el desorden en la enumeración, ocasionando conflictos de IP para los demás equipos de cómputo conectados en la red de datos.

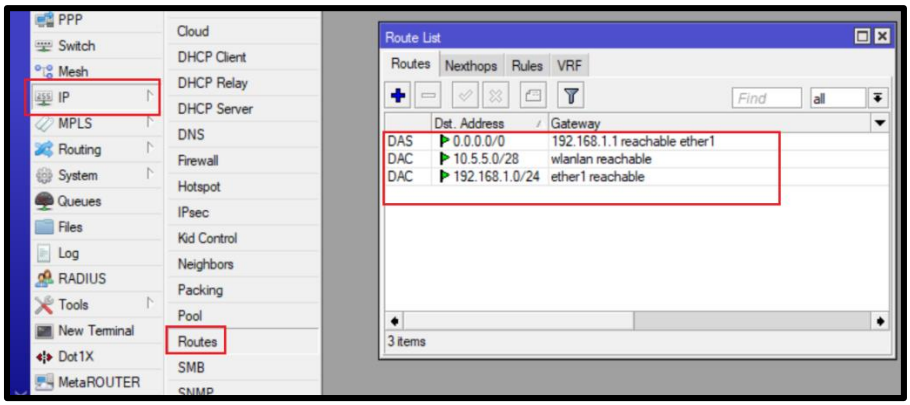


Figura 1.2: evidencia del problema, conectividad.

d) El cableado de red de datos es precario, en la figura 1.3 se muestra que las ubicaciones de varios puntos están sin protección. También, existe conexiones por los techos donde la temperatura en horas del mediodía y la tarde es alta.

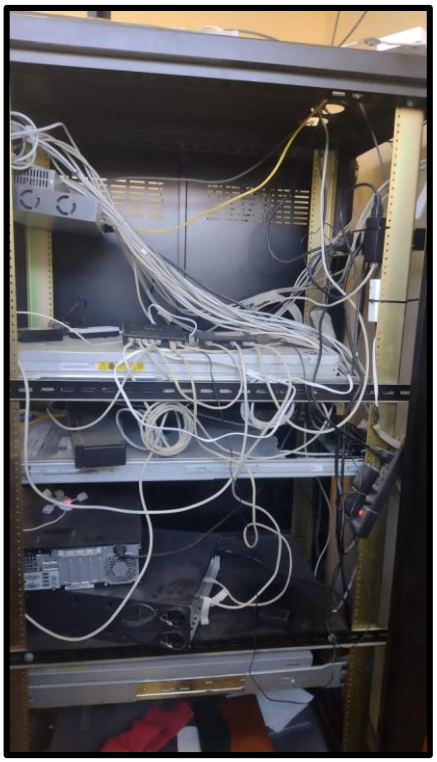


Figura 1.3: evidencia del problema, cableado precario.

e) Los usuarios internos que utilizan los sistemas de información web han manifestado quejas mencionado en varias oportunidades su inconformidad sobre los ambientes que son pequeños e inadecuados para realizar un trabajo estable, así mismo la navegación de internet esta lenta en horas punta como son de ocho a diez de la mañana y por las tardes de cinco a seis de la tarde ocasionando incomodidad y desesperación de los usuarios y público en general. Ver la figura 1.4.

Figura 1.4: evidencia del problema, ambientes inadecuados.

f) En la figura 1.5 podemos percibir la inseguridad, en los ambientes donde se ubican los equipos de comunicación (Switch) de la red de datos. Se observa que el cableado de internet y eléctrico es precario, que no cuenta con equipos de protección como un rack o gabinete para con su respectivo organizador de cable.

Figura 1.5: evidencia del problema, inseguridad.

1.2 Formulación y sistematización del Problema

1.2.1 Problema General

¿Cómo la implementación de infraestructura de redes mejorará la comunicación y seguridad de datos en la UGEL Huanca Sancos?

1.2.2 Problemas Específicos

a) ¿En qué medida la implementación de infraestructura de redes influirá en el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos?

b) ¿En qué medida la implementación de infraestructura de redes influirá en la seguridad de la red en la UGEL Huanca Sancos?

c) ¿Cómo implementar la infraestructura de redes, para mejorar la comunicación y seguridad en la UGEL Huanca Sancos?

1.3 Justificación

1.3.1 Social o práctica

Al realizarse la investigación de la implementación de infraestructura de redes de la UGEL Huanca Sancos permitirá mejorar la comunicación entre los trabajadores de las diferentes áreas y equipos informáticos enlazados con los servidores del MINEDU y Dirección Regional Ayacucho, así mismo mejorará el servicio de atención a los directivos, docentes, administrativos, padres de familia y público en general de la jurisdicción de la UGEL Huanca Sancos.

1.3.2 Científica o teórica

Al realizarse la investigación se desarrollará una revisión y colección de algunos conocimientos teóricos para sustentar el estudio. Así mismo se recopilará información y conocimientos de los resultados de la investigación que pueden servir de referencia para problemáticas similares.

1.3.3 Metodológica

La aplicación de esta metodología de investigación, establecerá un procedimiento en la búsqueda de solución a los problemas proyectados en la organización del diseño

estructurado. Este procedimiento se podrá tomar como referencia metodológica en la realización de otras investigaciones que aborden problemas similares.

1.4 Delimitaciones

1.4.1 Espacial

El desarrollo y la implementación del cableado estructurado se ha desarrollado en todas las áreas de la UGEL, las cuales se encuentran en un área bastante amplio, por lo que el mapeo y la instalación se realizó de manera ordenada para evitar la confusión de la gran cantidad de cables existentes, además se realizó la verificación de los estándares de cableado para evitar interferencia con otros cables como los de luz y así garantizar la óptima transferencia de datos e información en todo el área.

1.4.2 Temporal

El tiempo asignado para el desarrollo de toda la implementación fue de 4 meses, hasta el último día del mes de diciembre por lo que se realizó la optimización de actividades, así como un plan de trabajo y un plan de contingencia en caso de dificultades al momento de realizar las actividades. Tiene mucha importancia en la priorización de actividades y el desarrollo de las mismas, ya que cada día de retraso pudo significar una gran pérdida de recursos no sólo sobre la instalación sino también la limitación del trabajo del personal que depende de los equipos y de las conexiones.

1.4.3 Económica

El proyecto actual para poder realizar la implementación de toda la infraestructura de red fue financiado por la UGEL, y la investigación por parte del investigador.

1.5 Limitaciones

Actualmente en la entidad pública, se están brindando todas las facilidades para poder realizar la implementación del proyecto. El único inconveniente o limitación es que la instalación de la infraestructura de la red, en algunos casos, tuvo que paralizar las actividades laborales que se desarrollan de ciertos ambientes. Para evitar esto, la instalación se debió desarrollar en momentos en el que el personal no esté laborando o se encuentre de vacaciones o fuera de oficina. Sólo si era muy necesario, se pedía pausar las actividades por el menor

tiempo posible. En este sentido, muchas de las actividades se desarrollan en las noches o después del cierre del horario regular de trabajo de los colaboradores.

1.6 Objetivos

1.6.1 Objetivo General

Determinar cómo la implementación de infraestructura de redes mejora la comunicación y seguridad de datos en la UGEL Huanca Sancos.

1.6.2 Objetivos Específicos

a) Determinar en qué medida la implementación de infraestructura de redes influirá en el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos.
b) Establecer como la implementación de infraestructura de redes influirá en la seguridad de la red en la UGEL Huanca Sancos.
c) Implementar una infraestructura de redes que mejora la comunicación y seguridad de la red en la UGEL Huanca Sancos.

CAPITULO II
MARCO TEÓRICO

2.1. Antecedentes

Para realizar la propuesta de investigación mediante el plan de tesis se ha revisado los siguientes trabajos:

2.1.1. Antecedentes Nacionales

- La tesis [1], aborda el problema de demora en el acceso a las aplicaciones WAN debido a que el servicio de internet es satelital con un ancho de banda 2028 Kbps. Así mismo, la red presenta problemas constantes de duplicidad de IP, accesos no autorizados por usuarios no identificados. Para superar esta problemática se plantea realizar el diseño de red convergente para mejorar los servicios de comunicación de la Municipalidad Distrital de Manta.

- En la tesis [2], se trata el problema del tráfico de comunicación al momento del acceso a los sistemas informáticos como sistema de Información de Gestión Documentaria (SISGEDO), el Sistema Integral de Gestión Administrativa (SIGA) y el sistema Integral de Administración Financiera (SIAF) y otros sistemas que se usan frecuentemente en la DIRESA JUNIN. El problema se enfrenta con la implementación de red diseñada mediante la tecnología Top Down Network Desing para descongestionar el tráfico de datos y mejorar la conectividad de los equipos informáticos de la DIRESA JUNIN.

- El artículo [3], indaga el problema de acceso a recursos de internet mediante la gestión de una red de computadoras que no contaba con controles para una adecuada gestión del servicio que trajo como consecuencia un limitado acceso a diversos recursos

demandados por usuarios para el desarrollo de actividades académicas o administrativas. Para mejorar la conectividad y control de ancho de banda se planteas diseñar la red en base a la metodología propuesta por James McCabe. Se usa dispositivos Mikrotik para gestionar la red que logra mejorar la calidad de uso del servicio de internet demandados por usuarios de la Escuela Profesional de Contabilidad de la Facultad de Ciencias Empresariales de la Universidad Nacional de Huancavelica.

- La tesis [4], se enfoca en el problema del estado actual de la seguridad de la información en la red que carece de políticas y controles eficientes. También, se presenta perdida de información por la actividad de intrusos externos a la organización, por acceso fraudulentos o por accesos no autorizados. Por lo tanto, se plantea la implementación de la red, la misma que permitirá minimizar la perdida de información en la Municipalidad de Paita.

- La tesis [5], Ugarte L. en el 2016 en su tesis titulada "Implementación de un sistema de administración de redes usando plataformas de software libre para mejorar el servicio de internet inalámbrico en la ciudad de Tayabamba-Pataz" menciona que Actualmente, los sistemas de telecomunicaciones y las redes están experimentando una gran evolución tecnológica, especialmente en el ámbito de las comunicaciones móviles, las comunicaciones inalámbricas e Internet. Sin embargo, la ubicación de áreas extensas y poblaciones dispersas en zonas rurales como en el caso de la localidad de Tayabamba en Perú, que está situada en una zona montañosa a muchos kilómetros de distancia de la ciudad de Trujillo, dificulta la implementación de estas soluciones. En esta localidad, es casi imposible contar con servicios de telefonía fija, televisión por cable o conexión a Internet de banda ancha mediante cable ADSL o fibra óptica, por lo que el acceso a Internet se da a través de enlaces satelitales muy costosos y lentos. La tesis "Implementación de un sistema de administración de redes usando plataformas de software libre para mejorar el servicio de internet inalámbrico en la ciudad de Tayabamba-Pataz" tiene como objetivo mejorar el servicio de internet inalámbrico y el acceso a la red de manera más rápida y eficiente. Se utilizarán plataformas tecnológicas basadas en software libre (Linux), y se optará por la tecnología Mikrotik (RouterOS basado en Linux), que es una poderosa herramienta para la administración de redes, y brinda seguridad, calidad de servicio (QoS), estabilidad y rapidez. Además, se implementará el alojamiento web caché a través de Thunder Cache, un sistema de

cacheo web basado en Linux (FreeBSD) que permite almacenar contenido web con URL dinámico y mejora la velocidad de navegación y ahorra ancho de banda de Internet.

- En la tesis [6], En el 2018 Rojas Mattos José Leoncio, desarrolló: "Diseño y Simulación de una red basada en VLAN's para mejorar la comunicación de datos en la empresa Grupo El Saber S.A.C" Este estudio investigativo tiene como objetivo mejorar la comunicación de datos en la empresa Grupo el Saber a través de un diseño y simulación de un sistema de cableado estructurado. Se utilizó un enfoque experimental y pre-experimental, manipulando la variable independiente mediante un pre y post test. La población total era de 72 Broadcast diarios. Se siguió la metodología de redes de Errol Simón y se utilizó la herramienta de simulación de red Cisco Packet Tracer. Al comparar el sistema actual con el diseño propuesto de las VLAN, se encontró una reducción del 83.47% en el tiempo promedio de transferencia de datos, un nivel de seguridad en los dispositivos de comunicación mejorado en 8.40, y una disminución en la tormenta de Broadcast generados en la red de datos en un 97.24%.

- En la tesis [7], En el 2018 Doodicio Corpus Chávez desarrolló: "Diseño de la red de comunicaciones para mejorar la transmisión de datos de la municipalidad distrital de Chavín de Huántar, provincia de Huari – Áncash 2018" la cual resume lo siguiente: El objetivo de esta investigación es mejorar la comunicación de datos en la municipalidad de Chavín de Huántar, debido a los muchos errores en el diseño y la conectividad de la red antigua que se ha ido agravando con el tiempo y el aumento de oficinas. Se busca hacer un diseño adecuado a las necesidades de la municipalidad para acelerar la transmisión de datos y ayudar a los funcionarios a trabajar de manera más eficiente y sin estrés laboral, para poder atender a los usuarios que necesitan tramitar sus documentos. La tesis busca mejorar una institución pública en su manejo de información y ajustarse a las exigencias tecnológicas de la actualidad, sin presentar problemas en su red de comunicación de datos.

- En la tesis [8], En el 2020 Morón P. desarrolló su tesis titulada "Implementación de un centro de operaciones de red para la empresa Redycom Solutions bajo el marco de trabajo ITILv4 en la ciudad de Lima - 2019" la cual resume que en esta empresa ocurría constantes problemas en la Red, como pérdida de comunicación, pérdida de datos y lentitud, lo cual generaba a su vez la lentitud en la transferencia información y en el

desarrollo del trabajo regular. En ese sentido es investigación realizó la implementación de un centro de operaciones de Red para poder optimizar el flujo de información en la empresa, logrando obtener resultados óptimos para la empresa, y reduciendo sus problemas de comunicación y seguridad.

- En la tesis [9], Fuerte R. (2021) desarrolló su tesis titulada: Diseño de un sistema de monitoreo de red LAN para una empresa Pyme, para mejorar la disponibilidad y la gestión de red, tomando como referencia el modelo de gestión de red en OSI, en donde resume lo siguiente: En este informe se describe la implementación de un sistema de monitoreo y gestión para una pequeña empresa mediante el uso de software libre u Open Source. El objetivo es optimizar la red y mejorar la disponibilidad de servicios y productos, así como reducir el tiempo de solución de problemas que se presentan a diario en la empresa. La empresa no tenía un sistema de monitoreo y gestión de incidencias, lo que hacía que el tiempo de solución de cada fallo fuera de 4 horas a 1 día. Solo el equipo Router estaba siendo monitoreado por el proveedor de servicios, lo que causaba un retraso en la identificación de problemas y sus gestiones de la red, y para facilitar el monitoreo por parte del administrador de red sin tener que gastar en un software profesional de membresía.

- En la tesis [10], Valladares G. en el 2019 desarrolló su tesis titulada “Influencia del cableado estructurado en la plataforma de comunicaciones de voz - Programa Juntos Cerro de Pasco. Universidad nacional Daniel Alcides Carrión. 2019” la cual menciona lo siguiente: Este informe examina y analiza cómo el cableado estructurado afecta la plataforma de comunicaciones de voz y datos en la Oficina del Programa Nacional de Apoyo Directo a los Más Pobres Juntos - Unidad Territorial Pasco. Se define técnicamente qué es el cableado estructurado, incluyendo su conectividad, conectores y distribución, con el objetivo de analizar cada una de estas características. Los resultados indican una relación directa entre el rendimiento de las señales medidas en paquetes por segundo (PPS) en las comunicaciones de cada terminal con la infraestructura de red a través del cableado estructurado.

2.1.2. Antecedentes Internacionales

- La tesis [11], aborda el problema de la infraestructura tecnológica en la que no cuenta con ningún diseño integrado de red por ello se determina la cantidad de estación es de trabajo, identificar y establecer las necesidades de cada área., para mejorar el servicio debe contar con todo el equipo de red y de uso final con la arquitectura de Cliente – Servidor, permitiendo la distribución de información de manera eficiente y en tiempo real.

- La tesis [12], se enfoca en el problema de reorganización de la red de voz y datos con calidad de servicios y tecnologías de voz sobre IP por la falta de uso de estándares y normas generales en el diseño de la Red de Área Metropolitana (MAN), así mismo la ausencia de protocolos y servicios de calidad que distribuyan de manera eficiente el tráfico de datos. Se plantea el objetivo de rediseñar la red con calidad de servicio para datos y voz sobre IP en el ilustre Municipio de Ambato - Ecuador.

- La tesis [13], aborda en el problema de interconectividad en las estudiantes de del centro, debido a las peculiaridades físicas del centro, formado por dos edificios independientes, el centro contara con una red local de ancho de banda de 1 Gbps que establecerá a todo los servicios que podrá acceder hoy y en futuras posibles ampliaciones, así mismo se conectaran equipos de cómputo en las aulas y otras estancias para su mejor uso y adecuado del diseño de infraestructura de redes y soporte informático en Madrid.

- La tesis [14], Se enfoca en el problema de infraestructura actual, la congestión en cierto servicio de la red en algún momento del día, así mismo la perdida de conectividad entre ciertas sedes y la administración de direcciones de red y servicios, etc. Este proyecto permitirá actualizar y proyectar la infraestructura de red de la organización a fin de cumplir con las metas estratégicas planteadas para tener un mayor control y disponibilidad en la red en SYC S.A en Bucaramanga.

- La tesis [15], Se sitúa en el ámbito de servicios de red que resuelve la necesidad de la entidad a fin de contar con una solución tecnológica que permita monitorear y gestionar la infraestructura industrial de redes de datos entre equipos activos influyendo la seguridad de los mismos. Así mismo las herramientas informáticas utilizadas en su

implementación y las normativas, estándares y buenas prácticas de gestión de las redes de datos y seguridad en la Empresa Eléctrica de Quito.

- La tesis [16], Aborda el problema del avance de la tecnología se proporciona a las personas la capacidad de compartir cantidad de información digital a través de correos electrónicos y otros medios de comunicación, gran parte de información contiene incrustados datos, conocidos como metadatos, los que indirectamente revelan información falsa, amenazas y desvió de información privada por lo que es un potencial riesgo para todos, por lo tanto se aplica eliminar lo metadatos de ciertos archivos, brindara protección ante correos electrónicos provenientes de dominios maliciosos y evitara que se envíen correos sin autorización por la seguridad de las personas. Managua - Nicaragua.

- La tesis [17], cordero P, Marcillo E. en el 2018 desarrollaron su tesis titulada "Propuesta de diseño de la data center y reestructuración de la red de datos de la universidad estatal de bolívar" la cual resume lo siguiente: En el proyecto de titulación se aborda el análisis de los datos de la red y el centro de datos de la Universidad Estatal de Bolívar con el objetivo de reestructurar la red y mejorar su diseño. Se utilizó la metodología PPDIOO y Top-Down para este propósito y se implementó una zona desmilitarizada (DMZ) y el modelo de 3 capas en la red de datos. Se empleó un simulador OPNET para comparar la red inicial con la propuesta y evaluar el tráfico generado por los servidores. También se realizaron presupuestos y análisis de factibilidad técnica y económica para elegir la solución más viable que asegure la disponibilidad, seguridad y escalabilidad de la red de la Universidad Estatal de Bolívar.

- En la tesis [18], en el 2019 John Raúl Oliva Cuevas, desarrolló su tesis titulada "Aplicación de metodología para el diseño e implementación de redes de campus universitario" el cual menciona que El presente trabajo de tesis tiene como objetivo principal hacer una contribución a la Facultad de Ciencias Físicas y Matemáticas (FCFM) al proporcionar una guía con las mejores prácticas para el diseño de Redes de Campus. Para lograr este objetivo, se analizan y aplican diferentes metodologías para el diseño, licitación e implementación de proyectos de tecnología de redes de campus. El objetivo es diseñar redes de campus que sean sostenibles, escalables y seguras, y especificar los requerimientos técnicos y comerciales para la licitación. Las

metodologías utilizadas han sido validadas en el mercado y respondieron favorablemente a los modelos planteados. La tesis propone una solución innovadora para la infraestructura de red de la Universidad de Chile, con un valor agregado en comparación con la infraestructura actual, y con posibilidades de investigación futura.

- En la tesis [19], en el 2017 Iturralde Piedra, Daniel Esteban y Lazo Vélez, Cristian Esteban desarrollaron su tesis titulada: Implementación de un Laboratorio de Redes de Telecomunicaciones utilizando Infraestructura Mikrotik. Este proyecto combina investigación y formación, y tiene como objetivo diseñar e implementar un laboratorio de redes y un manual de prácticas para los estudiantes y el profesorado. Ofrece un entorno de aprendizaje real en el área de redes y demuestra que, siguiendo los protocolos y estándares universales, se pueden usar equipos alternativos a las marcas dominantes en proyectos tecnológicos. Se han desarrollado una serie de prácticas basadas en una estructura de red modelo, que permiten implementar diferentes servicios de red para conmutación y enrutamiento, estableciendo así las bases para futuros avances.

- En la tesis [20], en el 2019 Felipe Orozco Portillo desarrolló su tesis titulada: Instalación de una red 802.11n de largo alcance que provea servicios de Internet a la Escuela Telesecundaria: “María Montessori”, y servicios de Telemedicina a localidades del Municipio de Ometepec, Gro. La tesis describe un proyecto que consistió en la creación de una red inalámbrica de larga distancia en la escuela Telesecundaria "María Montessori" en la comunidad indígena Amuzga de Arroyo de Barranca Honda, en el municipio de Ometepec, en el estado de Guerrero. En el primer capítulo se describen las características de la comunidad, la historia del lugar, el problema que se pretende abordar y los objetivos, hipótesis, alcances y limitaciones del proyecto. El capítulo 2 presenta el estado del arte, incluyendo investigaciones relacionadas y artículos de revistas relevantes. El capítulo 3 se centra en los conceptos teóricos utilizados en el proyecto, mientras que el capítulo 4 detalla la metodología empleada. Finalmente, en el capítulo 5 se presentan los resultados obtenidos y las conclusiones finales.

2.2. Marco Conceptual

2.2.1. Introducción Networking

Una red informática según [21], se define un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo. Asimismo, hay mensajes, que es lo que estos roles intercambian. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares siendo el más extendido de todos los modelos TCP/IP, basados en el modelo de referencia o teórico OSI. De la definición anterior podemos identificar los actores principales de toda la red informática.

2.2.2. Modelo TCP/IP

En las dos décadas desde su invención, la heterogeneidad de las redes se ha expandido aún más con el despliegue de Ethernet, Token Ring, Interfaz de datos distribuidos por fibra (FDDI), X.25, Frame Relay, Servicio de datos multimegabit conmutado (SMDS), Servicios integrados digitales (ISDN) y, más recientemente, Modo de transferencia asíncrono (ATM). Los protocolos de Internet son el enfoque mejor probado para interconectar esta diversa gama de tecnologías LAN y WAN.

El conjunto de protocolos de Internet incluye no solo especificaciones de nivel inferior, como el Protocolo de control de transmisión (TCP) y el Protocolo de Internet (IP), sino también especificaciones para aplicaciones comunes como el correo electrónico, la emulación de terminales y la transferencia de archivos. Para obtener información sobre el modelo de referencia OSI y la función de cada capa, consulte el documento Conceptos básicos de interconexión de redes.

Los protocolos de Internet son el conjunto de protocolos de múltiples proveedores más implementado en la actualidad. El soporte para al menos una parte del conjunto de protocolos de Internet está disponible en prácticamente todos los proveedores de computadoras.

2.2.3. Clasificación de redes

Las clasificaciones de red se determinaron de acuerdo y se muestran en la figura 2.1 y estos son los siguientes, ver [21].

PAN

Según [21], la red de área personal (Personal Área Network), está conformada por dispositivos utilizados por una sola persona. Tiene un rango de alcance de unos pocos metros de distancia.

LAN

La red de área local (Local Área Network); está compuesta por dispositivo como celulares, notebooks, computadoras de escritorio, routers, módems, switches, televisores inteligentes, consolas de videojuegos, impresoras, etc. Como medio de transporte puede utilizar tecnologías inalámbricas, como Wi-Fi, cable coaxial o UTP; o combinaciones de más de una tecnología en particular. Las definiciones del alcance máximo entre 1 km y 5 km, pero no suelen superar los 200 metros.

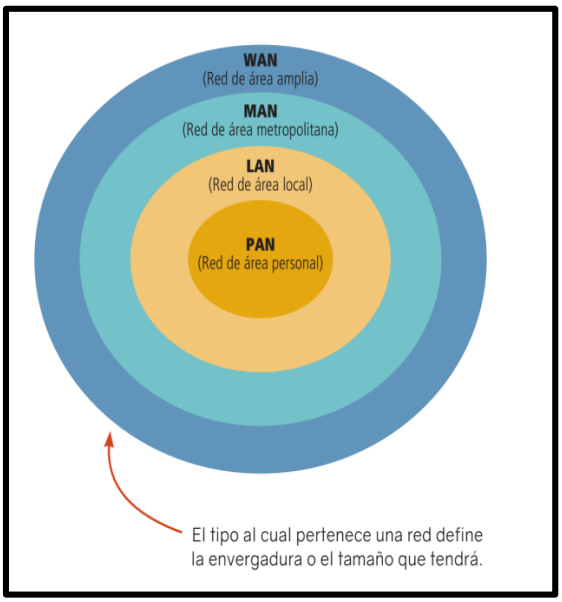


Figura 2.1: clasificación de redes. [21]

MAN

En la red de área metropolitana (Metropolitana Área Network); es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica más extensa que un campus, pero limitada.

WAN

La red de área amplia (Wide Área Network); se extiende sobre un área geográfica extensa empleando medios de comunicación poco habituales, como satélites, cables interoceánicos, fibra óptica, etc. Utiliza medios públicos.

2.2.4. Topologías de red

La topología de red, está determinada, únicamente por la naturaleza de las conexiones entre los nodos y la disposición de estos. La distancia entre los nodos, las tasas de transmisión y los tipos de sales no pertenecen a la topología de la red, aunque pueden verse afectados por ella.

Se debe seleccionar una que nos ayude a minimizar los costos de enrutamiento de datos, nos ofrezca una mayor tolerancia a fallos y facilidad de localización de estos y sea sencilla de instalar y de configurar.

a) Topología bus.

Topología bus se muestra en la figura 2.2 y consiste en que todos los nodos están conectados directamente por medio de enlaces individuales, un enlace especial denominado bus o backbone, este bus, por lo general, es un cable que posee un terminador de cada extremo; es decir, una resistencia [21].

Ventajas:

- Fácil conectar un nuevo dispositivo
- Fácil de extender o escalar
- Requiere menos cableado.

Desventajas:

- Afectada a todo si se produce un error o ruptura.
- Rendimiento decae a medida que se conectan más dispositivos.
- Es difícil detectar fallos.

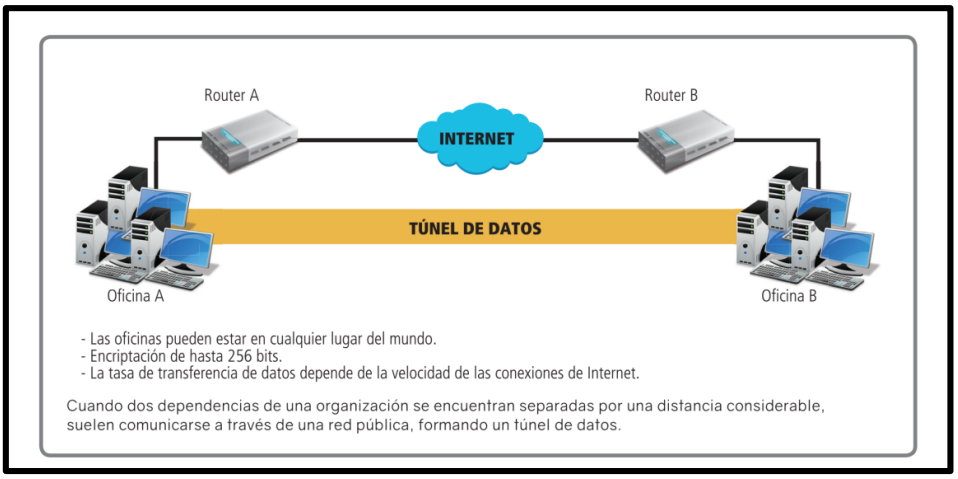


Figura 2.2: topología bus de datos [21]

b) Topología anillo

En [21], menciona que en la topología anillo, los nodos están conectados unos con otros formando un circulo o anillo (el ultimo nodo se conecta con el primero para cerrar el círculo.) la información solo fluye en una sola dirección.

Ventajas:

- No requiere enrutamiento.
- Es fácil de extender, ya que los nodos se encuentran diseñados como repetidores para ampliar la señal.

Desventajas:

- Cuando un nodo falla puede provocar la caída de toda la red.
- Existe dificultades para detectar fallos.

c) Topología estrella

Según [21], la topología estrella es una red donde todos los nodos se conectan a un nodo central denominado concentrador. Por lo general, un concentrador suele ser un hub o un switch. La información fluye de cualquier de los posibles emisores hacia el concentrador. Esta topología se muestra en la figura N° 2.3.

Ventajas:

- Facilidad de implantación.
- Facilidad para detectar fallos.

Desventajas:

- Un fallo en el nodo central provoca la caída de toda la red.
- Requiere enrutamiento.
- En rendimiento decae a medida que se conectan más dispositivos a la red.

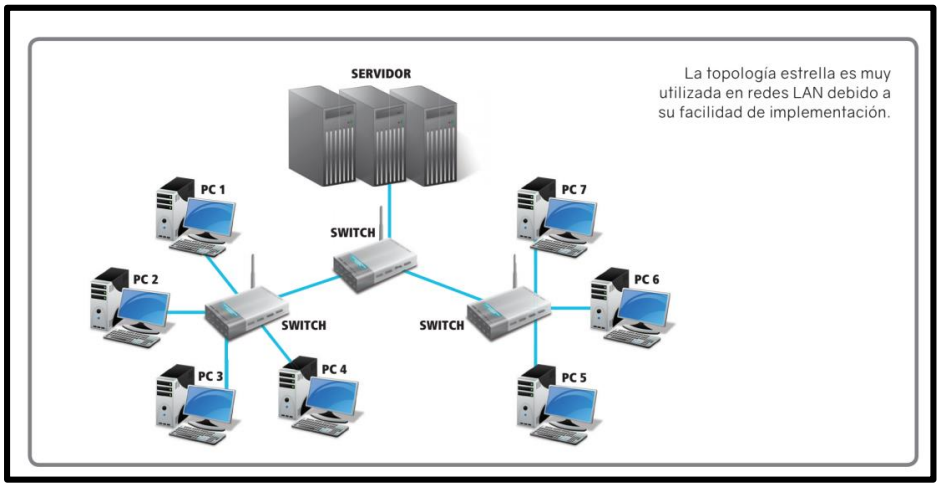


Figura 2.3: topología estrella [21]

d) Topología árbol

En [21], se explica cómo la topología árbol está compuesta por más de un nodo central o concentrador dispuesto de manera jerárquica. Todos los nodos centrales de una red árbol deben estar conectados entre sí.

Ventajas:

- Facilidad de implementación.
- Podemos desconectar nodos sin afectar la red.
- Facilidad para detectar fallos.

Desventajas:

- Requiere enrutamiento.
- El rendimiento decae con más dispositivos conectados a la red.

e) Topología Malla completa.

En [21], se explica cómo cada nodo que forma parte de la red posee un enlace punto a punto, individual y exclusivo con cada uno de los demás nodos que también integran la red.

Ventajas:

- Tolerancia a fallos.
- Desconexión de nodos sin afectar a toda la red.
- Aporta privacidad en la comunicación entre nodos.

Desventajas:

- Es costosa y compleja de implementar.
- El mantenimiento resulta costoso.

f) Topología celda o red celular.

En [21], nos menciona que esta topología se encuentra compuesta por áreas circulares o hexagonales, cada una de las cuales posee un nodo en el centro.

g) Topología mixta.

Esta topología es una combinación de dos a más de las mencionadas anteriormente las combinaciones más comunes dentro de esta clasificación son estrella - bus estrella – anillo.

2.2.5. Seguridad de datos

a) Importancia de la seguridad de datos.

Según [22], la seguridad de datos es la práctica de proteger la información digital ante accesos no autorizados, corrupción o robos a lo largo de todo su ciclo de vida. Es un concepto que abarca todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye políticas y procedimientos de la organización.

b) Tipos de seguridad de datos.

Los tipos de seguridad de datos se determinaron de acuerdo a [22], y estos son:

- **Cifrado**

En [22], se explica un algoritmo para transformar caracteres de texto normal en un formato ilegible, las claves de cifrado mezclan datos para que solo los usuarios autorizados puedan leerlos. Las soluciones de cifrado de base de datos y archivos sirven como última

línea de defensa para volúmenes sensibles ya que oscurecen su contenido a través de cifrado o tokenización. La mayoría de las soluciones también incluyen prestaciones de gestión de claves de seguridad.

- **Eliminación de datos**

En [22], más seguro que el borrado de datos estándar, la eliminación de datos utiliza software para sobrescribir completamente los datos en cualquier dispositivo de almacenamiento. Comprueba que los datos sean irrecuperables.

- **Enmascaramiento de datos**

Según [22], al enmascarar datos, las organizaciones pueden permitir a los equipos desarrollar aplicaciones o formar a personas utilizando datos reales. Enmascara información de identificación personal (PII) en los casos necesarios para que el desarrollo pueda producirse en entornos en conformidad con la normativa.

- **Resiliencia de datos**

En [22], la resiliencia está determinada por cómo una organización soporta o se recupera de cualquier tipo de fallo, desde problemas de hardware hasta cortes de electricidad o cualquier otro suceso que afecta a la disponibilidad de datos. La velocidad de recuperación es vital para minimizar el impacto.

c) Fundamentos de la ciberseguridad.

Según [27], la ciberseguridad es el conjunto de tecnologías, procesos y prácticas destinados a proteger sistemas, infraestructuras, dispositivos y datos sensibles contra ataques, usos indebidos y amenazas cibernéticas.

En [27], el Centro de Investigación y Seguridad en Tecnologías de la Información (CERT-UNAM), la ciberseguridad es el mantenimiento de la confidencialidad, integridad y disponibilidad de la información y de los sistemas de información en el ciberespacio.

Los tres pilares de la seguridad.

Los tres pilares de seguridad se muestran en la figura 2.4 y estos son los siguientes:

- **Confidencialidad:**

Consiste en asegurar que solo el personal autorizado accede a la información que le corresponde, de este modo sistema controla que un usuario solo podrá usar los recursos que necesita para ejercer sus tareas para garantizar la confidencialidad.

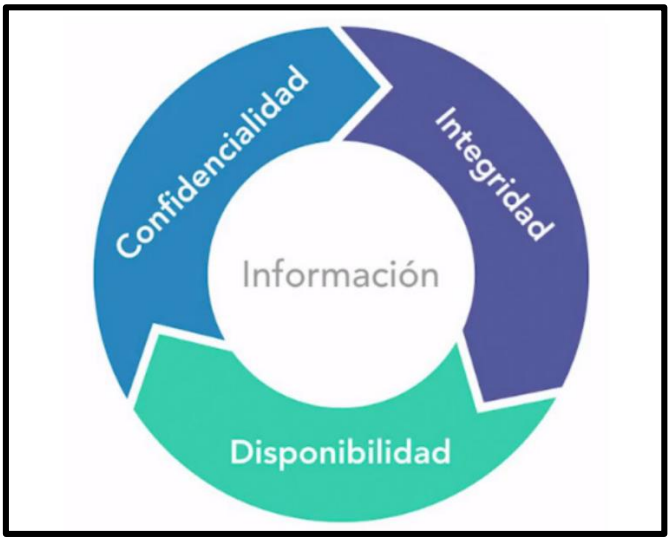


Figura 2.4: Pilares de la seguridad

- **Integridad:**

Según consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente. El hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información. De hechos, si la manipulación de la información es incorrecta puede causar que se arrastre una cadena de errores.

- **Disponibilidad:**

Para resultar una información útil y valiosa debe estar disponible para quien la necesita y se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles.

2.2.6. Teorías de las metodologías

Top-Down Network Design

El diseño de red de arriba hacia abajo es una metodología para diseñar redes que comienza en las capas superiores del modelo de referencia OSI antes de pasar a las capas

inferiores. Se enfoca en aplicaciones, sesiones y transporte de datos antes de la selección de enrutadores, conmutadores y medios que operan en las capas inferiores.

El proceso de diseño de red de arriba hacia abajo incluye la exploración de estructuras divisionales y grupales para encontrar a las personas a las que la red brindará servicios y de quienes debe obtener información valiosa para que el diseño tenga éxito. El diseño de red descendente también es iterativo. Para evitar atascarse demasiado rápido en los detalles, es importante obtener primero una visión general de los requisitos del cliente. Posteriormente, se pueden recopilar más detalles sobre el comportamiento del protocolo, los requisitos de escalabilidad, las preferencias tecnológicas, etc. El diseño de red de arriba hacia abajo reconoce que el modelo lógico y el diseño físico pueden cambiar a medida que se recopila más información. Debido a que la metodología de arriba hacia abajo es iterativa, algunos temas se cubren más de una vez en este libro. Por ejemplo, este capítulo analiza las aplicaciones de red. Las aplicaciones de red se analizan nuevamente en el Capítulo 4, "Caracterización del tráfico de red", que cubre el tráfico de red causado por patrones de uso de aplicaciones y protocolos. Un enfoque de arriba hacia abajo le permite al diseñador de la red obtener primero "el panorama general" y luego descender en espiral hacia los requisitos y especificaciones técnicas detalladas.

Uso de un proceso de diseño de red estructurado: El diseño de redes de arriba hacia abajo es una disciplina que surgió del éxito de la programación de software estructurado y el análisis de sistemas estructurados. El objetivo principal del análisis de sistemas estructurados es representar con mayor precisión las necesidades de los usuarios, que lamentablemente a menudo se ignoran o se tergiversan. Otro objetivo es hacer que el proyecto sea manejable dividiéndolo en módulos que se puedan mantener y cambiar más fácilmente. El análisis de sistemas estructurados tiene las siguientes características:

- El sistema está diseñado en una secuencia de arriba hacia abajo.
- Durante el proyecto de diseño, se pueden usar varias técnicas y modelos para caracterizar el sistema existente, los nuevos requisitos del usuario y una estructura para el sistema futuro.
- Se hace hincapié en comprender el flujo de datos, los tipos de datos y los procesos que acceden a los datos o los modifican.

- Se pone énfasis en comprender la ubicación y las necesidades de las comunidades de usuarios que acceden o cambian datos y procesos.

Metodología CISCO – PPDIOO (Prepara Plan Diseño Infraestructura Operar Optimizar).

PPDIOO significa Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. PPDIOO es una metodología de Cisco que define el ciclo de vida continuo de los servicios necesarios para una red.

Fases PPDIOO, Las fases del PPDIOO son las siguientes:

- **Preparar:** implica establecer los requisitos de la organización, desarrollar una estrategia de red y proponer una arquitectura conceptual de alto nivel que identifique las tecnologías que mejor pueden respaldar la arquitectura. La fase de preparación puede establecer una justificación financiera para la estrategia de red al evaluar el caso de negocios para la arquitectura propuesta.

- **Plan:** implica identificar los requisitos iniciales de la red en función de los objetivos, las instalaciones, las necesidades del usuario, etc. La fase del plan implica la caracterización de los sitios y la evaluación de las redes existentes y la realización de un análisis de brechas para determinar si la infraestructura del sistema existente, los sitios y el entorno operativo pueden soportar el sistema propuesto. Un plan de proyecto es útil para ayudar a administrar las tareas, responsabilidades, hitos críticos y recursos necesarios para implementar cambios en la red. El plan del proyecto debe alinearse con los parámetros de alcance, costo y recursos establecidos en los requisitos comerciales originales.

- **Diseño:** Los requisitos iniciales que se derivaron en la fase de planificación impulsan las actividades de los especialistas en diseño de redes. La especificación de diseño de red es un diseño detallado integral que cumple con los requisitos comerciales y técnicos actuales e incorpora especificaciones para respaldar la disponibilidad, la confiabilidad, la seguridad, la escalabilidad y el rendimiento. La especificación de diseño es la base para las actividades de implementación.

- **Implementar:** se construye la red o se incorporan componentes adicionales de acuerdo con las especificaciones de diseño, con el objetivo de integrar dispositivos sin interrumpir la red existente o crear puntos de vulnerabilidad.

- **Operar:** La operación es la prueba final de la idoneidad del diseño. La fase operativa implica mantener la salud de la red a través de las operaciones diarias, incluido el mantenimiento de una alta disponibilidad y la reducción de gastos. La detección de fallas, la corrección y el monitoreo del desempeño que ocurren en las operaciones diarias brindan los datos iniciales para la fase de optimización.

- **Optimizar:** Implica una gestión proactiva de la red. El objetivo de la gestión proactiva es identificar y resolver problemas antes de que afecten a la organización. La detección y corrección de fallas reactivas (resolución de problemas) es necesaria cuando la administración proactiva no puede predecir y mitigar las fallas. En el proceso PPDIOO, la fase de optimización puede provocar un rediseño de la red si surgen demasiados problemas y errores en la red, si el rendimiento no cumple con las expectativas o si se identifican nuevas aplicaciones para respaldar los requisitos técnicos y organizacionales.

Metodología por la INEI (Instituto nacional de estadística e informática)

Esta metodología adopta un marco metodológico único, el cual está conformada por las siguientes etapas: organización, análisis, desarrollo e implementación

- Organización: En esta etapa se realiza el modelamiento del requerimiento, que va depender del tipo de rede que se va implementar, la manera, la forma y todos los que el cliente requiere para su empresa, organización o lugar de trabajo.

- Análisis: en esta etapa se realiza el análisis de los recursos de la Red y la estructura, se realiza la estrategia para realizar la integración de todas las áreas a la Red, se debe considerar la topología que se va a implementar, se realiza el mapeo de cada punto, computadora y cada elemento que se va a utilizar.

- Desarrollo: en este paso se realiza el diseño y el diseño lógico de todo el proyecto, para poder tener mapeado cada uno de los enlaces, el cableado, las canaletas, etc.

- Implementación: aquí comprende la instalación de todo el proyecto, es decir el cableado completo desde la implementación de los conductos hasta el paso de los cables, la configuración y las pruebas de implementación.

Para este proyecto la metodología utilizada fue la de PPDIOO, por manejar un estándar que ya ha funcionado correctamente en anteriores proyectos de implementación.

2.3. Definición de términos

Implementación de infraestructura de redes

Uno de los conceptos fundamentales de la implementación, es que las redes, las arquitecturas y los diseños tienen en cuenta los servicios que cada red proporcionará el apoyo. Esto refleja la creciente sofisticación de las redes, que han evolucionado de proporcionar conectividad básica y rendimiento de reenvió de paquetes a una plataforma para diversos servicios.

Servicio de red

Cuando una red se ve como parte de un sistema que proporciona servicios, los sistemas funcionan bastante bien para una variedad de redes, desde pequeñas y simples a redes grandes y complejas. Ayuda a determinar, definir y describir las características y capacidades importantes en su red.

Tráfico y desempeño de la red.

- El tráfico y desempeño de la red son dos conceptos clave en la era digital en la que vivimos. Con la creciente dependencia de la tecnología y el aumento del número de dispositivos conectados a internet, la calidad de la red se ha convertido en un factor crítico para la satisfacción de los usuarios y el éxito de las empresas.

- El tráfico de red se refiere a la cantidad de datos que se transmiten a través de la red en un momento dado. El aumento del tráfico es una consecuencia directa del creciente número de dispositivos conectados a internet y del aumento del uso de aplicaciones en

línea. Si la cantidad de tráfico supera la capacidad de la red, se producirán retrasos y caídas en el servicio, lo que puede generar una experiencia insatisfactoria para los usuarios.

- Por otro lado, el desempeño de la red se refiere a la velocidad y fiabilidad de la transmisión de datos a través de la red. El desempeño de la red es crucial para garantizar una experiencia de usuario satisfactoria. Los usuarios esperan que las páginas web se carguen rápidamente, que las aplicaciones respondan de manera instantánea y que la calidad del video sea alta. Si la red no cumple con estas expectativas, los usuarios pueden perder interés y buscar alternativas que ofrezcan una mejor experiencia.

- Para mejorar el tráfico y el desempeño de la red, existen diversas estrategias que pueden ser implementadas. Una de las más efectivas es la optimización de la red, que se refiere a la implementación de tecnologías que mejoran la capacidad de la red y reducen la congestión del tráfico. Otra estrategia es la segmentación de la red, que permite dividir la red en segmentos más pequeños y administrables, lo que facilita la identificación de problemas y su resolución.

- Otras medidas incluyen la adopción de nuevas tecnologías de red, como el 5G, que ofrece velocidades de transmisión mucho más rápidas y una mayor capacidad de tráfico. También se pueden implementar medidas de seguridad, como la autenticación de usuarios y la implementación de firewalls, que protejan la red de ataques externos y reduzcan el riesgo de interrupciones del servicio.

- En conclusión, el tráfico y el desempeño de la red son dos factores críticos para garantizar una experiencia de usuario satisfactoria en la era digital. La congestión del tráfico y una red de bajo desempeño pueden generar retrasos, caídas en el servicio y una experiencia insatisfactoria para los usuarios. La optimización de la red, la segmentación de la red y la adopción de nuevas tecnologías son algunas de las estrategias que pueden ser implementadas para mejorar el tráfico y el desempeño de la red y garantizar una experiencia de usuario satisfactoria.

Comunicación y seguridad de redes

- Según [23], la seguridad de la red es un tema crítico en la era digital en la que vivimos. Con la creciente dependencia de la tecnología y la gran cantidad de datos confidenciales que se transmiten a través de la red, la seguridad de la red se ha convertido en un factor clave para la protección de la privacidad y la seguridad de los usuarios.

- La seguridad de la red se refiere a la protección de la información que se transmite a través de la red. La información puede ser confidencial, como datos financieros o información personal, y su protección es esencial para garantizar la privacidad y la seguridad de los usuarios. La seguridad de la red también incluye la protección contra el malware y otros tipos de ataques que pueden comprometer la seguridad de la red.

- La importancia de la seguridad de la red radica en el hecho de que la información es un activo valioso que debe ser protegido. Los datos confidenciales pueden ser utilizados de manera malintencionada por hackers o delincuentes informáticos para cometer fraudes o robar información. La pérdida de información confidencial también puede tener un impacto negativo en la reputación de una empresa y la confianza de los usuarios.

- Para mejorar la seguridad de la red, existen diversas estrategias que pueden ser implementadas. Una de las más efectivas es la implementación de medidas de seguridad, como la autenticación de usuarios, el cifrado de datos y la implementación de firewalls, que protejan la red de ataques externos y reduzcan el riesgo de interrupciones del servicio.

- Otra estrategia es la educación del usuario. Los usuarios deben ser conscientes de los riesgos de seguridad y deben tomar medidas para proteger su información personal. Es importante que los usuarios utilicen contraseñas fuertes y que no compartan información personal o financiera en línea sin la debida protección.

- Otras medidas incluyen la actualización regular del software y la implementación de políticas de seguridad sólidas. Los empleados también deben ser capacitados en prácticas de seguridad y deben estar informados sobre las políticas y procedimientos de seguridad de la empresa.

- En conclusión, la seguridad de la red es un factor crítico para garantizar la privacidad y la seguridad de los usuarios en la era digital. La implementación de medidas de seguridad, la educación del usuario y la implementación de políticas sólidas son algunas de las estrategias que pueden ser utilizadas para mejorar la seguridad de la red y garantizar una experiencia de usuario segura y satisfactoria. Es importante que tanto los usuarios como las empresas tomen medidas para proteger la información confidencial y garantizar la seguridad de la red en todo momento.

La seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración. Modificación. Lectura, inspección, registro o destrucción no autorizados [23].

Administración de redes

La seguridad en la red es el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación.

Latencia

- Según [25] el tiempo de retraso entre una acción y una respuesta a esa acción se conoce como latencia. Es el tiempo transcurrido desde el momento en que se entrega un paquete desde el origen hasta el destino y el tiempo que tarda la confirmación del destino en llegar al origen en el ámbito de las redes. En este contexto, se refiere al tiempo que se tarda en ir del origen al destino y viceversa.

- Para darle un ejemplo, la latencia es la cantidad de tiempo que tarda un sitio web en cargarse después de hacer clic en la URL.

- En teoría, los datos de Internet deberían viajar a la velocidad de la luz, por lo que no debería haber retrasos. Sin embargo, la infraestructura, el equipo y, a veces, incluso la distancia entre las computadoras de origen y de destino limita su adopción. La buena noticia es que existe una variedad de métodos para reducir la latencia que, al igual que el Jitter, puede influir en su experiencia en Internet.

- Echemos un vistazo a algunos conceptos relacionados, como el ancho de banda y el rendimiento, que a veces se usan indistintamente con el retraso. La cantidad máxima de datos que pueden moverse a través de una red en un momento dado se denomina ancho de banda, pero la cantidad real de tráfico que pasa a través de la red se denomina rendimiento. En otras palabras, si no hay problemas de latencia, el ancho de banda permanece constante en todo momento, pero la latencia cero es casi inalcanzable, por lo que el rendimiento siempre será menor que el ancho de banda.

Jitter

- Según [25], Jitter es un fenómeno en el que los paquetes de datos se retrasan en la transmisión debido a la congestión de la red o, en casos excepcionales, a las modificaciones de la ruta. Esta es con frecuencia la fuente de retrasos en el almacenamiento en búfer en la transmisión de video, y los niveles extremos de fluctuación pueden incluso provocar llamadas VoIP interrumpidas.

- Dado que todos los paquetes entrantes tienen el mismo retraso, el primer tipo de retraso no afectaría a aplicaciones como audio y video. Sin embargo, en el segundo caso, la demora variable del paquete es inaceptable y también da como resultado que los paquetes lleguen desordenados. El término "fluctuación alta" denota una variación significativa en los retrasos, mientras que "fluctuación baja" denota un cambio menor.

- Al mismo tiempo, se considera aceptable cierta fluctuación promedio porque no interfiere con su experiencia de navegación o visualización. Una fluctuación de 30 milisegundos o menos generalmente se considera aceptable porque apenas es aparente, pero cualquier valor superior afecta su experiencia de navegación, así como sus llamadas. Sin embargo, cuando se descargan archivos, los niveles más altos de fluctuación apenas son visibles.

Ancho de banda (bandwidth)

- Según [25], el ancho de banda de la red es una medida de la tasa de transferencia de datos o la capacidad de una red determinada. Es una medida de red crucial para comprender la velocidad y la calidad de una red.

- El ancho de banda de la red se suele medir en bits por segundo (Bps). En la práctica, las organizaciones y los proveedores de servicios de Internet (ISP) miden el ancho de banda en megabits por segundo (Mbps) o gigabits por segundo (Gbps).

2.4. Hipótesis

2.4.1. Hipótesis General

La implementación de infraestructura de redes permitirá mejorar la comunicación y seguridad de datos en la UGEL Huanca Sancos.

2.4.2. Hipótesis Específica(s)

- La implementación de infraestructura de redes, mejora el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos.
- La implementación de infraestructura de redes, aumenta la seguridad de la red en la UGEL Huanca Sancos.
- La implementación de infraestructura de redes, mejora la comunicación y seguridad de la red en la UGEL Huanca Sancos. Esto se realizó en base a los requerimientos de la institución en estudio.

2.5. Variables

2.5.1. Definición conceptual de la variable

Las definiciones que establecemos se enmarcan dentro de la problemática planteada para la investigación.

- **Implementación de infraestructura de redes**

Es el proceso que permite la descripción formal de los elementos de hardware y software de la red, incluyendo su arquitectura en modo de operación para la productividad de la UGEL Huanca Sancos.

- **Comunicación y Seguridad de datos**

Es el proceso que permite que se pueda compartir datos entre los usuarios autorizados conectados a la red garantizando la integridad e inviolabilidad de los mismos.

2.5.2. Definición operacional de variable

a) Variable Independiente (VI) Implementación de Infraestructura de Redes

Implementación de infraestructura de redes es el desarrollo del cableado estructurado en la UGEL, la cual mantendrá una estructura que permitirá y garantizará la comunicación fluida de la información por cada uno de los puntos instalados.

Dimensiones de implementación de infraestructura de red

- Confiabilidad de redes, refleja la capacidad de mantener operativa frente a posibles fallos de algunos componentes.
- Capacidad de red, es una medida de la capacidad del sistema para transferir información, (voz, datos, video, combinaciones de estos).

Indicadores de las dimensiones

- Frecuencia de fallas de la red y sus componentes que representa las interrupciones no programadas del servicio.
- Capacidad de transmisión de ancho de banda y rendimiento.

b) Variable Dependiente (VD) Comunicación y Seguridad de Datos

En la UGEL Huanca Sancos, la comunicación y seguridad de datos se desea proteger adecuadamente su red, lo cual se aplicará una política de la seguridad en ejecución cualquier actividad diseñada para proteger el acceso, el uso de la integridad de la red y los datos corporativos de la institución.

Dimensiones de la comunicación y seguridad de datos

- **Tráfico de la red**

El tráfico de red se refiere a la cantidad de datos que se transmiten a través de la red en un momento dado. El aumento del tráfico es una consecuencia directa del creciente número de dispositivos conectados a internet y del aumento del uso de aplicaciones en línea. Si la cantidad de tráfico supera la capacidad de la red, se producirán retrasos y caídas en el servicio, lo que puede generar una experiencia insatisfactoria para los usuarios.

- **Seguridad de la red**

La seguridad de la red se refiere a la protección de la información que se transmite a través de la red. La información puede ser confidencial, como datos financieros o

información personal, y su protección es esencial para garantizar la privacidad y la seguridad de los usuarios. La seguridad de la red también incluye la protección contra el malware y otros tipos de ataques que pueden comprometer la seguridad de la red.

Indicadores de las dimensiones de tráfico de red

- **Nivel de latencia**

Es un término utilizado para describir la cantidad de tiempo que tarda un paquete en transferirse a su destino.

- **Retraso de envío de paquetes (Jitter)**

Es el retraso que varía con el tiempo cuando la señal se desvanece o tiembla.

Indicadores de las dimensiones seguridad de la red

Índice de detección de intrusiones

Mide la capacidad de la red para detectar y responder a posibles intrusiones y se puede calcular como el número de intrusiones detectadas y respondidas dividido por el número total de intrusiones.

2.5.3. Operacionalización de variable

En la siguiente tabla 2.1 podemos observar la definición de, dimensiones, indicadores y el instrumento usado para los variables independientes y dependientes.

VARIABLES	DEFINICION	DIMENSIONES	INDICADORES	INSTRUMENTOS
VARIABLE INDEPENDIENTE **(Implementación de infraestructura de redes)**	Es el proceso que permite la descripción formal de los elementos de hardware y software de la red, incluyendo su arquitectura en modo de operación para la productividad de la UGEL Huanca Sancos.	Confiabilidad	Frecuencia de fallas	Ficha de recolección de datos
		Capacidad	Capacidad de transmisión	Ficha de recolección de datos
VARIABLE DEPENDIENTE **(Comunicación y seguridad de datos)**	Es el proceso que permite que se pueda compartir datos entre los usuarios autorizados conectados a la red garantizando la integridad e inviolabilidad de los mismos.	Trafico de la red	- Latencia - Retraso de envio de paquetes (jitter)	Ficha de recolección de datos
		Seguridad de la red	Detección de intrusiones	Ficha de recolección de datos

Tabla 2.1: Opercionalización de variable

CAPITULO III
METODOLOGIA

3.1. Método de investigación

Luego de analizar y estudiar la bibliografía relacionado a los métodos de la investigación existentes nos encontramos con una variedad de clasificaciones, pero se pudo llegar a la conclusión de que en esta investigación se ha utilizado el método deductivo para definir los problemas a partir de la amplia problemática de la institución; el método inductivo para definir y generalizar los conocimientos de la hipótesis, ya que se interactuara con la realidad para validar la hipótesis; y el método analítico sintético para diseñar el sistema de red que se plantea.

3.2. Tipo de investigación

Nuestra investigación es de tipo cuantitativo tecnológico debido a que se realizará algunas mediciones para probar las relaciones de las variables, y para descubrir como diseñar e implementar un artefacto artificial que en nuestro caso será la infraestructura de red en la organización.

3.3. Nivel de investigación

De acuerdo a las preguntas de investigación planteadas en la presente Investigación, el nivel de investigación será explicativa porque se busca establecer una relación causal. En relación a los niveles de investigación tecnológica, se definen dentro del marco de la investigación holística, donde el nivel de investigación para proponer diseños es proyectivo [24].

3.4. Diseño de investigación

Según [24] de acuerdo a las variables de la investigación que se usarán, serán los diseños experimentales, debido a que se manipulan deliberadamente una o más variables independiste para observar su efecto y relación con una o varias dependientes.

Se realizó según a la situación problemática las pruebas (antes y después de la implementación del sistema de red) mediante las fichas de recolección de datos para la investigación.

3.5. Población y muestra

La población que será investigada para probar la hipótesis serán los puntos instalados a la red actual que son usadas por lo que laboran en las diversas áreas de la UGEL Huanca Sancos que cumplen las diferentes funciones tecnológicas como pedagógicas y administrativas. Es decir, los 120 puntos. La muestra se tomará de esta población.

Muestra:

Para determinar el tamaño adecuado de la muestra, se utilizará la siguiente formula estadística para población finita:

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

N= tamaño de la población = 120

Z= 1.96 para nivel de confianza del 95%

E= 0.05 error estándar.

P= 0.50 probabilidad de éxitos.

Q= 0.50 probabilidad de fracaso.

Probabilístico /// Aleatorio simple

Remplazando los valores de la formula, se tiene como tamaño de muestra n=92

$$n = \frac{120 * 1.96^2 * (0.5) * (0.5)}{(0.05)^2(120-1) + (1.96)^2 * (0.5) * (0.5)} = 91.62 \approx 92$$

El muestreo utilizado será el aleatorio simple, ya que se para la selección de la muestra no se está realizando restricciones, es decir todos los individuos tienen la misma cantidad de probabilidad de ser seleccionado.

3.6. Técnicas e instrumentos de recolección de datos

Dentro de las técnicas para recolección de información, se utilizó la técnica del fichaje por medio de la ficha de recolección de datos, para poder recopilar toda la información de la evaluación previa a la implementación y la evaluación posterior a la implementación.

Ficha de recolección de datos

Una ficha de recolección de datos es un formulario o un cuestionario utilizado para registrar o recopilar información de una fuente específica. Se utiliza en una variedad de contextos, incluyendo investigaciones científicas, estudios de mercado, encuestas y evaluaciones.

Una ficha de recolección de datos que hemos utilizado en nuestro estudio para recopilar los datos de la UGEL 312 Huanca Sancos – Ayacucho. Para el Pre-test y como para el Post-test, se presentan en los anexos 8 y 9. Sin embargo mostramos un fragmento del detalle de nuestra ficha.

Ficha de recolección de datos Nivel de latencia

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Institución investigada	**UGEL 312 Huanca Sancos - Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de latencia**	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio del nivel de latencia (Ms)**
1	1-Jul	7280	92	79.13
2	1-Jul	7400	92	80.43
3	1-Jul	6800	92	73.91
4	2-Jul	8900	92	96.74
5	2-Jul	6700	92	72.83
6	3-Jul	9400	92	102.17
7	3-Jul	5400	92	58.70
8	4-Jul	6544	92	71.13
9	4-Jul	7400	92	80.43
10	4-Jul	6300	92	68.48
11	5-Jul	5600	92	60.87
12	5-Jul	7345	92	79.84

Tabla 3.1: Ficha de recolección de datos Nivel de latencia

En la figura 3.1 se detallan en la parte superior los datos generales de nuestra investigación cómo, nombre de empresa y otros.

En la primera columna digitamos la cantidad de ítems, en la segunda columna la fecha que recolectamos los datos, en la tercera columna tenemos la sumatoria de la latencia en Ms, en la cuarta columna la cantidad de equipos (muestra) y en la quinta y última columna el promedio de nivel de latencia en Ms.

Ficha de recolección de datos Nivel de Jitter

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Institución investigada	**UGEL 312 Huanca Sancos - Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	Nivel de Jitter	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio de nivel de jitter**
1	1-Jul	3450	91	37.91
2	1-Jul	3800	91	41.76
3	1-Jul	4120	91	45.27
4	2-Jul	4200	91	46.15
5	2-Jul	4134	91	45.43
6	3-Jul	4323	91	47.51
7	3-Jul	3989	91	43.84
8	4-Jul	3678	91	40.42
9	4-Jul	3545	91	38.96
10	4-Jul	4213	91	46.30
11	5-Jul	3908	91	42.95
12	5-Jul	3897	91	42.82

Tabla 3.2: Ficha de recolección de datos Nivel de Nivel de Jitter

En la figura 3.2 se detallan en la parte superior los datos generales de nuestra investigación cómo, nombre de empresa y otros.

En la primera columna digitamos la cantidad de ítems, en la segunda columna la fecha que recolectamos los datos, en la tercera columna tenemos la sumatoria en Ms, en la cuarta columna la cantidad de equipos (muestra) y en la quinta y última columna el promedio de nivel de Jitter en Ms.

Ficha de recolección de dato Índice de detección de intrusiones

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Institución investigada	**UGEL 312 Huanca Sancos - Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	Índice de detección de intrusiones	**MS**	IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)	
Item	**Area**	**Intrusiones detectadas**	**Intrusiones totales**	**IDI**
1	1-Jul	5	10	50.00
2	1-Jul	4	12	33.33
3	1-Jul	4	11	36.36
4	2-Jul	4	12	33.33
5	2-Jul	3	12	25.00
6	3-Jul	4	10	40.00
7	3-Jul	5	11	45.45
8	4-Jul	4	10	40.00
9	4-Jul	3	11	27.27
10	4-Jul	4	12	33.33
11	5-Jul	3	9	33.33
12	5-Jul	4	9	44.44
13	5-Jul	6	10	60.00
14	6-Jul	4	11	36.36
15	6-Jul	3	12	25.00

Tabla 3.3: Ficha de recolección Índice de detección de intrusiones

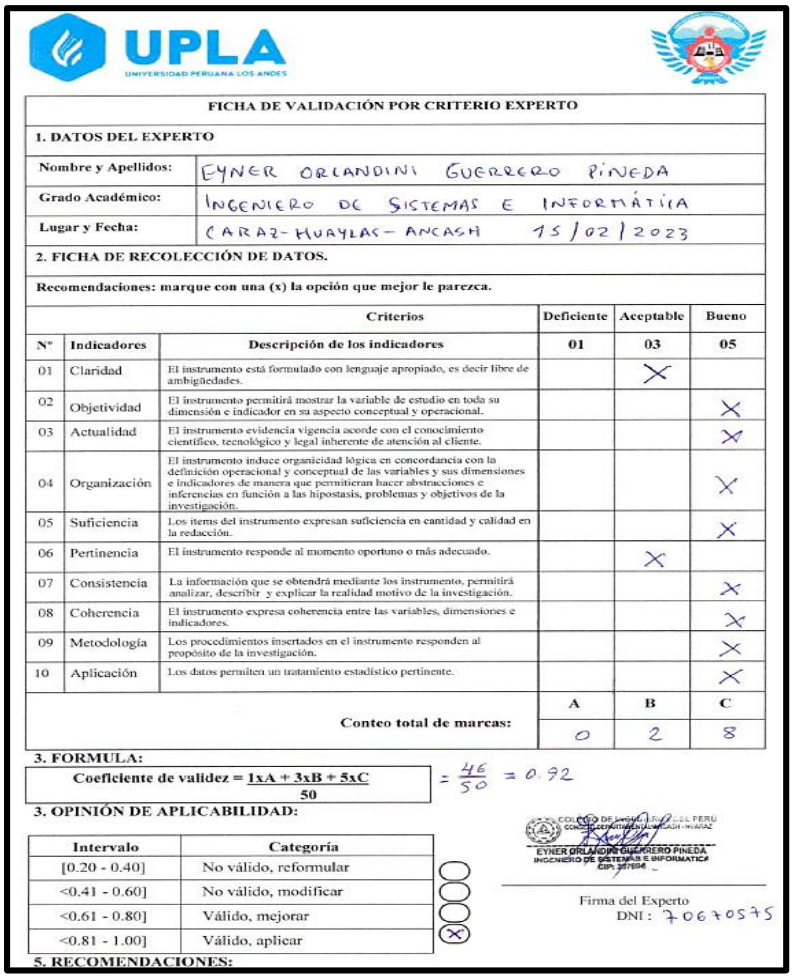
En la figura 3.3 se detallan en la parte superior los datos generales de nuestra investigación cómo, nombre de la UGEL y otros.

En la primera columna digitamos la cantidad de ítems, en la segunda columna la fecha que recolectamos los datos, en la tercera columna tenemos las intrusiones detectadas, en la cuarta columna las intrusiones totales y en la quinta y última columna el promedio de IDI.

Validez y Confiabilidad de instrumento

Validez: Según [26] manifiesta que “Grado en el que un instrumento en verdad mide la variable que se busca medir”.

El instrumento para dicho trabajo son las fichas de registro como (Ver anexo 3 y 4) fueron validadas por el juicio de dos expertos como podemos observar la Tabla 3.1.



UPLA
UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDACIÓN POR CRITERIO EXPERTO

1. DATOS DEL EXPERTO

Nombre y Apellidos:	EYNER ORLANDINI GUERRERO PINEDA
Grado Académico:	INGENIERO DE SISTEMAS E INFORMÁTICA
Lugar y Fecha:	CARAZ - HUAYLAS - ANCASH 15/02/2023

2. FICHA DE RECOLECCIÓN DE DATOS.

Recomendaciones: marque con una (x) la opción que mejor le parezca.

			Criterios	Deficiente	Aceptable	Bueno
N°	**Indicadores**		**Descripción de los indicadores**	**01**	**03**	**05**
01	Claridad		El instrumento está formulado con lenguaje apropiado, es decir libre de ambigüedades.		X	
02	Objetividad		El instrumento permitirá mostrar la variable de estudio en toda su dimensión e indicador en su aspecto conceptual y operacional.			X
03	Actualidad		El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal inherente de atención al cliente.			X
04	Organización		El instrumento induce organicidad lógica en concordancia con la definición operacional y conceptual de las variables y sus dimensiones e indicadores de manera que permitieran hacer abstracciones e inferencias en función a las hipostasis, problemas y objetivos de la investigación.			X
05	Suficiencia		Los ítems del instrumento expresan suficiencia en cantidad y calidad en la redacción.			X
06	Pertinencia		El instrumento responde al momento oportuno o más adecuado.		X	
07	Consistencia		La información que se obtendrá mediante los instrumento, permitirá analizar, describir y explicar la realidad motivo de la investigación.			X
08	Coherencia		El instrumento expresa coherencia entre las variables, dimensiones e indicadores.			X
09	Metodología		Los procedimientos insertados en el instrumento responden al propósito de la investigación.			X
10	Aplicación		Los datos permiten un tratamiento estadístico pertinente.			X
				A	**B**	**C**
			Conteo total de marcas:	0	2	8

3. FORMULA:

Coeficiente de validez = $\frac{1xA + 3xB + 5xC}{50}$ = $\frac{46}{50}$ = 0.92

3. OPINIÓN DE APLICABILIDAD:

Intervalo	Categoría	
[0.20 - 0.40]	No válido, reformular	○
<0.41 - 0.60]	No válido, modificar	○
<0.61 - 0.80]	Válido, mejorar	○
<0.81 - 1.00]	Válido, aplicar	⊗

COLEGIO DE INGENIEROS DEL PERÚ
CONSEJO DEPARTAMENTAL ANCASH - HUARAZ
EYNER ORLANDINI GUERRERO PINEDA
INGENIERO DE SISTEMAS E INFORMÁTICA
CIP. 207696

Firma del Experto
DNI : 70670575

5. RECOMENDACIONES:

Figura 3.1: Ficha de juicio de experto

El instrumento juicio de expertos tiene la siguiente descripción.

Claridad: El instrumento está formulado de forma adecuada, es decir, libre de ambigüedades.

Objetividad: La herramienta enseña la variable de análisis en su tamaño completo y el indicador en su aspecto conceptual y operativo.

Actualidad: El instrumento prueba validez de acuerdo con el razonamiento científico, tecnológico y legal.

Organización: La herramienta induce organicidad lógica según definiciones operacionales y conceptuales de variables y sus magnitudes e índices.

Suficiencia: Los elementos de la herramienta están representados en cuanto a cantidad y la calidad de texto.

Pertinencia: La herramienta responderá en el momento más adecuado.

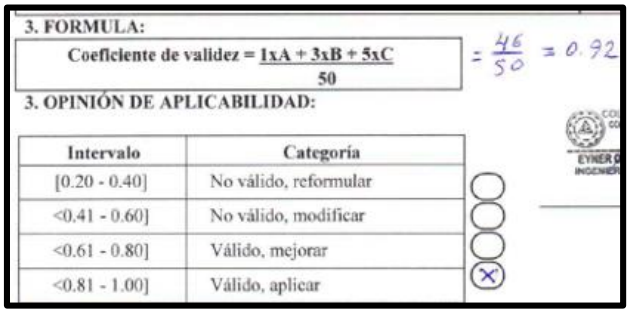
Consistencia: La información obtenida a través de las herramientas permite el análisis, explicación e interpretación de los hechos que fundamentan la investigación.

Coherencia: Esta herramienta muestra consistencia entre variables, dimensiones y criterios de encuesta.

Metodología: Los procesos integrados en la herramienta cumplen con nuestros objetivos de investigación.

Aplicación: Estos datos permiten un procesamiento estadístico relevante.

Tabla 3.4: Formula y opción de aplicabilidad



3. FORMULA:

Coeficiente de validez = $\frac{1xA + 3xB + 5xC}{50}$ = $\frac{46}{50}$ = 0.92

3. OPINIÓN DE APLICABILIDAD:

Intervalo	Categoría	
[0.20 - 0.40]	No válido, reformular	○
<0.41 - 0.60]	No válido, modificar	○
<0.61 - 0.80]	Válido, mejorar	○
<0.81 - 1.00]	Válido, aplicar	⊗

El coeficiente de validez nos permite saber en qué intervalo de aplicabilidad se encuentra nuestro instrumento. El coeficiente de validez se aplica usando la formula, como se muestra en la Tabla 3.4

Confiabilidad:

De acuerdo a este autor [26], la confiabilidad se refiere a la consistencia y estabilidad de un resultado o medición. En otras palabras, se refiere al grado en que un resultado o medición es preciso y seguro. En investigación y estadística, la confiabilidad también se puede referir a la estabilidad de los resultados obtenidos a lo largo del tiempo o al repetir una medición. Y se mide por medio de la evaluación del test y retest.

Confiabilidad Test-Retest

El Test-Retest "es la medida que son aplicadas 2 o más veces a un mismo conjunto de personas o casos, después de un cierto periodo de tiempo.

Para ola confiabilidad de nuestra ficha de recolección de datos, se utiliza la técnica Test-Retest para todas las herramientas, la cual se aplica del 5 agosto al 30 de agosto de 2022 para

el Test, y para Retest del 1 al 30 de septiembre de 2022; los dos periodos tienen 52 muestras La información se encuentra en el Anexo 5.

Esta prueba según requiere de un único uso, y debe resultar un coeficiente que este en el rango de 0 y 1, y cuanta más cerca este al 1 se demuestra que el resultado tiene una alta confiabilidad ver Tabla 3.5.

Tabla 3.5: Nivel de confiabilidad

Escala	Nivel
0.00 < sig. <0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Para determinar cómo hallar la correlación es necesario determinar si los datos se comportan de acuerdo a una distribución de probabilidad normal o no normal. Para lo cual probamos la normalidad de los datos.

Para nuestro caso se considera la prueba de Kolmogorov-Smirnov por que la muestra es >=50. La cual se observa en la tabla.

Confiabilidad del instrumento Indicador 1: Nivel de latencia

Procedemos a determinar la normalidad de los datos y obtener el resultado que se muestra en la tabla 3.6.

Tabla 3.6: Prueba de normalidad Test Retest Nivel de latencia

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,361	92	,000	,732	92	,000
a. Corrección de significación de Lilliefors						

Esta prueba de normalidad, se obtiene de la diferencia entre el Test y Retest. La tabla además nos indica que la significancia (sig.) es de 0,00 que significa que los datos son de distribución no Normal, y se debe usar la prueba de Spearman.

Tabla 3.7: Coeficientes de Rho de Spearman Nivel de latencia

Correlaciones				
			Nivel de latencia PRETEST	Nivel de latencia POSTTEST
Rho de Spearman	Nivel de latencia PRETEST	Coeficiente de correlación	1,000	,793**
		Sig. (bilateral)	.	,000
		N	92	92
	Nivel de latencia POSTTEST	Coeficiente de correlación	,793**	1,000
		Sig. (bilateral)	,000	.
		N	92	92
**. La correlación es significativa en el nivel 0,01 (bilateral).				

En la Tabla 3.7 el Test-Retest para nivel de latencia tiene un coeficiente de correlación de 0.793 y según la tabla tiene una confiabilidad "Aceptable".

Confiabilidad del instrumento Indicador 2 Nivel de Jitter

Tabla 3.8: Prueba de normalidad Test Retest Nivel de jitter

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA2	,059	51	,200*	,969	51	,205
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

La prueba de normalidad se obtiene de la diferencia entre el test y el Retest. La significancia obtenida es 0.200 que significa que los datos son de distribución Normal, y se debe usar la prueba de Pearson.

Tabla 3.9: Coeficientes de Pearson

Correlaciones			
		Nivel de Jitter PreTest	Nivel de Jitter Post_Test
Nivel de Jitter PreTest	Correlación de Pearson	1	,707**
	Sig. (bilateral)		,000
	N	51	51
	Correlación de Pearson	,707**	1

Nivel de Jitter Post_Test	Sig. (bilateral)	,000	
	N	51	51
**. La correlación es significativa en el nivel 0,01 (bilateral).			

En la Tabla 3.9 al realizar el Test-Retest para nivel de Jitter, el coeficiente de fiabilidad es 0.707, cerca al 1. Que es aceptable según la tabla de confiabilidad.

Confiabilidad del instrumento Indicador 3 índice de detección de intrusiones

En la tabla 3.10 se muestra la prueba de normalidad, que sale de la diferencia entre el Test y Retest. La tabla además nos indica que la significancia (sig) es de 0,06 que significa que los datos son de distribución no Normal, y se debe usar la prueba de Spearman.

Tabla 3.10: Prueba de normalidad Test retest índice de detección de intrusiones

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,149	51	,006	,926	51	,004
a. Corrección de significación de Lilliefors						

Tabla 3.11: Coeficientes de Rho de Spearman índice de detección de intrusiones

Correlaciones				
			Nivel de Jitter PreTest	Nivel de Jitter Post Test
Rho de Spearman	Nivel de Jitter PreTest	Coeficiente de correlación	1,000	,700**
		Sig. (bilateral)	.	,000
		N	51	51
	Nivel de Jitter Post Test	Coeficiente de correlación	,700**	1,000
		Sig. (bilateral)	,000	.
		N	51	51
**. La correlación es significativa en el nivel 0,01 (bilateral).				

En la Tabla 3.11 el Test-Retest para nivel de latencia tiene un coeficiente de correlación de 0.700, cerca al 1. Y según la tabla tiene una confiabilidad “Aceptable”.

3.7. Procesamiento de la información

El procesamiento de la información se realizó en dos tiempos, teniendo en cuenta que los indicadores a evaluar son: el nivel de latencia y el nivel de Jitter e índice de detección de intrusiones en primer lugar se realizó la medición de ambos niveles antes de la implementación de la nueva red, luego se realiza la implementación y después de realizar las pruebas respectivas se realiza la segunda evaluación con la implementación correctamente desarrollada. Mostramos los datos recolectados en la institución de nuestro estudio, en el anexo 06.

Tabla 3.12: Ficha de registro de datos. Nivel de latencia

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Institución investigada	**UGEL 312 Huanca Sancos - Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de latencia**	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio del nivel de latencia (Ms)**
1	1-Jul	7280	92	79.13
2	1-Jul	7400	92	80.43
3	1-Jul	6800	92	73.91
4	2-Jul	8900	92	96.74
5	2-Jul	6700	92	72.83
6	3-Jul	9400	92	102.17
7	3-Jul	5400	92	58.70
8	4-Jul	6544	92	71.13
9	4-Jul	7400	92	80.43
10	4-Jul	6300	92	68.48
11	5-Jul	5600	92	60.87
12	5-Jul	7345	92	79.84
13	5-Jul	5300	92	57.61
14	6-Jul	8400	92	91.30
92	28-Jul	6540	92	71.09

Los datos que se muestran se tabularon en el MS Excel, con la finalidad de tenerlos en un orden para poder ingresarlos al SPSS. En la Tabla 3.12 se listan las 92 muestras tabuladas del indicador nivel de latencia

Tabla 3.13: Ficha de registro de datos. Nivel de Jitter

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Institución investigada	**UGEL 312 Huanca Sancos - Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de Jitter**	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio de nivel de jitter**
1	1-Jul	3450	92	37.50
2	1-Jul	3800	92	41.30
3	1-Jul	4120	92	44.78
4	2-Jul	4200	92	45.65
5	2-Jul	4134	92	44.93
6	3-Jul	4323	92	46.99
7	3-Jul	3989	92	43.36
8	4-Jul	3678	92	39.98
[illegible]	4-Jul	[illegible]	[illegible]	[illegible]
92	28-Jul	3455	92	37.55

Los datos que se muestran se tabularon en el MS Excel, con la finalidad de tenerlos en un orden para poder ingresarlos al SPSS. En la tabla 3.13: se listan las 92 muestras tabuladas del indicador nivel de Jitter.

Tabla 3.14: Ficha de registro de datos, índice de nivel de intrusiones

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Post Test**
Institución investigada	**UGEL 312 Huanca Sancos - Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Índice de detección de intrusiones**	**MS**	IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)	
Item	**Area**	**Intrusiones detectadas**	**Intrusiones totales**	**IDI**
1		6	7	85.71
2		5	8	62.50
3		7	7	100.00
4		6	6	100.00
5		5	7	71.43
6		6	8	75.00
7		6	7	85.71
8		6	6	100.00
9		5	6	83.33
10		6	7	85.71
11		6	6	100.00

Los datos que se muestran se tabularon en el MS Excel, con la finalidad de tenerlos en un orden para poder ingresarlos al SPSS. En la tabla 3.14: se listan las 92 muestras tabuladas del indicador índice de nivel de intrusiones.

3.8. Técnicas y análisis de datos

Las técnicas de procesamiento y análisis de datos fueron las técnicas estadísticas descriptivas e inferenciales, dentro de cada una de estas se eligió las fichas de recolección de datos.

Entonces se realiza el análisis estadístico con los resultados de ambos tiempos, el primer tiempo es denominado pre test y el segundo tiempo post test, el análisis estadístico tendrá tres pasos: el primer paso será el análisis descriptivo en donde se realiza una evaluación general de los resultados y un comparativo de cada uno de ellos, el siguiente paso es la prueba de normalidad, para poder identificar la distribución de los resultados, en base al resultado si es que la distribución resulta normal, la prueba de hipótesis se realizará con la prueba T-Student, de lo contrario si la distribución resulta no normal la prueba de hipótesis será la de Wilcoxon.

Como parte del estudio los resultados obtenidos en el pre test, es resultado del proceso sin implementar la infraestructura de datos y seguridad, se comparan con los resultados obtenidos con el post test, la cual fue realizado después de la implementación la infraestructura de datos y seguridad. Se utilizaron estadísticas descriptivas como media y desviación estándar.

CAPITULO IV
RESULTADOS

4.1. Solución tecnológica

4.1.1. Metodología tecnológica

Se utilizó la metodología PPDIOO, que es una de las metodologías que da un buen beneficio en manejar la complejidad de una red en ella tenemos el crecimiento de una infraestructura, mejora la estabilidad, disponibilidad, escalabilidad y también la seguridad de la red.

A continuación, se detallan la siguiente metodología que se utilizó para la implementación.

Metodología CISCO – PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar)

PPDIOO significa Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. PPDIOO es una metodología de Cisco que define el ciclo de vida continuo de los servicios necesarios para una red.

Fases PPDIOO, Las fases del PPDIOO son las siguientes:

- **Preparar:** implica establecer los requisitos de la organización, desarrollar una estrategia de red y proponer una arquitectura conceptual de alto nivel que identifique las tecnologías que mejor pueden respaldar la arquitectura. La fase de preparación puede establecer una justificación financiera para la estrategia de red al evaluar el caso de negocios para la arquitectura propuesta.

- **Plan:** implica identificar los requisitos iniciales de la red en función de los objetivos, las instalaciones, las necesidades del usuario, etc. La fase del plan implica la caracterización de los sitios y la evaluación de las redes existentes y la realización de un análisis de brechas para determinar si la infraestructura del sistema existente, los sitios y el entorno operativo pueden soportar el sistema propuesto. Un plan de proyecto es útil para ayudar a administrar las tareas, responsabilidades, hitos críticos y recursos necesarios para implementar cambios en la red. El plan del proyecto debe alinearse con los parámetros de alcance, costo y recursos establecidos en los requisitos comerciales originales.
- **Diseño:** Los requisitos iniciales que se derivaron en la fase de planificación impulsan las actividades de los especialistas en diseño de redes. La especificación de diseño de red es un diseño detallado integral que cumple con los requisitos comerciales y técnicos actuales e incorpora especificaciones para respaldar la disponibilidad, la confiabilidad, la seguridad, la escalabilidad y el rendimiento. La especificación de diseño es la base para las actividades de implementación.
- **Implementar:** se construye la red o se incorporan componentes adicionales de acuerdo con las especificaciones de diseño, con el objetivo de integrar dispositivos sin interrumpir la red existente o crear puntos de vulnerabilidad.
- **Operar:** La operación es la prueba final de la idoneidad del diseño. La fase operativa implica mantener la salud de la red a través de las operaciones diarias, incluido el mantenimiento de una alta disponibilidad y la reducción de gastos. La detección de fallas, la corrección y el monitoreo del desempeño que ocurren en las operaciones diarias brindan los datos iniciales para la fase de optimización.
- **Optimizar:** Implica una gestión proactiva de la red. El objetivo de la gestión proactiva es identificar y resolver problemas antes de que afecten a la organización. La detección y corrección de fallas reactivas (resolución de problemas) es necesaria cuando la administración proactiva no puede predecir y mitigar las fallas. En el proceso PPDIOO, la fase de optimización puede provocar un rediseño de la red si surgen demasiados problemas y errores en la red, si el rendimiento no cumple con las expectativas o si se identifican nuevas aplicaciones para respaldar los requisitos técnicos y organizacionales.

4.1.2. Definición y especificación de requerimientos

Después de hacer el estudio de las necesidades sobre la red se pudo determinar los siguientes requerimientos:

- El requerimiento principal es reducir los problemas actuales de conectividad, velocidad, eficiencias y orden que se tiene en la UGEL Huanca Sancos.
- Reducir el nivel de Latencia que actualmente se tiene.
- Reducir el nivel de Jitter que actualmente se tiene.
- Crear una red segura en la UGEL Huanca Sancos, que permita compartir información, pero que mantenga las respectivas restricciones.
- Mejorar la transferencia de datos para mejorar el manejo de los sistemas informáticos.
- Crear una red que mantenga un orden en esa estructura y arquitectura física, con ambientes ventilados y cableado ordenado.
- Reducir las vulnerabilidades y amenazas que se tienen hacia la información.
- En la siguiente tabla 4.1 se deriva la información extraída según las necesidades de cada trabajador de la sede UGEL Huanca Sancos, teniendo un ancho de banda estandarizada para cada punto, así mismo se realiza la medición de velocidad UPLOAND y DOWLOAND por áreas y también por cada tipo de trabajo que realiza cada usuario.
- Los puntos de red que son requeridos en la UGEL Huanca Sancos, se muestra en la tabla 4.1.

Tabla 4.1: Puntos de acceso a la red UGEL Huanca Sancos

PUNTO DE ACCESO A LA RED - UGEL HUANCA SANCOS					
N°	PUNTO DE RED	UPLOAND	DOWLOAND	CONECTIVIDAD	CUMPLE
ORGANO DE DIRECCIÓN: DIRECCIÓN					
01	Directora de Programa Sectorial III	20 M	15 M	Giga Ethernet	si
02	Abogado I - Asesor Jurídico	10 M	5 M	Giga Ethernet	si
03	Secretaria I (e)	5 M	5 M	Giga Ethernet	si
04	Responsable de Mesa de Partes/Trab. Servic. II-Guardianìa	5 M	5 M	Giga Ethernet	si
05	Responsable de Certificación y Numeración (e)	15 M	15 M	Giga Ethernet	si
06	Impresora Multifuncional	768 K	768 K	Giga Ethernet	si

07	Impresora de Impacto Matricial	768 K	768 K	Giga Ethernet	si
08	Reloj Biometrico	768 K	768 K	Giga Ethernet	si
09	Impresora Personal	768 K	768 K	Giga Ethernet	si
10	Impresora Personal	768 K	768 K	Giga Ethernet	si
11	Impresora Personal	768 K	768 K	Giga Ethernet	si
12	Fotocopiadora	768 K	768 K	Giga Ethernet	si
ORGANO DE LÍNEA: ÁREA DE GESTIÓN PEDAGÓGICA					
13	Jefe del Área de Gestión Pedagógica	20 M	20 M	Giga Ethernet	si
14	Especialista en Educación Inicial	10 M	10 M	Giga Ethernet	si
15	Especialista en Educación Primaria EBR	10 M	10 M	Giga Ethernet	si
16	Especialista en Educación Primaria EBI	10 M	10 M	Giga Ethernet	si
17	Especialista en Educación Secundaria	10 M	10 M	Giga Ethernet	si
18	Especialista en Educación Secundaria - TIC	10 M	10 M	Giga Ethernet	si
19	Especialista en Educación TOE, Ed. Ambiental	10 M	10 M	Giga Ethernet	si
20	Asistente en Servicios de Educación y Cultura I	10 M	10 M	Giga Ethernet	si
21	Secretaria	5 M	5 M	Giga Ethernet	si
22	Coordinadora de PRONOEI	10 M	10 M	Giga Ethernet	si
23	Coordinadora de PRONOEI	10 M	10 M	Giga Ethernet	si
24	Coodinador RED	10 M	10 M	Giga Ethernet	si
25	Anthony	10 M	10 M	Giga Ethernet	si
26	Especialista en Convivencia	10 M	10 M	Giga Ethernet	si
27	Acompañante Pedagógico EIB -Ed. Inicial	10 M	10 M	Giga Ethernet	si
28	Acompañante Pedagógico EIB Educación Inicial	10 M	10 M	Giga Ethernet	si
29	Acompañante Pedagógico EIB-Ed. Primaria	10 M	10 M	Giga Ethernet	si
30	Acompañante Pedagógico EIB Educación Primaria	10 M	10 M	Giga Ethernet	si
31	Acompañante Pedagógico EIB -Ed. Primaria	10 M	10 M	Giga Ethernet	si
32	Responsable de CRAEI	5 M	5 M	Giga Ethernet	si
33	Responsable de Calidad de Información	5 M	5 M	Giga Ethernet	si
34	Coordinador Local PREVAED	5 M	5 M	Giga Ethernet	si

35	Impresora Multifuncional	768 K	768 K	Giga Ethernet	si
36	Router WIFI	768 K	768 K	Giga Ethernet	si
37	Impresora Personal	768 K	768 K	Giga Ethernet	si
38	Impresora Personal	768 K	768 K	Giga Ethernet	si
39	Fotocopiadora	768 K	768 K	Giga Ethernet	si
40	Fotocopiadora	768 K	768 K	Giga Ethernet	si
ORGANO DE LÍNEA: ÁREA DE GESTIÓN INSTITUCIONAL					
41	Director de Gestión Institucional / Racionalizador	10 M	10 M	Giga Ethernet	si
42	Responsable de Finanzas / Gestor Local (e)	15 M	15 M	Giga Ethernet	si
43	Responsable de Planificación	5 M	5 M	Giga Ethernet	si
44	Esp. En Monitoreo y Evaluación	5 M	5 M	Giga Ethernet	si
45	Fotocopiadora	768 K	768 K	Giga Ethernet	si
46	Impresora Personal	768 K	768 K	Giga Ethernet	si
ORGANO DE APOYO: ÁREA DE ADMINISTRACIÓN					
47	Director de Sistema Administrativo II	10 M	10 M	Giga Ethernet	si
48	Tesorero	10 M	10 M	Giga Ethernet	si
49	Contador I	10 M	10 M	Giga Ethernet	si
50	Responsable de Abastecimiento (e)	10 M	10 M	Giga Ethernet	si
51	Analista en Abastecimiento	10 M	10 M	Giga Ethernet	si
52	Trabajador de Servicio II - Limpieza	5 M	5 M	Giga Ethernet	si
53	Responsable de Caja	5 M	5 M	Giga Ethernet	si
54	Responsable de Infraestructura	5 M	5 M	Giga Ethernet	si
55	Responsable de Control Previo	5 M	5 M	Giga Ethernet	si
56	Chofer I	10 M	10 M	Giga Ethernet	si
57	Responsable de Control Patrimonial	10 M	10 M	Giga Ethernet	si
58	Técnico Informático	15 M	15 M	Giga Ethernet	si
59	Responsable de Almacèn	5 M	5 M	Giga Ethernet	si
60	Secretaria	5 M	5 M	Giga Ethernet	si
61	Impresora Personal	768 K	768 K	Giga Ethernet	si
62	Impresora Personal	768 K	768 K	Giga Ethernet	si
63	Impresora Personal	768 K	768 K	Giga Ethernet	si
64	Impresora Personal	768 K	768 K	Giga Ethernet	si
65	Fotocopiadora	768 K	768 K	Giga Ethernet	si
66	Fotocopiadora	768 K	768 K	Giga Ethernet	si
67	Fotocopiadora	768 K	768 K	Giga Ethernet	si
68	Router WIFI	768 K	768 K	Giga Ethernet	si
ÓRGANO DE CONTROL: ÁREA DE AUDITORÍA INTERNA					
69	Director de Sistema Administrativo II-Jefe de OCI	5 M	5 M	Giga Ethernet	si
OFICINA DE PERSONAL					
70	Responsable de Personal (e)	20 M	15 M	Giga Ethernet	si

71	Tèc. Administrativo I-Proyectista/Resp.Nexus	10 M	10 M	Giga Ethernet	si
72	Resp. Mov. de Personal y Escalafón (e) / SIGA	15 M	15 M	Giga Ethernet	si
73	Resp. Remuneraciones y Pensiones	15 M	15 M	Giga Ethernet	si
74	Secretario Técnico (COPROA)	5 M	5 M	Giga Ethernet	si
75	Especialista en PAD	5 M	5 M	Giga Ethernet	si
76	Secretaria	5 M	5 M	Giga Ethernet	si
77	Servidor Asistencial (Enfermera)	5 M	5 M	Giga Ethernet	si
78	Fotocopiadora	768 K	768 K	Giga Ethernet	si
79	Fotocopiadora	768 K	768 K	Giga Ethernet	si
SERVIDORES					
80	SIAF	20 M	20 M	Giga Ethernet	si
81	SIGA	20 M	20 M	Giga Ethernet	si
82	SUP	20 M	20 M	Giga Ethernet	si
83	VPN	20 M	20 M	Giga Ethernet	si
84	NEXUS	5 M	5 M	Giga Ethernet	si
85	REGISTRO RELOJ BIOMETRICO	5 M	5 M	Giga Ethernet	si
86	CHAT BIGANT	5 M	5 M	Giga Ethernet	si
87	BOLETAS DE PAGO	5 M	5 M	Giga Ethernet	si
88	WEB	20 M	20 M	Giga Ethernet	si
89	CAMARA VIGILANCIA	5 M	5 M	Giga Ethernet	si
SALA DE COMPUTO					
90	PC 01	3 M	3 M	Giga Ethernet	si
91	PC 02	3 M	3 M	Giga Ethernet	si
92	PC 03	3 M	3 M	Giga Ethernet	si
93	PC 04	3 M	3 M	Giga Ethernet	si
94	PC 05	3 M	3 M	Giga Ethernet	si
95	PC 06	3 M	3 M	Giga Ethernet	si
96	PC 07	3 M	3 M	Giga Ethernet	si
97	PC 08	3 M	3 M	Giga Ethernet	si
98	PC 09	3 M	3 M	Giga Ethernet	si
99	PC 10	3 M	3 M	Giga Ethernet	si
AUDITORIO					
100	PIZARRA INTERACTIVA	768 K	768 K	Giga Ethernet	si
101	P1	768 K	768 K	Giga Ethernet	si
102	P2	768 K	768 K	Giga Ethernet	si
103	P3	768 K	768 K	Giga Ethernet	si
104	P4	768 K	768 K	Giga Ethernet	si
105	P5	768 K	768 K	Giga Ethernet	si
106	P6	768 K	768 K	Giga Ethernet	si
107	P7	768 K	768 K	Giga Ethernet	si
108	P8	768 K	768 K	Giga Ethernet	si
109	P9	768 K	768 K	Giga Ethernet	si
110	P10	768 K	768 K	Giga Ethernet	si

Escalabilidad

Los usuarios de la entidad se conectan a internet diariamente y utilizan diferentes plataformas digitales y sistemas de información, para admitir la cantidad de usuarios en

rápido crecimiento debe ser escalable la cual se pueden conectar a internet usuarios adicionales y redes enteras sin realizar ningún cambio ni degradar el rendimiento de los usuarios existentes.

La escalabilidad en las redes informáticas proviene de las tecnologías avanzadas que se actualizan cada año que va pasando, como vemos en el siguiente diagrama se visualiza las redes implementadas en el año 2022 y así mismo las posibles redes adicionales que serán implementadas en el año 2023 o en transcurso, así mismo dicha utilidad dan la escalabilidad de toda la infraestructura de redes para mejorar la calidad de servicio y estabilidad de conectividad como se visualiza en la figura 4.1.

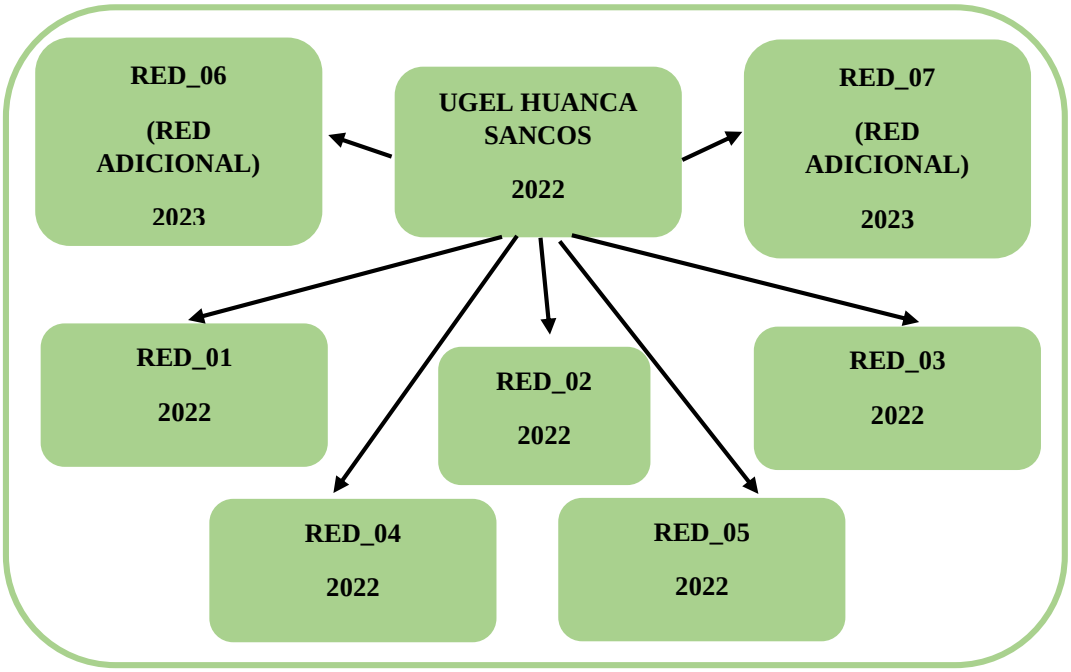


Figura 4.1: Escalabilidad de redes

Adaptabilidad

El diseño e infraestructura de redes que será implementada debe adecuarse y adaptarse a las nuevas futuras tecnologías de hardware y software. La red no debería incluir algunos elementos que limiten la implementación de nuevas tecnologías que se establece diariamente.

Definición de equipos a utilizar:

- **Mikrotik RB3011**

El RB3011 es un nuevo dispositivo multipuerto, el primero en ejecutar una CPU de arquitectura ARM para un rendimiento más alto que nunca. El RB3011 tiene diez puertos Gigabit divididos en dos grupos de conmutadores, una caja SFP y, por primera vez, un puerto USB 3.0 de tamaño completo SuperSpeed, para agregar almacenamiento o un módem 3G/4G externo.

La unidad RB3011UiAS-RM viene con una carcasa de montaje en rack de 1U, un panel LCD con pantalla táctil, un puerto de consola en serie y funcionalidad de salida PoE en el último puerto Ethernet.

El Mikrotik RB3011 se eligió este equipo de acuerdo al seguridad implementada que manejan los usuarios de la sede UGEL Huanca Sancos, así mismo los enrutadores Mikrotik necesarios con las especificaciones adecuadas que incluyen Firewall & Nat, Hotspot, Ruteo y la limitación de ancho de banda y estará ubicado en el gabinete central, punto oficial donde llega el servicio de internet fibra óptica para su respectiva configuración de seguridad de que se encuentra en la oficina de Informática de la UGEL Huanca Sancos, luego será conectado al servidor correspondiente para luego ser controlado cada punto de acceso.

La cantidad de Mikrotik es único como también necesario para la configuración del servicio internet, el control de banda ancha y seguridad de toda red de la UGEL Huanca Sancos.

Tabla 4.2: Especificaciones Mikrotik RB3011

ESPECIFICACIONES	
UPC	IPQ-8064
Recuento de núcleos de CPU	2
UPC	IPQ-8064
Recuento de núcleos de CPU	2
Frecuencia nominal de la CPU	1,4 GHz
Dimensiones	443x92x44mm
Licencia del sistema operativo del enrutador	5
Sistema operativo	enrutadorOS
Tamaño de RAM	1 GB
Tamaño de almacenamiento	128 MB
Tipo de almacenamiento	NAND
MTBF	Aproximadamente 200'000 horas a 25C
Temperatura ambiente probada	-20°C a 70°C

Aceleración de hardware IPsec	Sí
ALIMENTACIÓN	
Número de entradas de CC	2 (toma de CC, PoE-IN)
Voltaje de entrada del conector de CC	10-30 V
Consumo máximo de energía	30W
Consumo máximo de energía sin accesorios	10 vatios
Tipo de refrigeración	Pasivo
PoE en	PoE pasivo
PoE en voltaje de entrada	10-30 V
SALIDA PoE	
Puertos de salida PoE	éter10
Salida PoE	PoE pasivo
Salida máxima por puerto de salida (entrada 18-30 V)	600mA
Salida total máxima (A)	600mA
ETHERNET	
Puertos Ethernet 10/100/1000	10
PERIFÉRICOS	
Puerto de consola serie	RJ45
Número de puertos USB	1
Restablecimiento de energía USB	Sí
Tipo de ranura USB	USB 3.0 tipo A
Corriente USB máxima (A)	1

Figura 4.2: Router mikrotik

- **SWITCH TP LINK TL-SF1024D**

El Switch de 24 puertos 10/100Mbps TL-SF1024D se proporciona por un diagnostico correctivo de la sede y tiene una solución de alto rendimiento, bajo costo, fácil de usar, sin fisuras y estándar para mejorar la red antigua una la red moderna, con un ancho de banda Fast Ethernet o 10/100Mbps, Up To 200Mbps y la velocidad de 3.57Mbps de tasa de envió de paquetes que es lo necesario y suficiente para la para la conectividad de todos los usuarios de la sede UGEL Huanca Sancos. Los 24 puertos soportan auto MDI / MDIX, no hay necesidad de preocuparse por el tipo de cable, sólo tiene que enchufar y listo.

Por otra parte, con la innovadora tecnología de eficiencia energética, el TL-SF1024D puede ahorrar en el consumo de energía, así mismo este Switch se eligió generalmente por la calidad de producto, escalabilidad, el crecimiento y la fiabilidad que esto reduce las caídas de red y pérdida de productividad.

Tabla 4.3: Características de hardware switch TP Link tl-sf1024d

CARACTERISTICAS DE HARDWARE	
ESTÁNDARES Y PROTOCOLOS	IEEE 802.3i, IEEE 802.3u, IEEE 802.3x
INTERFAZ	24 puertos RJ45 a 10/100 Mbps con detección automática de velocidad (MDI/MDIX automáticos)
MEDIOS DE RED	10Base-T: cable UTP categorías 3, 4, 5 (100 metros máximo) EIA/TIA-568 100Ω STP (máximo 100 m) 100Base-Tx: cable UTP categorías 5, 5e (máximo 100 metros) EIA/TIA-568 100Ω STP (máximo 100 m)
CANTIDAD DE VENTILADORES	Sin ventilador
BLOQUEO DE SEGURIDAD FÍSICO	Si
FUENTE DE ALIMENTACIÓN	Adaptador de Corriente Externo (Salida: 9VDC/0.6A)
DIMENSIONES	(294*180*44 mm)
MONTAJE	Montaje en rack
CONSUMO DE POTENCIA MÁXIMO	3.19W(220V/50Hz)
DISIPACIÓN MÁXIMA DE CALOR	10.88BTU/h
RENDIMIENTO	
CAPACIDAD DE CONMUTACIÓN	4.8Gbps
TASA DE REENVÍO DE PAQUETES	3.57Mpps
TABLA DE DIRECCIONES MAC	8K
MEMORIA DE BUFFER	2Mb
MÉTODO DE TRANSFERENCIA	Store-and-Forward

Este tipo de Switch TP-LINK TK-SF1024D estarán ubicados en cada uno de los ambientes de toda la UGEL Huanca Sancos, la cantidad de Switch utilizados serán de 06 aproximadamente enlazados consecutivamente con la red-01, red-02, red-03, red-04, red-05.

Figura 4.3: TP-LINK TK-SF1024D

- **D-LINK 1016A**

Este Switch provee 16 puertos con soporte NWAY. Las puertas tienen la capacidad de negociar las velocidades de red entre 10 BASE-T, 100BASE-TX Y 1000NASE-TX como también el modo de operación en Half o Full Duplex (para 10 y 100Mbps)

Este tipo de Switch D-LINK 1016A estarán ubicados en algunos ambientes de toda la UGEL Huanca Sancos.

Este tipo de Switch se eligió por un análisis y diagnóstico profundo en la sede UGEL Huanca Sancos por el responsable de informática, contabilizando la cantidad de usuarios que son beneficiados, realizando los cálculos respectivos según la muestra de los puntos de acceso en cada ambiente.

La cantidad de Switch utilizados serán de 04 aproximadamente enlazados consecutivamente con la red adicional y en los ambientes que sea necesario para poder compartir algún punto de red o adicional, completamente necesario por la calidad y escalabilidad necesario y preciso para la sede UGEL Huanca Sancos.

Figura 4.4: Switch D-LINK 1016A

Tabla 4.4: Especificaciones Switch D-LINK 1016A

ESPECIFICACIONES		
Key Features	• D-Link Green Technology • 3.2 Gbps switching fabric	• Sixteen 10/100 Mbps Fast Ethernet ports • Auto MDI/MDIX crossover for all ports
Standards	• IEEE 802.1P QoS support • IEEE 802.3 10BASE-T Ethernet (twisted-pair copper) • IEEE 802.3u 100BASE-TX Fast Ethernet (twisted-pair copper)	• IEEE 802.3az Energy-Efficient Ethernet (EEE) • ANSI/IEEE 802.3 NWay auto-negotiation • IEEE 802.3x Flow Control
FUNCIONALIDAD		
Data Transfer Rates	• Ethernet: • 10 Mbps (half duplex) • 20 Mbps (full duplex)	• Fast Ethernet: • 100 Mbps (half duplex) • 200 Mbps (full duplex)
Network Cables	• 10BASE-T: • UTP CAT 3, 4, 5/5e (100 m max.) • EIA/TIA-586 100-ohm STP (100 m max.)	• 100BASE-TX, 1000BASE-T: • UTP CAT 5/5e (100 m max.) • EIA/TIA-568 100-ohm STP (100 m max.)
LED Indicators	• Per port: Link/Activity/Speed	• Per device: Power
Packet Filtering/Forwarding Rates	• Ethernet: 14,880 pps per port	• Fast Ethernet: 148,800 pps per port
Media Interface Exchange	• Auto MDI/MDIX adjustment for all ports	
Transmission Method	Store-and-forward	
RAM Buffer	• 256 KBytes per device	

- **GABINETE DE PARED**

Los gabinetes de pared SATRA, están diseñados para brindar seguridad a sus equipos de red, distribuidores y demás equipos de telecomunicaciones.

Diseñado según normas internacionales con materiales de la mejor calidad lo cual brinda mayor resistencia y duración de la estructura. El marco de anclaje del gabinete de pared cuenta con 6 orificios para la distribución adecuada de cable, el cual se puede separar de la estructura para la administración de los equipos y cableado por la parte posterior.

Este tipo de gabinete estará ubicado en algunos ambientes de toda la UGEL Huanca Sancos.

La cantidad de gabinetes utilizados serán de 05 unidades, empotrados fijamente en la pared en los ambientes asignados de las diferentes áreas para luego ser incluidos interiormente los respectivos equipos tecnológicos, Adecuado para los Switches adquiridos, y para almacenamiento de un UPS alterna, también por la dureza del material de este tipo de gabinetes es garantizado según las características.

Tabla 4.5: Características Gabinete de Pared 4 RU (4UR) Abatible 30.50 x 60 x 40 cm Puerta de Vidrio

MARCA	SATRA
DESCRIPCIÓN	Gabinete de Pared 4 RU (4UR) Abatible 30.50 x 60 x 40 cm Puerta de Vidrio
FORMATO	Montaje en Pared
MATERIAL	Acero Laminado al Frio (LAF) de alta resistencia
GROSOR	Plancha de 1.2 mm
COLOR	Negro
PINTURA	Al horno en Polvo con tratamiento electrostático
UNIDADES DE RACK	4 RU / 4UR
PESO APROX	15.2 Kg
UTILIZADO PARA	Comunicaciones Switch, UPS, Organizador de cable

Figura 4.5: Gabinete de Pared 4 RU (4UR) Abatible 30.50 x 60 x 40 cm Puerta de Vidrio

- **Organizador de cables**

El organizador horizontal de cables SATRA presenta un diseño basado en la norma EIA 310 – D de 19”, Rackeable en 2 y 1 RU. De base metálica con cuerpo de plástico para

mayor duración. Cuenta con divisiones para la correcta presentación y separación de los cables UTP. Diseño ideal para utilizarlo en gabinetes y racks.

Los organizadores de cable estarán ubicados en todos los racks empotrados en la pared de todos los ambientes de la UGEL Huanca Sancos y serán ubicados en el interior de cada gabinete de pared para mejorar la estructura de la distribución de cables.

La cantidad de organizadores de cables utilizados serán de 05 por ser la cantidad de redes implementadas en toda la UGEL Huanca Sancos, igualmente recomendado y adquirido por lo frágil y rápido de distribución de cables, con una alta calidad de producto.

Tabla 4.6: Características Organizador horizontal de cables SATRA

Rackeable	Si, 1RU
Dimensiones físicas	(Alt. x Anc. x Prof.) cm: **4.4 x 49 x 7.**
Color	Negro.
Base	Metálico
Cuerpo y cubierta	Plástico ligero.
Capacidad máxima	24 ranuras para cable.
Estructura	Rack (pared, piso). / Gabinete (pared, piso, servidores).

Figura 4.6: Organizador horizontal de cables SATRA

- **Roseta para pared JE302-WH**

Roseta Adosable de 2 puertos – Blanco Roseta de dos salidas para soluciones sencillas. Acepta Jacks telefónicos y de data ser instaladas en pared.

Las rosetas de pared estarán ubicadas en todos los puntos de acceso empotrados en la pared de todos los ambientes de la UGEL Huanca Sancos y serán ubicados según la distancia de cada oficina para mejorar la estructura y la distribución de cables UTP.

La cantidad de rosetas utilizadas serán de 60 multiplicado ya que cada roseta contiene 2 puertos de Jack Rj45 por ser la cantidad de redes implementadas en toda la sede, recomendado y favorecido por su tamaño, uso práctico y adecuado para el tipo de pared que presenta la sede UGEL Huanca Sancos.

Tabla 4.7: Características Roseta Adosable de 2 puertos – Blanco Roseta

Marca	SATRA
Jack aceptables	Compatibles con diversas categorías de jacks
Color	Blanco
puertos	2

Figura 4.7: Roseta Adosable de 2 puertos – Blanco Roseta

- **Jack rj45**

Los Jack Rj45 son de alto desempeño cumplen con la normativa de conectorización T568A/T568B con modelos disponibles en 5 colores diferentes. Los conectores SATRA están en total cumplimiento e incluso superan los requerimientos publicados en los estándares de la ANSI/TIA 568-C tanto para categoría 6 logrando óptimos desempeños para transmisiones a más de 1Gbps satisfaciendo sus altos requerimientos de ancho de banda.

Los Jack Rj45 estarán ubicados en todos los puntos de toda la infraestructura de la UGEL Huanca Sancos y conectados en cada punto de acceso para su respectiva conexión mediante un Patch Cord.

La cantidad Jack RJ45 utilizados serán de 120 unidades, por ser la cantidad de puntos de acceso en la infraestructura de toda la UGEL Huanca Sancos. Recomendado por su calidad de producto, perfecto para la estructuración de redes que empareja con las rosetas de pared y su fiabilidad.

Tabla 4.8: Características JACKS CAT 6

Categoría	Cat 6
Descripción	Cat 6 punck Down Keystone Jack están diseñadas para proporcionar un rendimiento excelente.
Tipo panel	sin blindaje RJ45 (8P8C) Keystone Jack
Tapa	plástico para conector IDC
Color	Azul
Marca	Satra

Figura 4.8: JACKS CAT 6

- **Cable UTP (Unshielded Twisted Pai) CAT6e**

La principal diferencia entre los cables CAT6e reside en el ancho de banda que puede admitir el cable para las transferencias de datos.

Los cables CAT6e han sido diseñados para trabajar con frecuencias de hasta 250 MHz.

Cuando incremente la cantidad de usuarios en la sede, la velocidad requerida es flexible y rígido desde el momento que se interconectan con el Swicth con el cable CAT6e y se aprovecha las capacidades al máximo nivel desde el nodo principal.

El cable sólido UTP SATRA CAT6e de 4 pares trenzados, posee con un alto rendimiento y calidad con una frecuencia de operación de 100 MHz. Además, cumple y supera las normas ANSI/TIA-568-C.2.

La chaqueta de PVC retarda la propagación del fuego, contando con la calificación CM según las pruebas realizadas por la **Underwriters Laboratories (UL)** recomendado no solo para cableados horizontales sino también para usos en el Backbone o en espacios verticales.

Cable UTP CAT 6e estarán tendidos en todos los puntos de toda la infraestructura de la UGEL Huanca Sancos con las respectivas canaletas para luego ser conectados en los Jack RJ45 y puestos a las rosetas de pared de todos los puntos de la red.

La cantidad de cable utilizado será de 2 cajas de 305 metros c/u, para toda la cantidad de puntos de acceso en la infraestructura de toda la UGEL Huanca Sancos, así mismo adecuado para el tendido del cableado estructurado por su calibre conductor, componentes de frecuencia y calidad de producto.

Tabla 4.9: Comparativo entre los cables CAT5e y CAT6

DESCRIPCIÓN	CONSTRUCCION	INDENTIFICACIÓN DE PARES
• Categoría 5e Sólido. • Frecuencia de operación 100MHz. • Prueba de flama (UL) CM. • Estándares UL 444 > UL 1581 > UL E224754 • ANSI/TIA-568-B.2 • ISO/IEC 11801 & EN50173 • IEC 61156-5:2009 (Ed. 2.0)	• Calibre del conductor 24AWG • Diámetro del de Aislamiento 0.90mm ± 0.02mm • Promedio de grosor 0.19mm • Material de Aislamiento HDPE	• 1.- Azul: Blanco/Azul • 2.- Naranja: Blanco/Naranja • 3.- Verde: Blanco/Verde • 4.- Marrón: Blanco/Marrón • Material la chaqueta PVC • Grosor de la chaqueta 0.45mm • Diámetro de la chaqueta 5.1mm ± 0.2mm

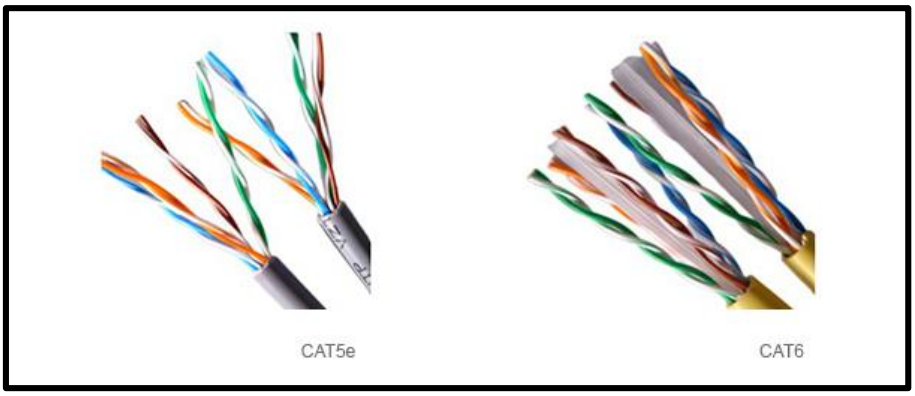


Figura 4.9 comparativo entre los cables CAT5e y CAT6

- **Estándares de cableado T568A-T568B:**

Como sabemos, los cables de red se componen de cuatro pares de cables, cada uno de los cuales consta de un cable de color sólido y una franja del mismo color. Para la red Ethernet 10/100BASE-T, solo se utilizan dos pares de cables (naranja y verde). Los otros dos pares de cables (de color marrón y azul) se utilizan para otra aplicación de red Ethernet o para conexiones telefónicas. La utilización de un cable directo o cruzado dependerá del tipo de conexión que se necesite. Para normalizar la disposición de cables, se utilizan dos estándares, el T568A y T568B, los cuales proporcionan esquemas de cableado para la terminación de los cables de red en enchufes, así como enchufes RJ45 de ocho posiciones. Recomendado por su calidad de producto y confiabilidad para este tipo de conexiones.

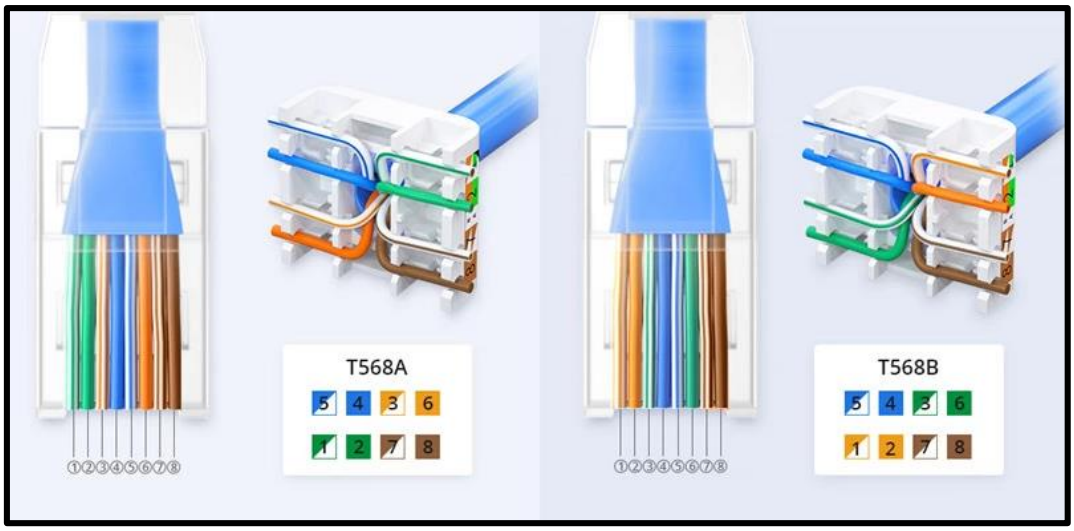


Figura 4.10: Estándares de cableado T568A-T568B

Principales costos:

A continuación, se detallan los costos que se han tenido para el desarrollo de este proyecto:

Tabla 4.10: Detalle de los principales rubros de costos del diseño e implementación de la red

PROGRAMAS	SISTEMA OPERATIVO. APLICACIONES NUEVAS DE LOS USUARIOS.
EQUIPOS	**USADOS POR LOS USUARIOS:** • ELEMENTOS COMPUTACIONALES (COMPUTADORAS, SERVIDORES) • PERIFERICOS (IMPRESORAS, FOTOCOPIADORAS) • DISPOSITIVOS SEGURIDAD (UPS) **USADOS PARA LA RED:** • EQUIPOS ESPECIALIZADO • DISPOSITIVOS DE INTERCONEXIÓN • SERVICIO DE INTERNET
PERSONAL	PREPARACIÓN DEL LOCAL DE INSTALACION E INSTALACIÓN DE LA RED
OTROS	CORRIENTE ELECTRICA CABLEADO ESTRUCTURADO RJ45, ROSETAS Y ACCESORIOS VARIOS.

Tabla 4.11: Costos en general

DETALLE		**CANT**	**PRECIO**	**TOTAL**
PROGRAMAS	SISTEMA OPERATIVO	0	S/ 0.00	**S/ 0.00**
	CONFIGURACIONES	**0**	S/ 0.00	**S/ 0.00**
	ANTIVIRUS	**0**	S/ 0.00	**S/ 0.00**
EQUIPOS	COMPUTADORAS	86	S/ 0.00	**S/ 0.00**
	FOTOCOPIADORAS	4	S/5.000	**S/ 20.000**
	UPS	07	S/ 600.00	**S/ 4.200**
	SERVIDORES	2	S/ 12.000	**S/ 24.000**
	SWITCH CENTRAL 24 PUERTOS	10	S/ 580.00	**S/ 5.800**
	MICROKTIK	1	S/ 750.00	**S/ 750.00**
	GABINETE	5	S/ 400.00	**S/ 2.000**
	SERVICIO DE INTERNET	1	S/ 2.600	**S/ 2.600**
PERSONAL	SERVICIO DE INSTALACIÓN	01	S/ 500.00	**S/ 1.000**
OTROS	MATERIALES CORRIENTE ELECTRICO	0	S/ 300.00	**S/ 300.00**
	METRO CABLE UTP CAT 6A	305	S/ 350.00	**S/ 350.00**
	RJ45, ROSETAS, JACK, CANALETAS, ETC	0	S/ 1.200	**S/ 1.200**
TOTAL				**S/ 62.200**

Niveles de seguridad

Dado que las amenazas cibernéticas evolucionan constantemente en complejidad y volumen, la batalla contra ellas implica 'extender' la protección a todos los sistemas de la red corporativa: servidores, bases de datos, servicios, software instalado, etc. Además, se debe

prestar atención para garantizar que Los empleados de la empresa entienden y siguen los principios de seguridad cibernética y no comprometerán (in)intencionadamente la seguridad de la red corporativa con sus acciones.

Sin embargo, las medidas de Ciberseguridad aplicadas dentro de la organización pueden diferir según el tamaño de la empresa, sus capacidades financieras, la industria en la que opera (regulada o no regulada), la información que tiene que manejar en el curso de las actividades comerciales, etc. Los niveles de seguridad que se han contemplado en esta implementación son 3:

Nivel 1: El fin de este nivel es garantizar la protección de la red corporativa de las amenazas cibernéticas más comunes, por ejemplo, los ataques de Phishing (los enlaces a sitios web maliciosos o descargas infectadas con virus se adjuntan a correos electrónicos o mensajes instantáneos y se envían a los empleados de una empresa) y malware (software malicioso que llega a la red de una empresa a través de Internet o correo electrónico y existe en forma de spyware, Ransomware, secuestradores de navegador, etc.).

La protección mínima se aplica a las pequeñas empresas que operan en industrias no reguladas y que tienen recursos financieros estrictamente limitados. Las empresas pequeñas y no muy conocidas (al menos no todavía) que no manejan información valiosa para los piratas informáticos (por ejemplo, datos personales de clientes como números de tarjetas de crédito, contraseñas, etc.) difícilmente pueden convertirse en objetivos de ataques cibernéticos sofisticados como DDoS (Distributed Denegación de servicio) o Spear Phishing.

El mínimo de medidas de Ciberseguridad esenciales para la implementación es una protección de firewall correctamente configurada que funcione junto con un software antivirus actualizado regularmente. Los cortafuegos escanean el tráfico de la red para detectar paquetes anómalos o fragmentos de paquetes. Los antivirus garantizan la protección contra amenazas cibernéticas como Ransomware, gusanos, Spyware, etc. al verificar cada archivo que los empleados abren o descargan de Internet u otras fuentes.
Para aplicar estas medidas de seguridad, no es necesario organizar un departamento de Ciberseguridad independiente. El departamento de TI de una empresa puede asumir la responsabilidad de esto, ya que la implementación de la protección de firewall, la instalación

de software antivirus y el mantenimiento continuo de su rendimiento no requieren habilidades relacionadas con la Ciberseguridad.

No obstante, el nivel de protección de una red corporativa debe comprobarse periódicamente. Realizar evaluaciones de vulnerabilidad y pruebas de penetración anualmente es suficiente para una pequeña organización que lleva a cabo su negocio en una industria no regulada. Estos servicios de Ciberseguridad realizados anualmente no supondrán grandes gastos para una empresa con un presupuesto limitado. Al mismo tiempo, estas actividades pueden ayudar a los administradores de sistemas a estar al tanto de las debilidades de seguridad que ocurren dentro de la red de la empresa como se muestra en la siguiente figura.

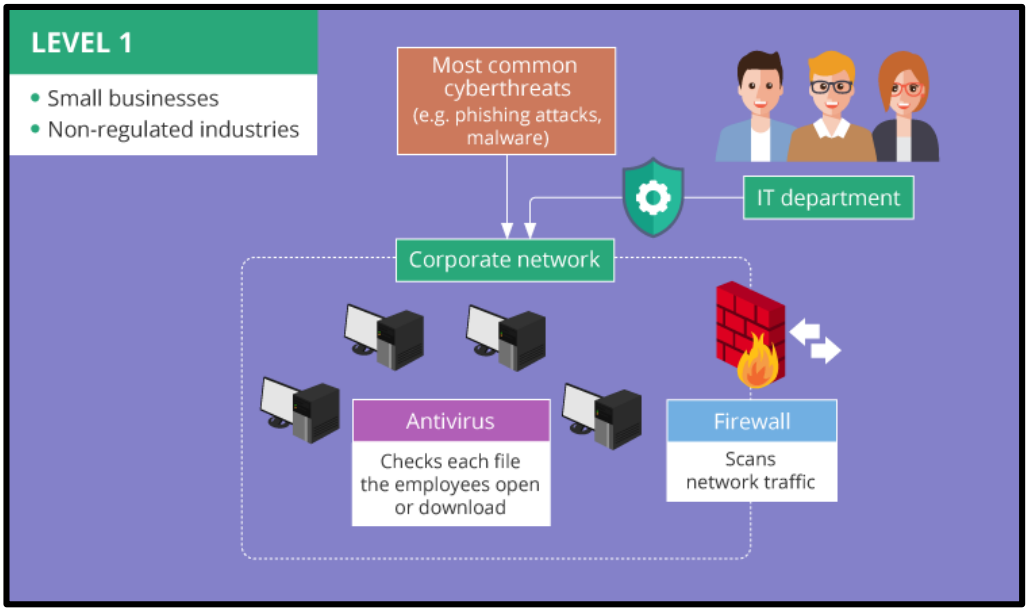


Figura 4.11: Nivel 1 de seguridad de la red

Nivel 2: Garantiza la protección de la red corporativa contra ataques no dirigidos, por ejemplo, malware enviado a una variedad de direcciones de correo electrónico, ataques de suplantación de identidad, Spam, etc. En este caso, el objetivo de los atacantes es robar cualquier información valiosa de cualquier IP. Dirección susceptible de conocer las debilidades de seguridad que posiblemente existan en la red corporativa.

La probabilidad de que instituciones pequeñas sean víctimas de ataques no dirigidos es grande. Dado que dichas organizaciones no tienen la necesidad de cumplir con los

estándares regulatorios, es probable que descuiden las fuertes medidas de Ciberseguridad en sus redes. Por lo tanto, pueden ser fáciles de comprometer.

Para asegurar una protección avanzada de la red corporativa, además de los elementos de protección mínima – Firewalls y Antivirus – se deben aplicar los siguientes componentes:

- La seguridad del correo electrónico implica una variedad de técnicas (escaneo de correos electrónicos en busca de malware, filtrado de Spam, etc.) para mantener segura la información corporativa tanto en las comunicaciones por correo electrónico 'internas' como 'externas' de cualquier ataque cibernético que use el correo electrónico como punto de entrada (Spyware, Adware, etc.).

- Segmentación de la red, por ejemplo, segmentación de la red por áreas de la sede con los segmentos conectados a través de firewalls que no permiten que el código malicioso u otras amenazas viajen de un segmento de la red a otro. Además, la segmentación de la red implica separar los activos de la red que almacenan los datos de una empresa de los segmentos externos (servidores web, servidores proxy), lo que reduce el riesgo de pérdida de datos.

- Detección de intrusos (IDS) y sistema de prevención de intrusos (IPS) utilizados para identificar y registrar información sobre posibles incidentes de seguridad, bloquearlos antes de que se propaguen por los entornos de red, etc.

Para mantener este nivel de seguridad en la red, una empresa necesita especialistas en seguridad de la información encargados de detectar y gestionar los riesgos de ciberseguridad, desarrollar procedimientos y políticas de seguridad, etc. A estos efectos, la empresa puede disponer de su propio departamento de seguridad de la información o recurrir a un servicio de seguridad gestionada proveedor (MSSP).

Organizar un departamento de seguridad de la información independiente implica grandes gastos tanto en la contratación de un equipo de seguridad experimentado como en la compra del equipo y el software necesarios. Trabajar con un MSSP es una solución más rentable, que permite a una empresa mantener el enfoque en las operaciones comerciales

principales. Sin embargo, la empresa aún necesitará un oficial de seguridad interno para coordinar el trabajo con MSSP.

Para controlar la eficiencia de la protección de la seguridad cibernética, una estrategia de seguridad cuidadosamente diseñada debe proporcionar una evaluación de vulnerabilidad trimestral y una prueba de penetración anual para detectar, mitigar y gestionar los riesgos de seguridad cibernética. Una empresa necesita una estrategia de Ciberseguridad, ya que se enfoca en proteger la red corporativa teniendo en cuenta que el personal usa sus dispositivos móviles personales y computadoras portátiles para fines comerciales (BYOD), el uso generalizado de la computación en la nube, etc. y brinda orientación directa a los empleados de la empresa sobre comportamiento dentro de la red corporativa como visualizamos en la siguiente figura.

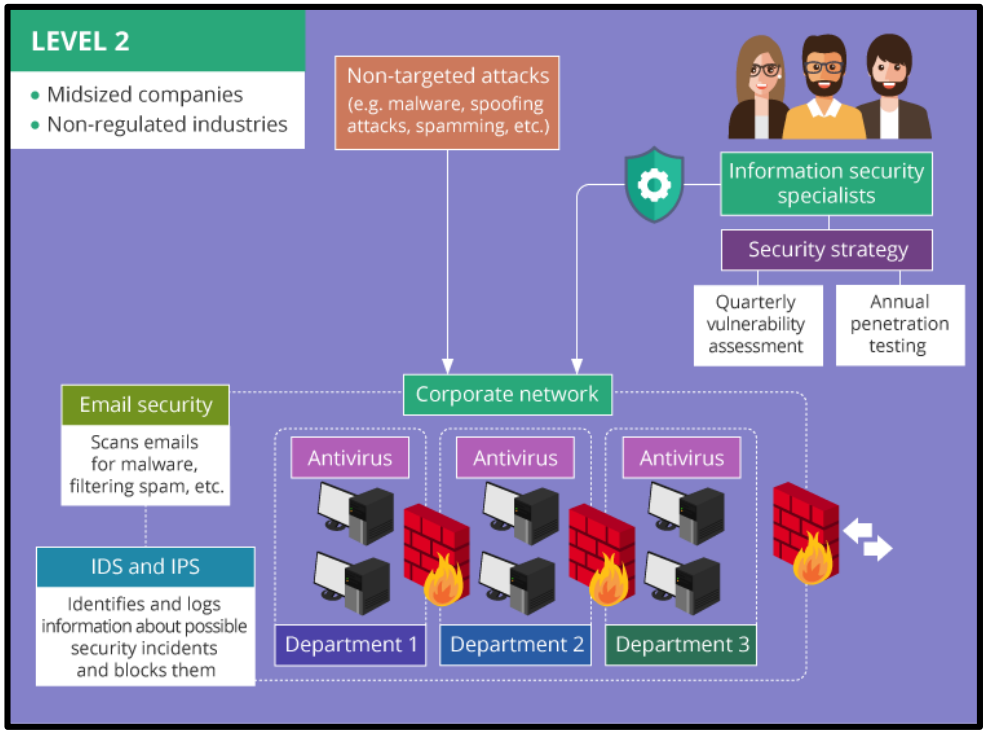


Figura 4.12: Nivel 2 de seguridad de la red

Nivel 3: El fin es garantizar la protección de la red corporativa contra ataques dirigidos. Este tipo de ciberataques (Spear, Phishing, propagación de Malware avanzado, etc.) implica campañas específicamente desarrolladas y dirigidas contra una determinada organización.

La sede de la UGEL Huanca Sancos si es que operan en campos regulados debe prestar la máxima atención para mantener la protección contra las amenazas cibernéticas y cumplir con las regulaciones y estándares (HIPAA, PCI DSS, etc.). Los siguientes componentes de Ciberseguridad pueden ayudar a cerrar todos los posibles vectores de ataque:

- Puesto final de Seguridad. Este método de seguridad implica proteger el acceso de cada dispositivo (un teléfono inteligente, una computadora portátil, etc.) que llega a la red corporativa y, por lo tanto, se convierte en un punto de entrada potencial para amenazas de seguridad. Por lo general, la seguridad de puntos finales incluye la instalación de software de seguridad especial en un servidor de administración dentro de la red corporativa, junto con la instalación de software de cliente en cada dispositivo. La combinación de estas medidas permite monitorear las actividades que realizan los usuarios al acceder a la red corporativa de forma remota desde sus teléfonos inteligentes, tabletas y otros dispositivos. Por lo tanto, la empresa obtiene una mejor visibilidad en tiempo real de toda la gama de posibles amenazas de seguridad con las que podría tener que lidiar.

- Prevención de pérdida de datos (DLP). La aplicación de esta medida es extremadamente importante dentro de una empresa dedicada al sector financiero o de salud. El software DLP garantiza la protección y evita la fuga de datos sensibles, personales y confidenciales, por ejemplo, números de tarjetas de crédito de clientes, números de seguridad social, etc., lo que brinda a los administradores de DLP un control total sobre los tipos de datos que se pueden transferir fuera de la red corporativa. DLP puede denegar los intentos de reenviar cualquier correo electrónico comercial fuera del dominio corporativo, cargar archivos corporativos a almacenamientos en la nube de código abierto, etc.

- Seguridad de la información y gestión de eventos (SIEM). Las soluciones SIEM rastrean, recopilan, analizan e informan sobre datos de registro y eventos en cada actividad que ocurre dentro del entorno de TI, lo que permite evitar situaciones de "no tengo idea de lo que sucedió" en caso de que la red de la empresa sea pirateada. Entre los beneficios de SIEM se encuentran la centralización de los datos de registro recopilados, lo que brinda soporte para cumplir con los requisitos de PCI DSS, HIPAA y otras regulaciones, lo que garantiza una respuesta a incidentes en tiempo real.

Para operar correctamente con las soluciones de seguridad mencionadas, la combinación de los esfuerzos de un departamento de seguridad de la información separado y la ayuda de un MSSP servirá mejor. Para muchas empresas, otorgar a un MSSP acceso total y control sobre datos confidenciales, información de identificación personal del cliente, etc. parece bastante arriesgado, especialmente desde la perspectiva del cumplimiento de la seguridad. Sin embargo, tiene sentido firmar un SLA detallado con una empresa de servicios de Ciberseguridad y delegar una parte de las responsabilidades de Ciberprotección a un MSSP externo. Permite a las empresas obtener informes y monitoreo del estado de seguridad las 24 horas del día, los 7 días de la semana y, al mismo tiempo, reducir sus gastos en protección de Ciberseguridad.

Entre las medidas de Ciberseguridad necesarias se encuentran el desarrollo y mantenimiento de una estrategia de seguridad, la realización de una evaluación de vulnerabilidades seguida de pruebas de penetración trimestrales (es mejor que se lleven a cabo antes de cada verificación de auditoría para cumplir con los estándares y las regulaciones), garantizar un monitoreo constante de amenazas y organizar una reunión estructurada. Respuesta a incidentes (IR).

El monitoreo de amenazas implica el monitoreo constante de la red corporativa y los puntos finales (servidores, dispositivos inalámbricos, dispositivos móviles, etc.) en busca de signos de amenazas de Ciberseguridad, por ejemplo, intentos de intrusión o exfiltración de datos. Hoy en día, el monitoreo de amenazas se está volviendo aún más importante con la tendencia en las empresas de contratar empleados de forma remota y aplicar la política BYOD, lo que pone la protección de los datos corporativos y la información confidencial bajo un riesgo adicional.

La respuesta a incidentes (IR) se ocupa de las situaciones en las que ya se han producido violaciones de seguridad. Por ello, una empresa necesita un equipo especial, propio o externo, preparado para los incidentes, listo para detectar eventos reales, encontrar las causas y responder a las amenazas de Ciberseguridad con el menor daño posible y el mínimo tiempo necesario para recuperarse del ataque. Las actividades de IR evitan que los problemas pequeños se transformen en problemas mayores, como la violación de datos o la interrupción del sistema como se muestra en la siguiente figura.

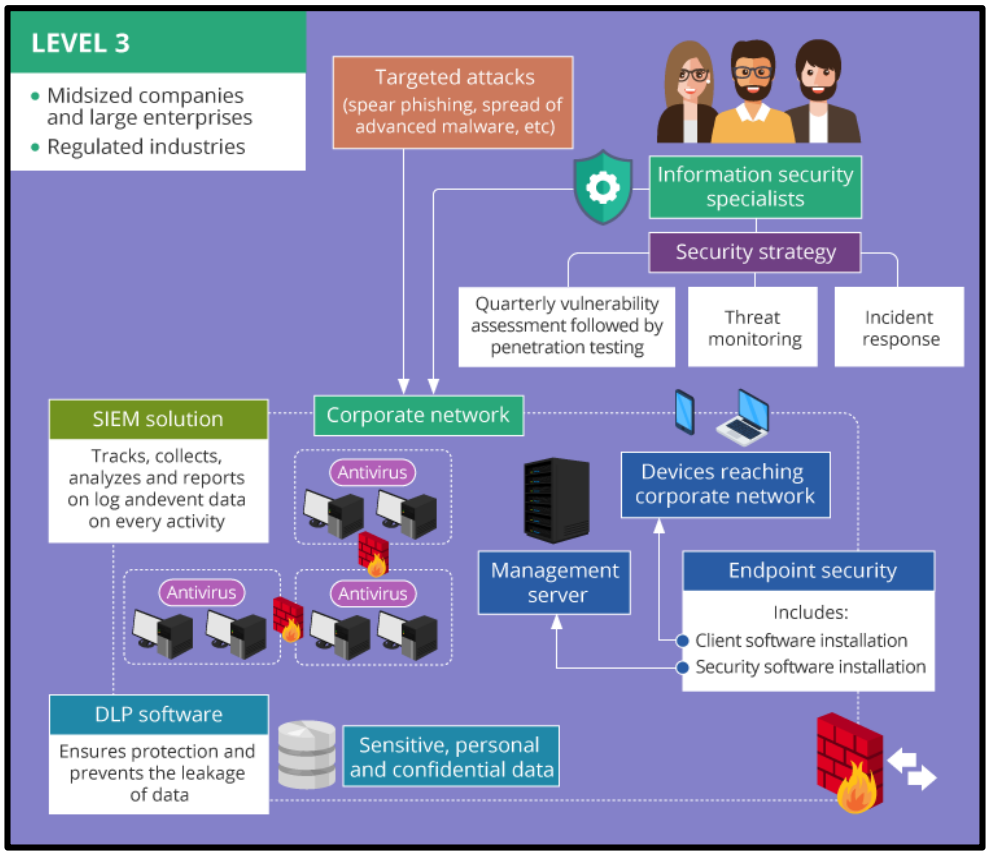


Figura 4.13: Nivel 3 de seguridad de la red

Aplicación que se van a utilizar en red.

Existen muchas aplicaciones informáticas del gobierno central como una herramienta para realizar operaciones o funciones específicas, generalmente son diseñadas para facilitar ciertas tareas complejas y hacer más sencilla la experiencia informática de los trabajadores de la UGEL Huanca Sancos, entre ellos menciono algunos.

- **Sistema Integral de Administración Financiera - SIAF**

En la siguiente figura se muestra una herramienta para ordenar la gestión administrativa de los Gobiernos Locales, simplificar sus tareas en este ámbito y reducir los reportes que elaboraban, así como el tiempo dedicado a la conciliación.

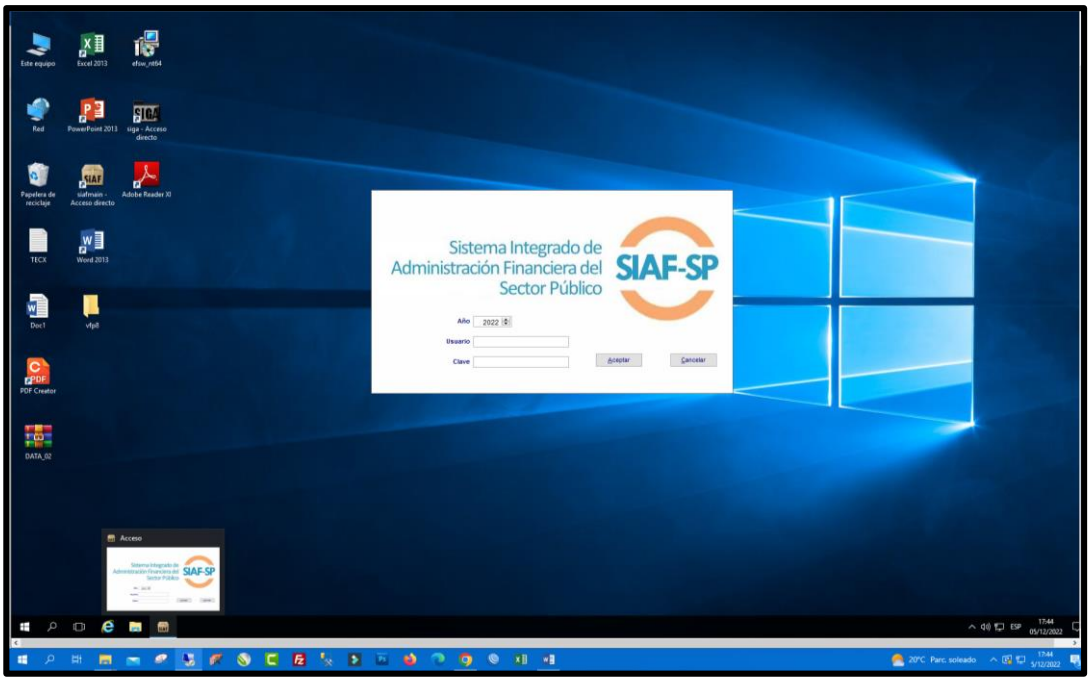


Figura 4.14: SIAF

- **Sistema Integrado de Gestión Administrativa - SIGA**

En la siguiente figura se muestra una herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del estado y que sigue las normas establecida por los Órganos Rectores de los Sistemas Administrativos del Estado.

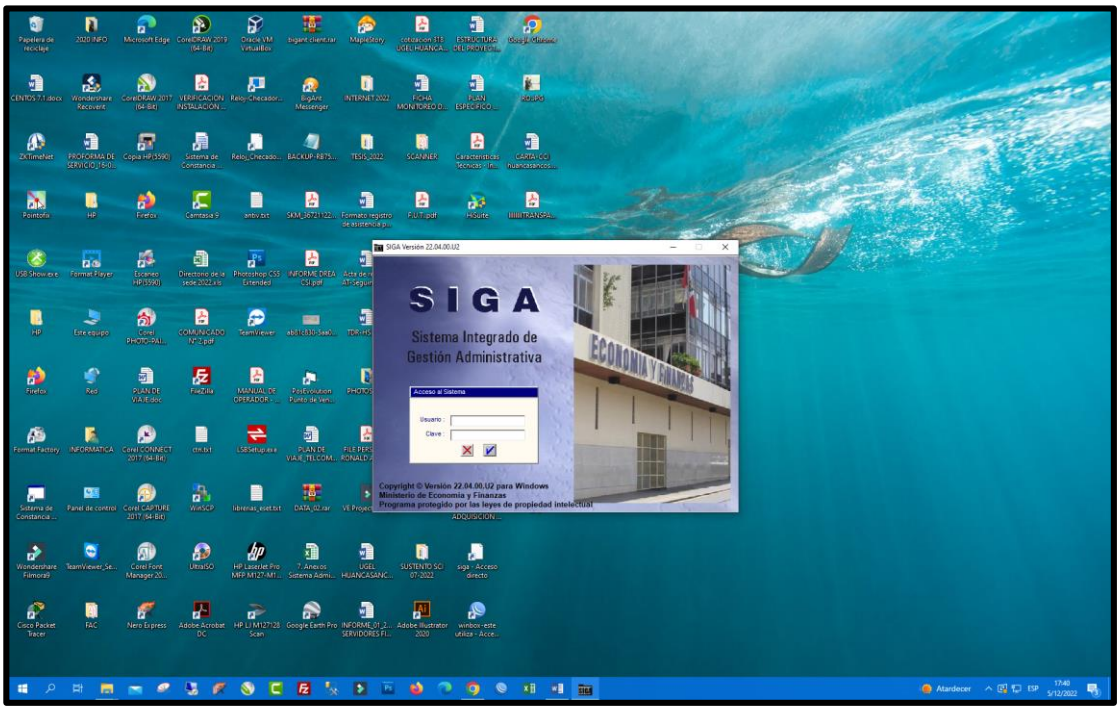


Figura 4.15: SIGA

4.1.3. Diseño e implementación del sistema

En la siguiente figura 4.16 se muestra el primer nivel considerado como RED-01 la cual encontramos la puerta principal y en los lados laterales las diferentes oficinas como mesa de partes, caja y almacén. En la parte posterior se ubican las oficinas de los PRONOEI, formadores tutores – AGP, y asesoría jurídica.

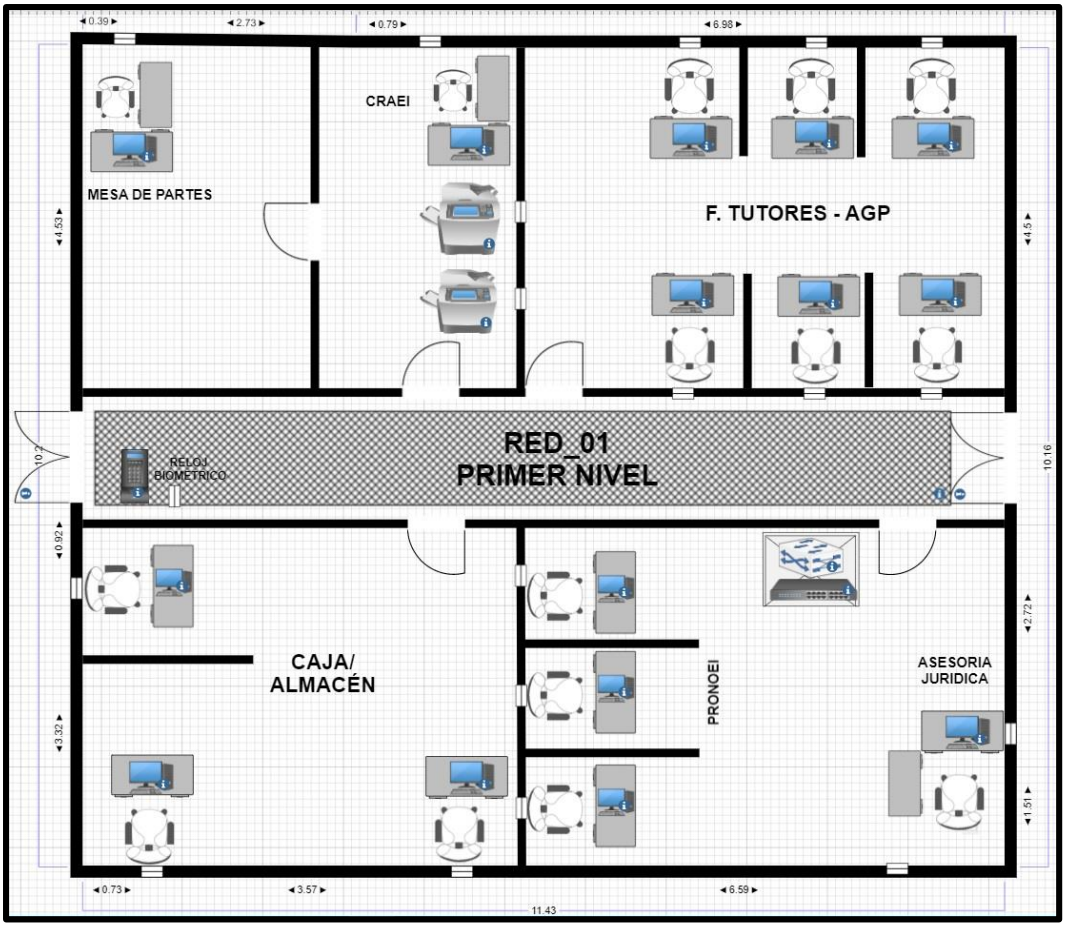


Figura 4.16: Diseño del mapeo del proyecto 1

En la siguiente figura 4.17 se muestra el primer nivel considerado como RED-02 la cual encontramos la oficina de Informática, donde se ubica el centro de cómputo y los respectivos servidores. En lado interior se ubica el auditorio donde se considera puntos de acceso a conectividad de red libre para cualquier dispositivo.

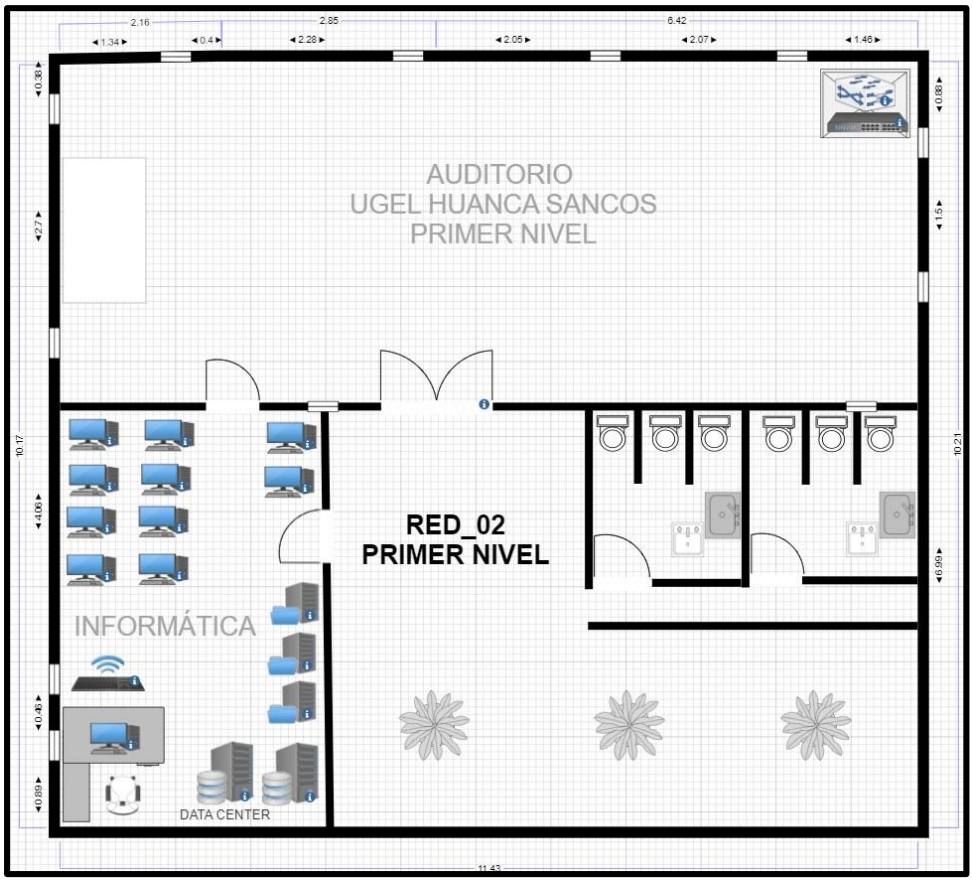


Figura 4.17: Diseño del mapeo del proyecto 2

En la siguiente figura 4.18 se muestra el segundo nivel considerado como RED-03 la cual encontramos el área de Gestión Pedagógica, donde se ubican los diferentes puntos de acceso a conectividad de red, distribuidos en las computadoras y otros dispositivos.

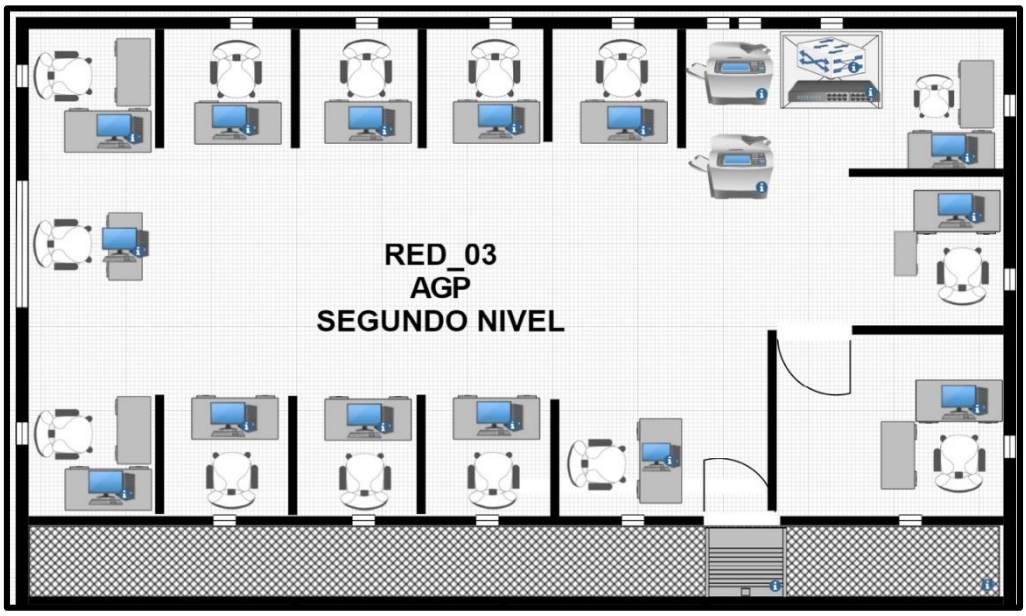


Figura 4.18: Diseño del mapeo del proyecto 3

En la siguiente figura 4.19 se muestra el segundo nivel considerado como RED-04 la cual encontramos el Área de Gestión Administrativa, donde se ubican los diferentes puntos de acceso a conectividad de red, distribuidos en las computadoras y otros dispositivos.

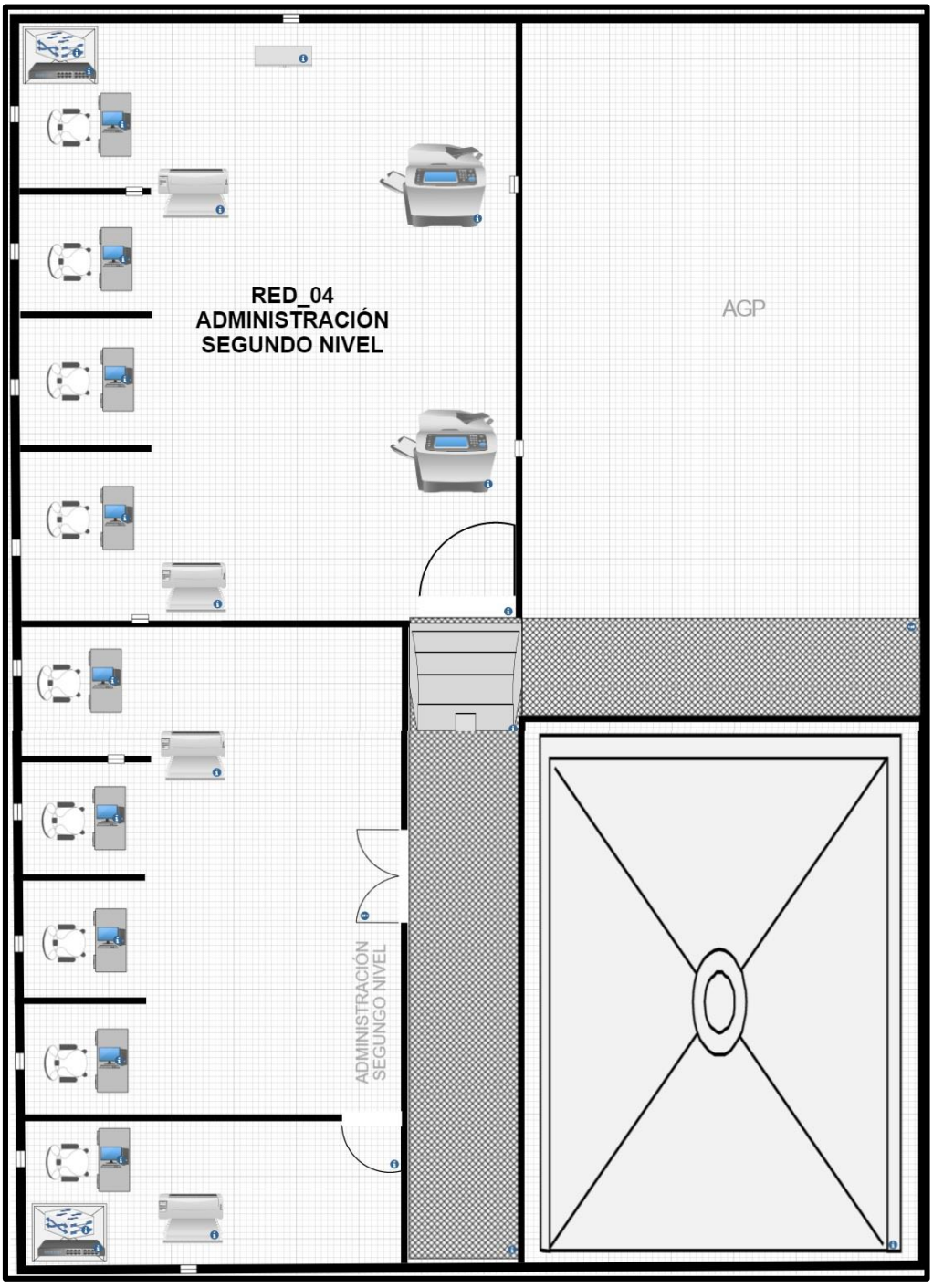


Figura 4.19: Diseño del mapeo del proyecto 4

En la siguiente figura 4.20 se muestra el segundo nivel considerado como RED-05 la cual encontramos el Área de Gestión Institucional, área de personal y dirección, donde se ubican los diferentes puntos de acceso a conectividad de red, distribuidos en las computadoras y otros dispositivos.

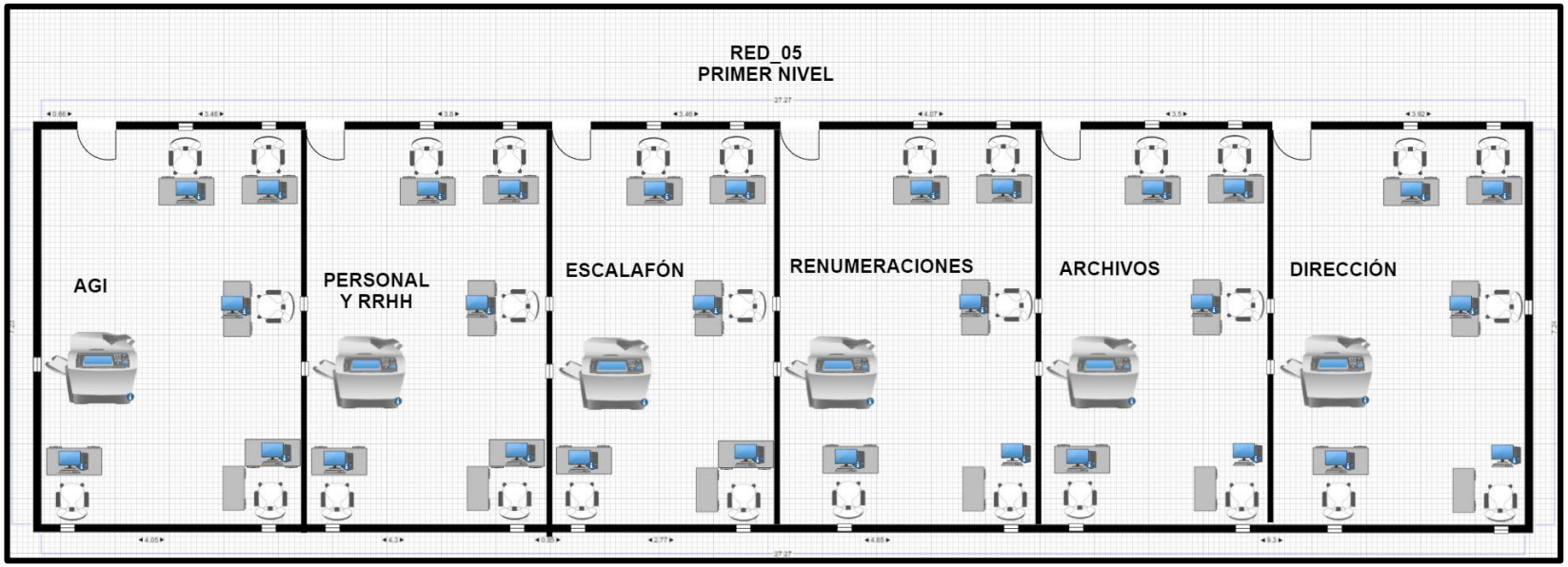


Figura 4.20: Diseño del mapeo del proyecto 5

En la siguiente figura 4.21 se muestra un modelo de simulación de la red en toda la sede de la UGEL Huanca Sancos con todas las características recomendadas para el buen funcionamiento y distribución de red.

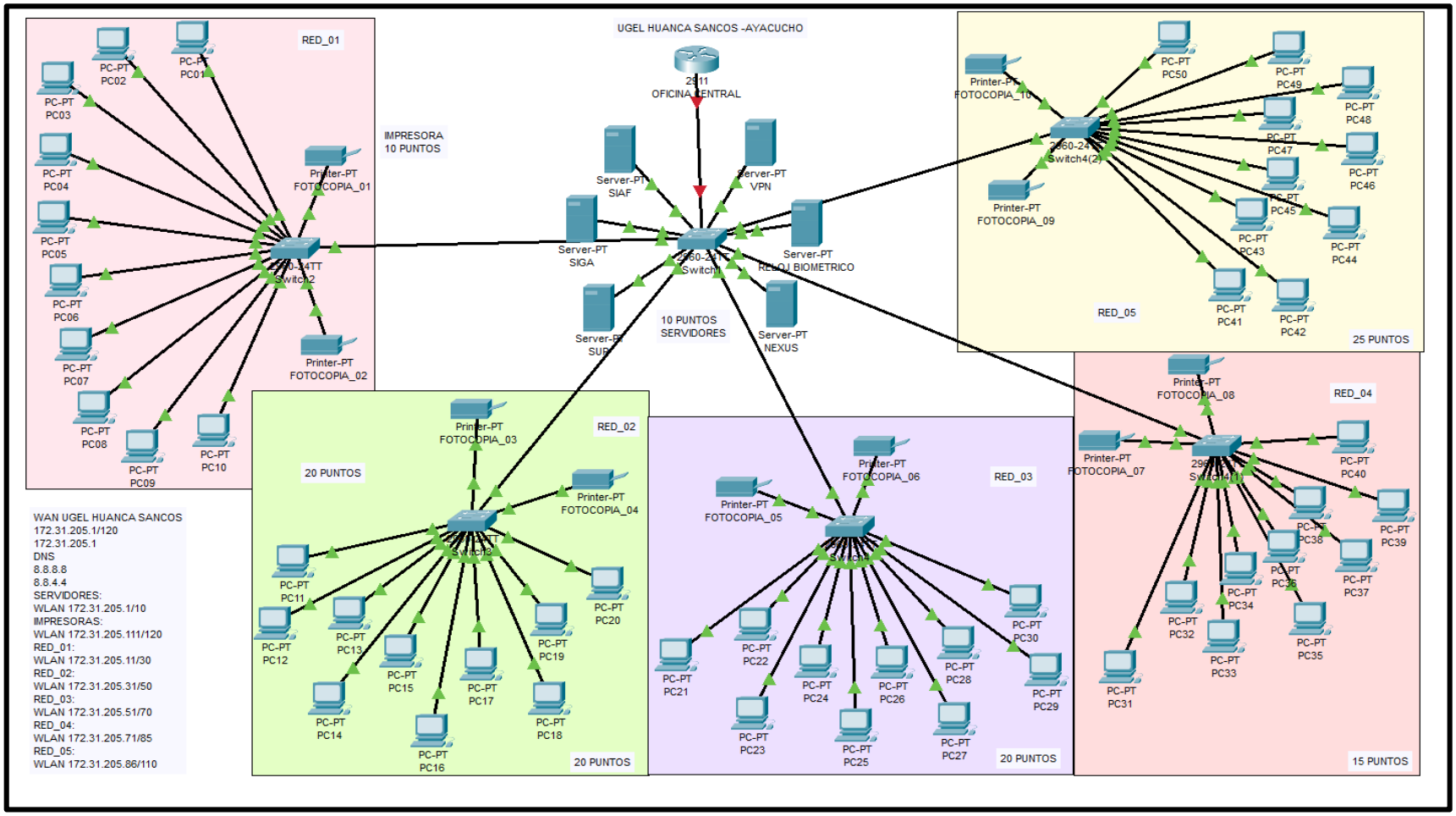


Figura 4.21: Diseño del mapeo del proyecto – Simulación con el software (Cisco Packet Tracer)

Asignación de direcciones IP por cada punto de red

En las siguientes tablas 4.12 al 4,17 se realiza la asignación de las direcciones IP de cada uno de los puntos de red para la UGEL

Tabla 4.12: Configuración y asignación de direcciones para: Servidores

UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
SERVIDORES	172.31.205.0	SERV_01	172.31.205.1	255.255.0.0	172.31.205.1
		SERV _02	172.31.20.2	255.255.0.0	172.31.205.1
		SERV _03	172.31.205.3	255.255.0.0	172.31.205.1
		SERV _04	172.31.205.4	255.255.0.0	172.31.205.1
		SERV _05	172.31.205.5	255.255.0.0	172.31.205.1
		SERV _06	172.31.205.6	255.255.0.0	172.31.205.1
		SERV _07	172.31.205.7	255.255.0.0	172.31.205.1
		SERV _08	172.31.205.8	255.255.0.0	172.31.205.1
		SERV _09	172.31.205.9	255.255.0.0	172.31.205.1
		SERV _10	172.31.205.10	255.255.0.0	172.31.205.1

Tabla 4.13: Configuración y asignación de direcciones para: RED-01 PRIMER NIVEL

UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
RED-01 PRIMER NIVEL	172.31.205.0	PC-01	172.31.205.11	255.255.0.0	172.31.205.1
		PC-02	172.31.205.12	255.255.0.0	172.31.205.1
		PC-03	172.31.205.13	255.255.0.0	172.31.205.1
		PC-04	172.31.205.14	255.255.0.0	172.31.205.1
		PC-05	172.31.205.15	255.255.0.0	172.31.205.1
		PC-06	172.31.205.16	255.255.0.0	172.31.205.1
		PC-07	172.31.205.17	255.255.0.0	172.31.205.1
		PC-08	172.31.205.18	255.255.0.0	172.31.205.1
		PC-09	172.31.205.19	255.255.0.0	172.31.205.1
		PC-10	172.31.205.20	255.255.0.0	172.31.205.1
		PC-11	172.31.205.21	255.255.0.0	172.31.205.1
		PC-12	172.31.205.22	255.255.0.0	172.31.205.1
		PC-13	172.31.205.23	255.255.0.0	172.31.205.1
		PC-14	172.31.205.24	255.255.0.0	172.31.205.1
		PC-15	172.31.205.25	255.255.0.0	172.31.205.1
		PC-16	172.31.205.26	255.255.0.0	172.31.205.1
		PC-17	172.31.205.27	255.255.0.0	172.31.205.1
		PC-18	172.31.205.28	255.255.0.0	172.31.205.1
		PC-19	172.31.205.29	255.255.0.0	172.31.205.1
		PC-20	172.31.205.30	255.255.0.0	172.31.205.1

Tabla 4.14: Configuración y asignación de direcciones para: RED-02 PRIMER NIVEL

UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
RED-02 PRIMER NIVEL	172.31.205.0	PC-21	172.31.205.31	255.255.0.0	172.31.205.1
		PC-22	172.31.205.32	255.255.0.0	172.31.205.1
		PC-23	172.31.205.33	255.255.0.0	172.31.205.1
		PC-24	172.31.205.34	255.255.0.0	172.31.205.1
		PC-25	172.31.205.35	255.255.0.0	172.31.205.1
		PC-26	172.31.205.36	255.255.0.0	172.31.205.1
		PC-27	172.31.205.37	255.255.0.0	172.31.205.1

		PC-28	172.31.205.38	255.255.0.0	172.31.205.1
		PC-29	172.31.205.39	255.255.0.0	172.31.205.1
		PC-30	172.31.205.40	255.255.0.0	172.31.205.1
		PC-31	172.31.205.41	255.255.0.0	172.31.205.1
		PC-32	172.31.205.42	255.255.0.0	172.31.205.1
		PC-33	172.31.205.43	255.255.0.0	172.31.205.1
		PC-34	172.31.205.44	255.255.0.0	172.31.205.1
		PC-35	172.31.205.45	255.255.0.0	172.31.205.1
		PC-36	172.31.205.46	255.255.0.0	172.31.205.1
		PC-37	172.31.205.47	255.255.0.0	172.31.205.1
		PC-38	172.31.205.48	255.255.0.0	172.31.205.1
		PC-39	172.31.205.49	255.255.0.0	172.31.205.1
		PC-40	172.31.205.50	255.255.0.0	172.31.205.1

Tabla 4.15: Configuración y asignación de direcciones para: RED-03
SEGUNDO NIVEL

UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
RED-03 SEGUNDO NIVEL	172.31.205.0	PC-41	172.31.205.51	255.255.0.0	172.31.205.1
		PC-42	172.31.205.52	255.255.0.0	172.31.205.1
		PC-43	172.31.205.53	255.255.0.0	172.31.205.1
		PC-44	172.31.205.54	255.255.0.0	172.31.205.1
		PC-45	172.31.205.55	255.255.0.0	172.31.205.1
		PC-46	172.31.205.56	255.255.0.0	172.31.205.1
		PC-47	172.31.205.57	255.255.0.0	172.31.205.1
		PC-48	172.31.205.58	255.255.0.0	172.31.205.1
		PC-49	172.31.205.59	255.255.0.0	172.31.205.1
		PC-50	172.31.205.60	255.255.0.0	172.31.205.1
		PC-51	172.31.205.61	255.255.0.0	172.31.205.1
		PC-52	172.31.205.62	255.255.0.0	172.31.205.1
		PC-53	172.31.205.63	255.255.0.0	172.31.205.1
		PC-54	172.31.205.64	255.255.0.0	172.31.205.1
		PC-55	172.31.205.65	255.255.0.0	172.31.205.1
		PC-56	172.31.205.66	255.255.0.0	172.31.205.1
		PC-57	172.31.205.67	255.255.0.0	172.31.205.1
		PC-58	172.31.205.68	255.255.0.0	172.31.205.1
		PC-59	172.31.205.69	255.255.0.0	172.31.205.1
		PC-60	172.31.205.70	255.255.0.0	172.31.205.1

Tabla 4.16: Configuración y asignación de direcciones para: RED-04
SEGUNDO NIVEL

UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
RED-04 SEGUNDO NIVEL	172.31.205.0	PC-61	172.31.205.71	255.255.0.0	172.31.205.1
		PC-62	172.31.205.72	255.255.0.0	172.31.205.1
		PC-63	172.31.205.73	255.255.0.0	172.31.205.1
		PC-64	172.31.205.74	255.255.0.0	172.31.205.1
		PC-65	172.31.205.75	255.255.0.0	172.31.205.1
		PC-66	172.31.205.76	255.255.0.0	172.31.205.1
		PC-67	172.31.205.77	255.255.0.0	172.31.205.1
		PC-68	172.31.205.78	255.255.0.0	172.31.205.1
		PC-69	172.31.205.79	255.255.0.0	172.31.205.1
		PC-70	172.31.205.80	255.255.0.0	172.31.205.1
		PC-71	172.31.205.81	255.255.0.0	172.31.205.1
		PC-72	172.31.205.82	255.255.0.0	172.31.205.1

		PC-73	172.31.205.83	255.255.0.0	172.31.205.1
		PC-74	172.31.205.84	255.255.0.0	172.31.205.1
		PC-75	172.31.205.85	255.255.0.0	172.31.205.1

Tabla 4.17: Configuración y asignación de direcciones para: RED-05 PRIMER NIVEL

UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
RED-05 PRIMER NIVEL	172.31.205.0	PC-76	172.31.205.86	255.255.0.0	172.31.205.1
		PC-77	172.31.205.87	255.255.0.0	172.31.205.1
		PC-78	172.31.205.88	255.255.0.0	172.31.205.1
		PC-79	172.31.205.89	255.255.0.0	172.31.205.1
		PC-80	172.31.205.90	255.255.0.0	172.31.205.1
		PC-81	172.31.205.91	255.255.0.0	172.31.205.1
		PC-82	172.31.205.92	255.255.0.0	172.31.205.1
		PC-83	172.31.205.93	255.255.0.0	172.31.205.1
		PC-84	172.31.205.94	255.255.0.0	172.31.205.1
		PC-85	172.31.205.95	255.255.0.0	172.31.205.1
		PC-86	172.31.205.96	255.255.0.0	172.31.205.1
		PC-87	172.31.205.97	255.255.0.0	172.31.205.1
		PC-88	172.31.205.98	255.255.0.0	172.31.205.1
		PC-89	172.31.205.99	255.255.0.0	172.31.205.1
		PC-90	172.31.205.100	255.255.0.0	172.31.205.1
		PC-91	172.31.205.101	255.255.0.0	172.31.205.1
		PC-92	172.31.205.102	255.255.0.0	172.31.205.1
		PC-93	172.31.205.103	255.255.0.0	172.31.205.1
		PC-94	172.31.205.104	255.255.0.0	172.31.205.1
		PC-95	172.31.205.105	255.255.0.0	172.31.205.1
		PC-96	172.31.205.106	255.255.0.0	172.31.205.1
		PC-97	172.31.205.107	255.255.0.0	172.31.205.1
		PC-98	172.31.205.108	255.255.0.0	172.31.205.1
		PC-99	172.31.205.109	255.255.0.0	172.31.205.1
		PC-100	172.31.205.110	255.255.0.0	172.31.205.1
UBICACIÓN	DIRECCION IP	PUNTOS DE ACCESO	DIRECCION IP DE HOST	MASCARA DE SUBRED	GATEWAY
IMPRESORAS	172.31.205.0	IMP_01	172.31.205.111	255.255.0.0	172.31.205.1
		IMP_02	172.31.20.112	255.255.0.0	172.31.205.1
		IMP_03	172.31.205.113	255.255.0.0	172.31.205.1
		IMP_04	172.31.205.114	255.255.0.0	172.31.205.1
		IMP_05	172.31.205.115	255.255.0.0	172.31.205.1
		IMP_06	172.31.205.116	255.255.0.0	172.31.205.1
		IMP_07	172.31.205.117	255.255.0.0	172.31.205.1
		IMP_08	172.31.205.118	255.255.0.0	172.31.205.1
		IMP_09	172.31.205.119	255.255.0.0	172.31.205.1
		IMP_10	172.31.205.120	255.255.0.0	172.31.205.1

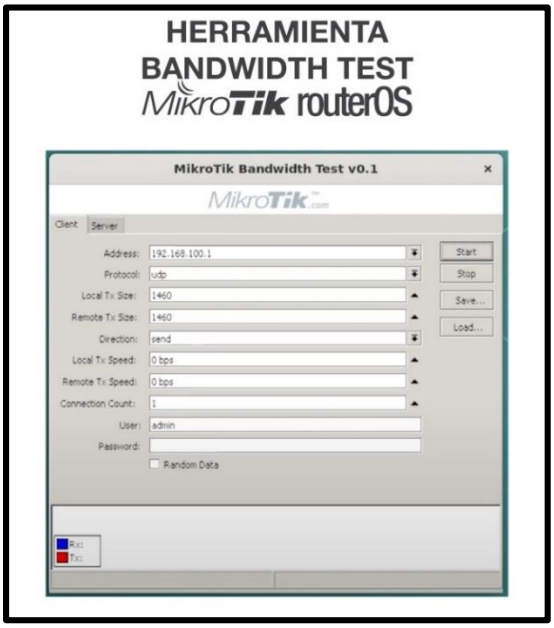
4.1.4. Pruebas y validación del sistema

Las pruebas realizadas para la validación de la clase de red fueron las siguientes:

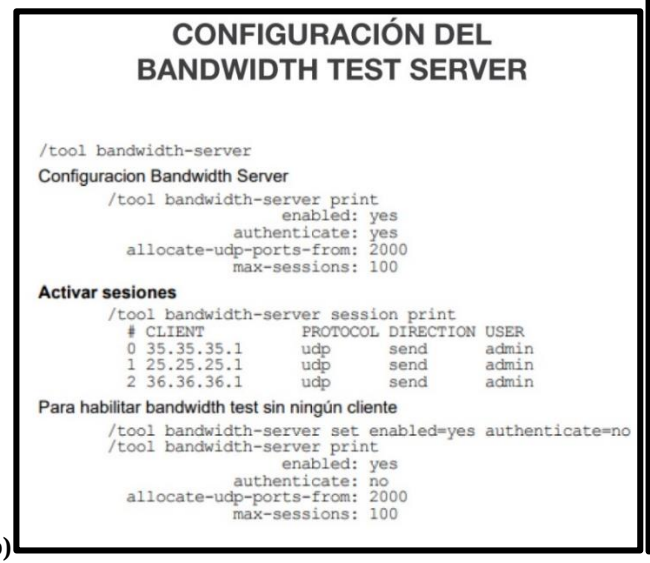
Pruebas Unitarias

Las pruebas unitarias comprueban la exactitud de los aspectos individuales de la configuración del dispositivo, como la configuración IP (V4 O V6) correcta, su uso es bastante simple.

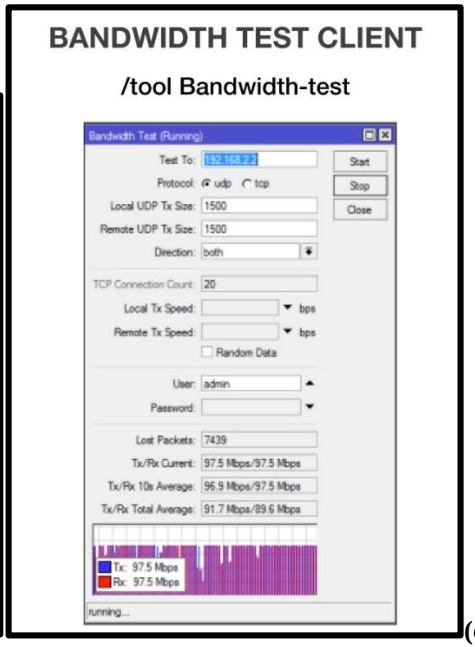
Bandwidth Test: esta herramienta permite pedir el Throughput de otro Router Mikrotik (cable o Wireless) ayudando así a descubrir redes con cuello de botella de las conexiones de la UGEL Huanca Sancos. Trabaja con los protocolos TCP y UDP para hacer los test como se muestra en las siguientes figuras 4.22.



(a)



(b)



(c)

Figura 4.22: (a), (b) y (c) Pasos para realizar Bandwidth Test

Se realizó las pruebas para el control del tráfico de red, Latencia, Jitter y en comunicación y seguridad detección de intrusiones obteniendo los resultados estadísticos en Pretest y Postest adjuntando todos los datos correspondientes para la conclusión satisfactorios.

Las pruebas unitarias son simples y directas: la causa raíz de la falla se aclara de inmediato cuando falla una prueba, pero dice poco sobre el comportamiento de la red de extremo a extremo. No es difícil imaginar situaciones en las que pasen todas las pruebas unitarias, pero la red no entregue un solo paquete.

Pruebas funcionales

Las pruebas funcionales verifican el comportamiento de un extremo a otro para escenarios específicos, como si los paquetes DNS del host1 pueden llegar al servidor, los enrutadores de hoja del centro de datos tienen una ruta predeterminada que apunta a la columna vertebral, se prefiere un enrutador de borde específico para el tráfico a Google.com, y el tráfico utiliza la ruta de respaldo cuando falla un enlace.

A diferencia de las pruebas unitarias, las pruebas funcionales pueden proporcionar garantías sobre los comportamientos de la red. Sin embargo, al igual que con las pruebas de software, su talón de Aquiles es la integridad. Proporciona garantías de corrección solo para escenarios probados, mientras que el espacio de posibles paquetes, fallas y rutas externas es astronómicamente grande. Solo para los paquetes, hay más de un billón de paquetes TCP posibles (encabezado de 40 bytes).

Debido a que es imposible probar todos los escenarios, las garantías de corrección de las pruebas funcionales son intrínsecamente incompletas. El hecho de que unos pocos (o incluso cien) paquetes de prueba no puedan cruzar el límite de aislamiento no significa que ningún paquete pueda hacerlo. La integridad de las garantías es donde entra en juego la verificación.

Verificación

La verificación garantiza la corrección para todos los escenarios posibles dentro de un contexto bien definido. Es un enfoque formal (matemático), aunque el término "verificación" a veces se usa incorrectamente para otros tipos de controles. Ejemplos de

garantías que puede proporcionar la verificación son: todos los paquetes DNS, independientemente del host o puerto de origen, pueden llegar al servidor DNS; se prefiere la ruta a través de un enrutador fronterizo específico para todos los destinos externos; y los servicios permanecen disponibles a pesar de cualquier falla en el enlace. Tales sólidas garantías ofrecen a los ingenieros de redes la confianza para evolucionar rápidamente sus redes.

4.2. Solución Experimental

4.2.1. Realización de experimentos

Para realizar la validación de que la implementación cumple con lo esperado, se realizó la recolección de los resultados obtenidos de la medición de la latencia y del Jitter, registrando todo lo recolectado en las fichas de recolección de datos, en dos tiempos, el primer tiempo antes de la implementación de la nueva red, y el segundo tiempo después de su implementación (Ver anexo 5,6 y 7).

4.2.2. Recolección y procesamiento de datos

Para el procesamiento de datos, se utilizó el software SPSS en su versión 25, para de esta manera poder realizar el procesamiento de los resultados y con el fin de rechazar la hipótesis nula y aceptar la alterna, iniciando por el análisis descriptivo:

- **Presentación de datos.**

Se presentan una muestra de la recolección de datos de los instrumentos utilizados durante esta investigación.

Datos obtenidos del instrumento N° 01 Nivel de Latencia

Tabla 4.18: Análisis descriptivo para el indicador nivel de Latencia

Ficha de Registro 01			Formula
Variable Dependiente	Comunicación y Seguridad		FORMULA
Indicador	Nivel de latencia		IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)
Items	PRE-TEST	POST-TEST	DIFERENCIA
Item	Promedio del nivel de latencia (Ms)	del nivel de latencia (Ms)	Diferencia Latencia
1	79.13	27.17	51.96
2	80.43	23.91	56.52
3	73.91	22.83	51.09
4	96.74	26.63	70.11
5	72.83	14.57	58.26
6	102.17	27.17	75.00
7	58.70	34.78	23.91
8	71.13	31.20	39.93
9	80.43	33.91	46.52
10	68.48	23.15	45.33
11	60.87	15.76	45.11
12	79.84	35.22	44.62
13	57.61	33.91	23.70
14	91.30	29.02	62.28
15	78.48	35.27	43.21
16	71.09	31.41	39.67
17	73.70	34.02	39.67
18	91.65	25.43	66.22
19	73.70	19.38	54.32
20	71.09	31.41	39.67
92	56.52	19.78	36.74

En la tabla 4.18 se muestran los datos de nuestra ficha de registro para el primer indicador.

Datos obtenidos del instrumento N° 02: Nivel de Jitter

Tabla 4.19: Análisis descriptivo para el indicador nivel de Jitter

Ficha de Registro 02			Formula
Variable Dependiente	Comunicación y Seguridad		FORMULA
Indicador	Nivel de Jitter		Sumatoria de ms / Número de equipos evaluados
Items	PRE-TEST	POST-TEST	DIFERENCIA
Item	Promedio de nivel de jitter	Promedio de nivel de jitter	Diferencia Nivel Jitter
1	37.50	19.01	18.49
2	41.30	19.79	21.51
3	44.78	16.74	28.04
4	45.65	18.03	27.62
5	44.93	15.54	29.39
6	46.99	14.57	32.42
7	43.36	13.41	29.95
8	39.98	15.59	24.39
9	38.53	16.66	21.87
10	45.79	14.86	30.93
11	42.48	16.93	25.54
12	42.36	19.45	22.91
13	45.78	12.17	33.61
14	38.65	13.37	25.28
15	34.91	12.21	22.71
16	37.57	14.13	23.43
17	53.35	14.39	38.96
18	49.66	15.57	34.10
19	37.57	17.32	20.25
20	37.55	20.54	17.01
92	25.43	17.83	7.61

En la tabla 4.19: se muestran los datos de nuestra ficha de registro para el 2do. Indicador

Datos obtenidos del instrumento N° 03 Índice de detección de intrusiones

Tabla 4.20: Análisis descriptivo para Índice de detección de intrusiones

Ficha de Registro 03			Formula
Variable Dependiente	Comunicación y Seguridad		FORMULA
Indicador	Índice de detección de intrusiones		IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)
Items	PRE-TEST	POST-TEST	DIFERENCIA
Item	Intrusiones detectadas	Intrusiones detectadas	Intrusiones totales
1	50.00	85.71	-35.71
2	33.33	62.50	-29.17
3	36.36	100.00	-63.64
4	33.33	100.00	-66.67
5	25.00	71.43	-46.43
6	40.00	75.00	-35.00
7	45.45	85.71	-40.26
8	40.00	100.00	-60.00
9	27.27	83.33	-56.06
10	33.33	85.71	-52.38
11	33.33	100.00	-66.67
12	44.44	71.43	-26.98
13	60.00	83.33	-23.33
14	36.36	71.43	-35.06
15	41.67	80.00	-38.33
16	40.00	83.33	-43.33
17	44.44	100.00	-55.56
18	50.00	80.00	-30.00
19	40.00	66.67	-26.67
20	40.00	66.67	-26.67
92	50.00	85.71	-35.71

En la tabla 4.20: se muestran los datos de nuestra ficha de registro para el 3er. Indicador

- **Análisis descriptivo**

A continuación, se realiza el análisis descriptivo en donde se puede visualizar de manera general los resultados obtenidos de la evaluación antes de implementar la nueva estructura de red y después de su implementación.

Indicador 01: Nivel de Latencia

Los resultados descriptivos del primer indicador nivel de latencia del pre – test y post – test.

Tabla 4.21. Estadísticos Descriptivos nivel de latencia Pretest y Postest

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Nivel de Latencia PRETEST	92	49,57	102,17	74,1717	11,54642

Nivel de Latencia POSTTEST	92	13,37	42,93	28,0700	8,36895
N válido (por lista)	92				

En la tabla 4.21: se observan los resultados estadísticos descriptivos. En el Pre-test se obtuvo la media de 74.17 con el mínimo de 49.57 y al máximo de 102.17 a diferencia en el Post-test se obtuvo una media de 28.07 con el mínimo de 13.37 y al máximo de 42.93, aquí se observa la diferencia entre el antes y el después de la implementación de infraestructura de datos y seguridad. Tal como se grafica en la figura 4.23.

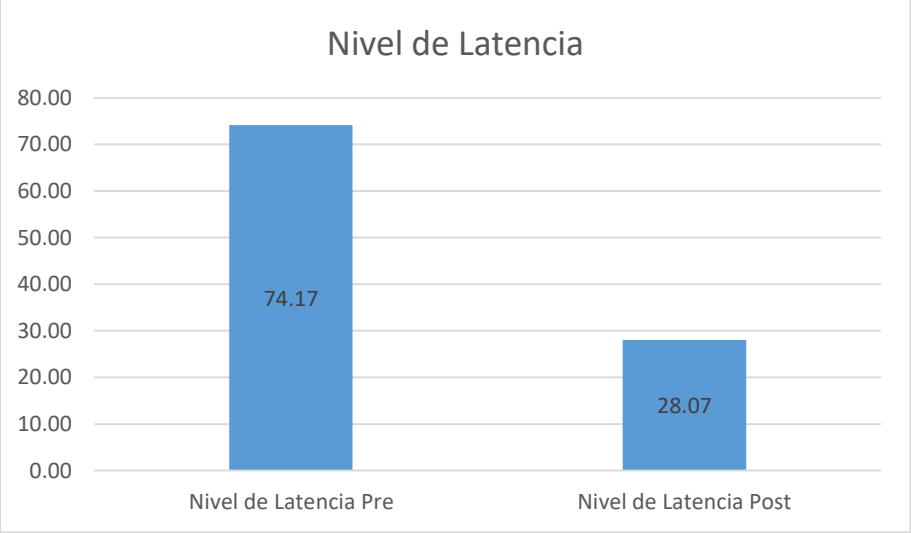


Figura 4.23: Nivel de latencia Pretest y Postest

Indicador 02 Nivel de Jitter

Los resultados descriptivos del primer indicador nivel de Latencia del Pretest y Postest.

Tabla 4.22. Estadísticos Descriptivos nivel de Jitter Pretest y Postest

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Nivel_de_Jitter_PreTest	92	16,52	53,35	35,5337	6,54743
Nivel_de_Jitter_PostTest	92	11,21	21,47	17,3100	2,50724
N válido (por lista)	92				

En la tabla 4.22: se observan los resultados estadísticos descriptivos. En el Pre-test se obtuvo la media de 35.53 con el mínimo de 16.52 y al máximo de 53.35 a diferencia en el Post test se obtuvo una media de 17.31 con el mínimo de 11.21 y al máximo de 21.47,

aquí se observa la diferencia entre el antes y el después de la implementación de infraestructura de datos y seguridad. Tal como se grafica en la figura 4.24.

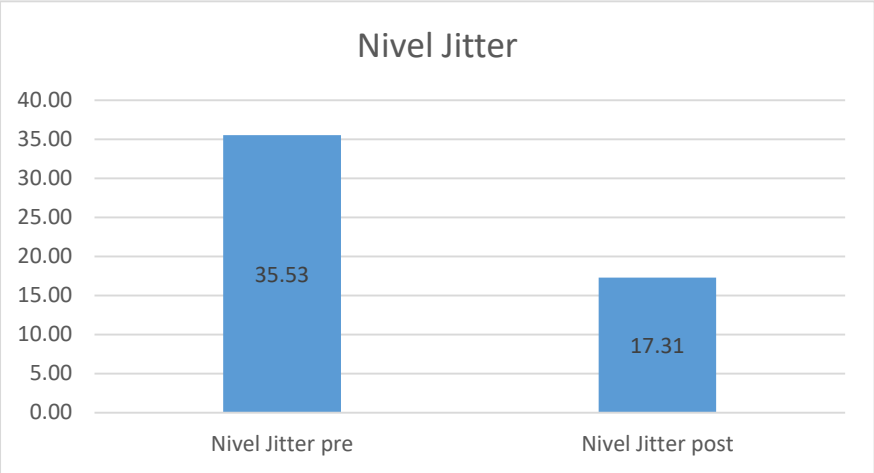


Figura 4.24: Nivel de Jitter Pretest y Postest

Indicador 03 Índice de detección de intrusiones

Tabla 4.23: Estadísticos Descriptivos Índice de detección de intrusiones Pretest y Postest

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
I_Detección_de_Intrusiones_PreTest	92	51,43	100,00	78,7182	13,11140
I_Detección_de_Intrusiones_PostTest	92	25,00	60,00	44,0367	8,11953
N válido (por lista)	92				

En la tabla 4.23 se observan los resultados estadísticos descriptivos. En el Pretest se obtuvo la media de 78.71 con el mínimo de 51.43 y al máximo de 100.00 a diferencia en el Post test se obtuvo una media de 44.03 con el mínimo de 25.00 y al máximo de 60.00, aquí se observa la diferencia entre el antes y el después de la implementación de infraestructura de datos y seguridad. Tal como se grafica en la figura 4.25.

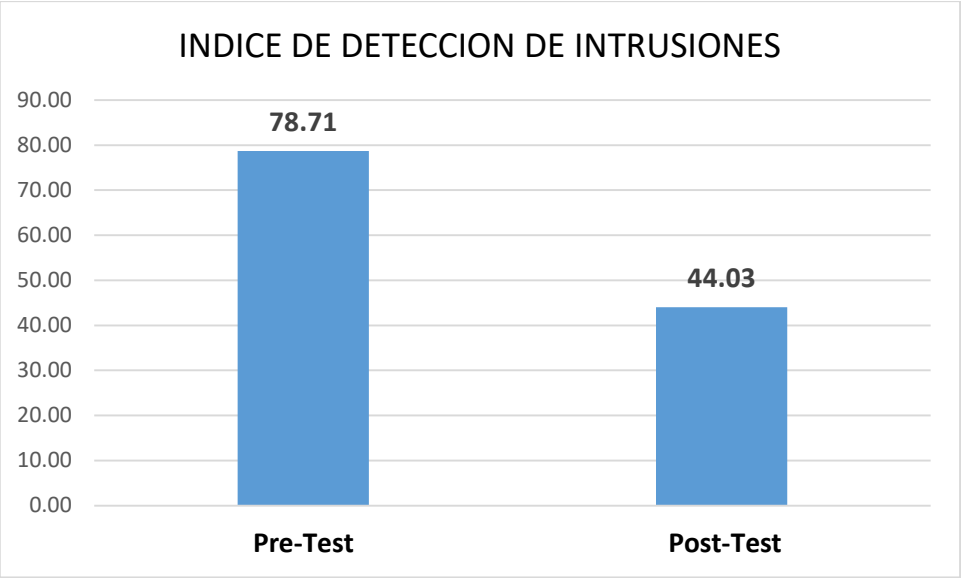


Figura 4.25: Nivel de latencia Pretest y Postest

- **Análisis inferencial**

Prueba de normalidad

La prueba de normalidad permite validar si es que la distribución es normal o no normal, la regla menciona que se debe utilizar los resultados del autor Shapiro wilk si es que la muestra evaluada es menor o igual a 50 individuos, de lo contrario se utiliza Kolmogorov. Luego se realiza la evaluación del nivel de significancia, si el nivel de significancia en ambos casos es mayor a 0.05 la distribución será de tipo normal, de lo contrario será no normal.

Indicador N° 01 Nivel de Latencia

Para este indicador se utiliza la prueba de normalidad de Kolmogorov-Smirnov

Tabla 4.24: Prueba de normalidad para el indicador nivel de latencia

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,053	92	,200*	,986	92	,439
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

En la tabla 4.24, se obtuvo el resultado de la diferencia entre el Pre-Test y Post-test. El Sig. Fue del valor de 0.200, esto viene a ser > 0,05. Entonces se afirma que los datos tienen una distribución normal de tal modo se debe usar la prueba paramétrica T_Student.

También se puede ver el comportamiento de la curva normal de la diferencia del Pretest y Postest. Esto lo podemos ver en la Figura 4.26.

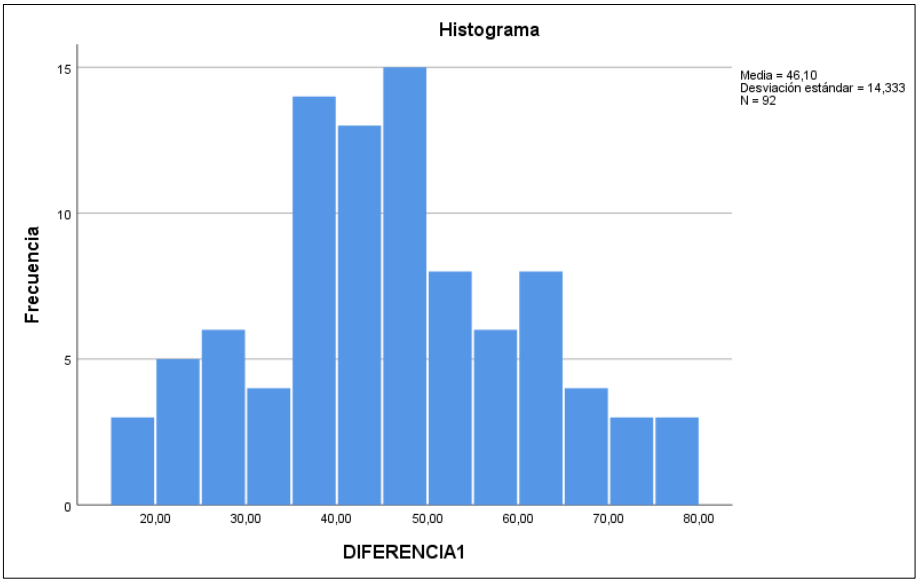


Figura 4.26: Diferencia Nivel de latencia

Prueba de hipótesis

El objetivo de la prueba de hipótesis es poder aceptar la hipótesis alterna, la cual es un supuesto que afirma lo que se espera respecto a la implementación de la nueva red, y también se rechaza la hipótesis nula que es aquella que niega la hipótesis alterna. Así se determina el nivel de influencia de la variable independiente sobre la dependiente.

- **Hipótesis de investigación n° 01**

H1: La implementación de infraestructura de redes mejora el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos.

H0: La implementación de infraestructura de redes No mejora el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos.

Indicador Nivel de Latencia

Prueba de muestras emparejadas								
	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. estándar	Desv. Error	95% de intervalo de Inferior	Superior			
Nivel de Latencia	46,10174	14,33317	1,49434	43,13342	49,07005	30,851	91	,000

Tabla 4.25: Estadística de muestras emparejadas nivel de Latencia

Según la tabla 4.25 podemos interpretar los siguientes datos

t=30.851

gl (grado de libertad) = 91

Valor de contraste 1.65821 ver detalle en el anexo 8 y 9.

Conclusión.

El valor t es de 30.851 está en la región de rechazo, por tanto, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha) donde, la implementación de infraestructura de redes mejora el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos con un 95% de confianza. Consulte la siguiente Figura 4.27.

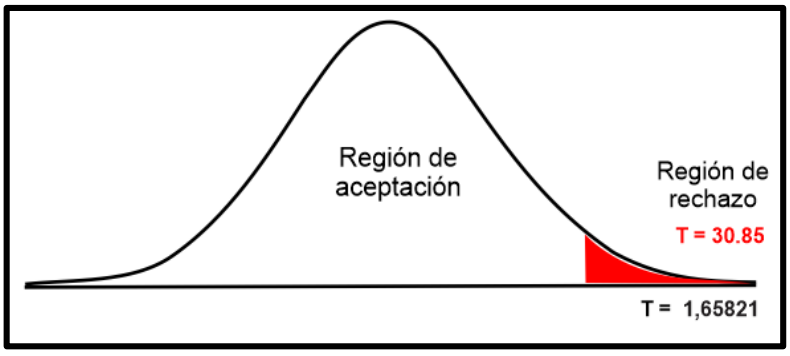


Figura 4.27: Distribución de T_Student

Indicador N° 02 Nivel de Jitter

Para este indicador se utiliza la prueba de normalidad de Kolmogorov-Smirnov

Tabla 4.2196: Prueba de normalidad para el indicador nivel de Jitter

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,058	92	,200*	,990	92	,691

*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

En la Tabla 4.26: se obtuvo el resultado de la diferencia entre el Pre-Test y Post-test. El Sig. Fue del valor de 0.200, esto viene a ser > 0,05. Entonces se afirma que los datos tienen una distribución normal de tal modo se debe usar la prueba paramétrica T_Student.

También se puede ver el comportamiento de la curva normal de la diferencia del Pretest y Postest. Esto lo podemos ver en la Figura 4.28.

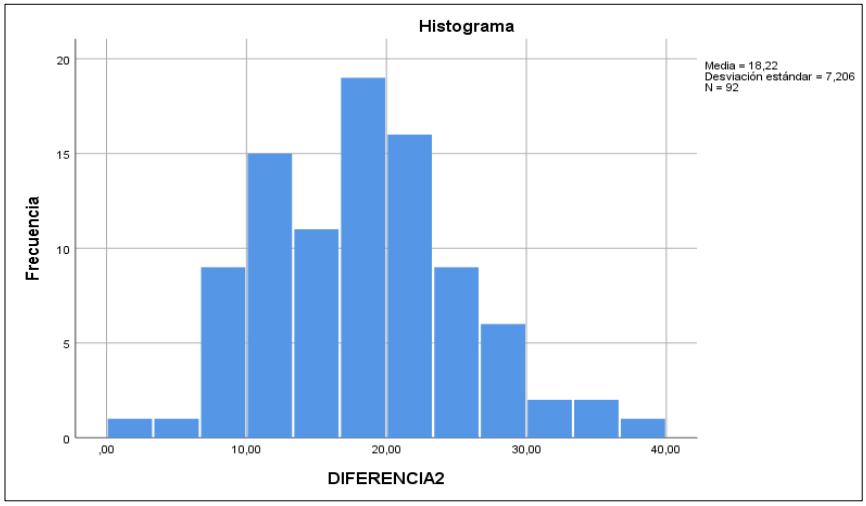


Figura 4.28: Diferencia Nivel de Jitter

Tabla 4.27: Estadística de muestras emparejadas Nivel de Jitter

PRUEBA DE MUESTRAS EMPAREJADAS								
	Diferencias emparejadas							
				95% de intervalo de confianza de la diferencia				
	Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1 Nivel de Jitter PreTest - PostTest	18,22370	7,20579	,75126	16,73142	19,71597	24,258	91	,000

Según la tabla 4.27: podemos interpretar los siguientes datos

t=24,258

gl (grado de libertad) = 91

Valor de contraste 1.65821 ver detalle en el anexo 10 y 11.

Conclusión.

El valor t es de 24,258está en la región de rechazo, por tanto, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha) donde, la implementación de infraestructura de redes mejora el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos con un 95% de confianza. Consulte la siguiente figura 4.28.

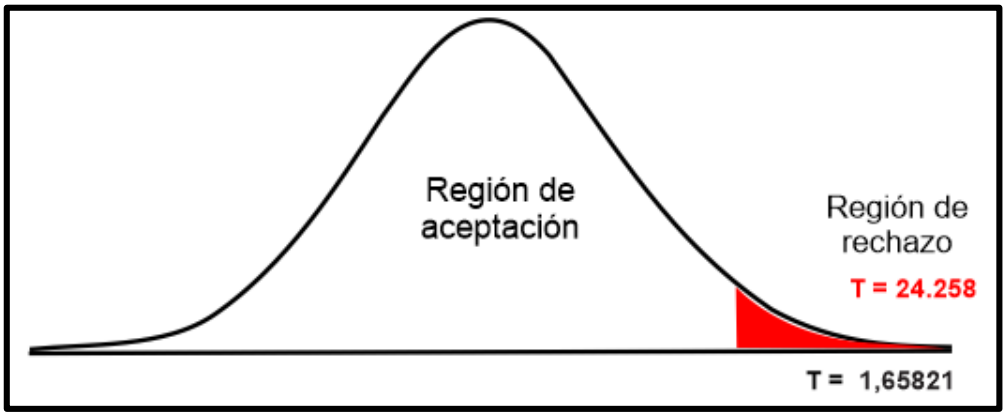


Figura 4.29: Distribución de T_Student

Indicador N° 03 índice de detección de intrusiones

Para este indicador se utiliza la prueba de normalidad de Kolmogorov-Smirnov porque el número de muestras es > 50. Ver más detalles en anexo 14.

Tabla 4.28: Prueba de normalidad para el indicador índice de intrusiones

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,138	92	,000	,967	92	,021
a. Corrección de significación de Lilliefors						

En la tabla 4.28, se obtuvo el resultado de la diferencia entre el Pre-test y Post-test. El significante (Sig), fue del valor de 0.000, esto viene a ser < 0,05. Entonces se afirma que los datos tienen una distribución no normal de tal modo se debe usar la prueba no paramétrica rangos de Wilcoxon. Ver detalle en anexo 12 y 13.

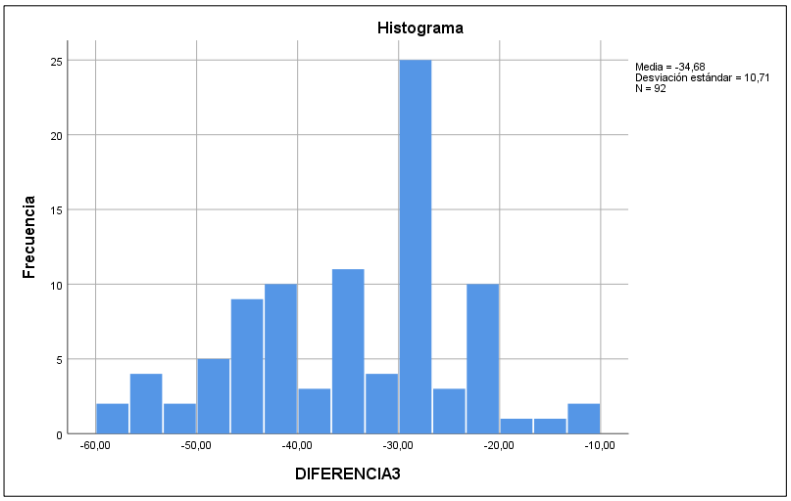


Figura 4.30: diferencia de índice de detección de instrumentos

Prueba de hipótesis

El objetivo de la prueba de hipótesis es poder aceptar la hipótesis alterna, la cual es un supuesto que afirma lo que se espera respecto a la implementación de la nueva red, y también se rechaza la hipótesis nula que es aquella que niega la hipótesis alterna. Así se determina el nivel de influencia de la variable independiente sobre la dependiente.

- **Hipótesis de investigación n° 02**

H1: La implementación de infraestructura de redes mejora la seguridad de la red en la UGEL Huanca Sancos.

H0: La implementación de infraestructura de redes NO mejora la seguridad de la red en la UGEL Huanca Sancos.

Indicador índice de detección de intrusiones

A continuación, se muestra en la tabla 4.29, la prueba de rangos para el indicador índice de detección de intrusiones.

Tabla 4.29: Prueba de Rangos de Wilcoxon del Pretest y Postest del indicador índice de detección de intrusiones

Rangos				
		N	Rango promedio	Suma de rangos
Detección de Intrusiones PostTest – I Detección de Intrusiones PreTest	Rangos negativos	0[a]	,00	,00
	Rangos positivos	92[b]	46,50	4278,00
	Empates	0[c]		
	Total	92		
a. I Detección de Intrusiones PostTest < I Detección de Intrusiones PreTest				

Tabla 4.30: Estadísticos de prueba Wilcoxon para nuestra

Estadísticos de prueba	
	Índice Detección de Intrusiones PostTest – Índice Detección de Intrusiones PreTest
Z	-8,331[b]
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

En la tabla 4.30, se observa que el nivel de significancia es de .000, en consecuencia, este valor es < 0.05.

Considerando lo siguiente tenemos:
Si, P (significancia) < 0.05, entonces se rechaza H0.
Si, P (significancia) > 0.05, entonces se acepta H0.

Como el resultado de P resultó 0,000 siendo p < 0,05, entonces se rechaza la hipótesis nula y se acepta la hipótesis alterna. Esto nos da como resultado que la implementación de infraestructura de redes mejora la seguridad de la red en la UGEL Huanca Sancos.

CAPITULO V
DISCUSION DE RESULTADOS

5.1. Interpretación de resultados tecnológicos

La implementación de la nueva infraestructura de red permitió la mejora de la transmisión de la información y los datos entre los puntos, reduciendo la latencia y el nivel de Jitter, mejorando la fluidez de los datos como también la seguridad de la red en la UGEL Huanca Sancos. La mejora en la latencia está en el orden del 46% debido a la nueva instalación y configuraciones y en relación al nivel de Jitter en una mejoría del 18%.

Anteriormente existía mucha latencia en la transmisión de los datos, como por ejemplo en el área de administración en muchas ocasiones los envíos de documentación de archivos comprimidos de más de 21 Mb se demoraban de 2 a 3 minutos en horario de oficina. En la actualidad los envíos de documentación están alrededor de 15 a 35 seg.

En cuanto al tema de la seguridad de los datos, antes de la realización de nuestra investigación, solamente se contaba con la instalación por defecto que trae el sistema operativo Windows 10 como es el firewall, también se recurría al antivirus o a los anti-malware. Esto por lo general causaba perdida de datos en la UGEL Huanca Sancos, La intercepción era uno de los ataques más frecuentes que afectaban los datos de la institución en mención. Luego la implementación de la infraestructura de redes, también se ha implementado un IDS (sistema para la detección de intrusos) basado en red para monitorear los datos que circulan por la red. De 10 a 12 intrusiones que se suscitaban en la UGEL Huanca Sancos como caída en el ancho de banda o acceso no autorizado a nuestra base datos, se redujo a 2 o 3 intrusiones que pueden ser manejados por el encargado de sistemas.

5.2. Interpretación de resultados experimentales

Variable especifica Y1

Para la interpretación de resultados con respecto al o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos, se tomó la Media, del Pre-test y Post-test, del cuadro estadístico descriptivo, visto en el capítulo 4, ver Tabla 5.1.

Tabla 5.1 Nivel de Latencia para la mejora de datos

	Pre-Test	Post-Test	Mejora	% de mejora
Media	74.17	28.07	46.10	62.0%

Con respecto al nivel de latencia en la tabla 5.1 se confirma que la implementación de infraestructura de redes ha reducido la latencia en un 46.10%. En el Pre-test sin la implementación la implementación de infraestructura de redes, el tiempo de latencia eran de 74,17%, sin embargo, luego de la implementación de infraestructura de redes este se redujo al 28,07%, influyendo la mejora por medio de la implementación de una nueva infraestructura de redes.

Variable especifica Y2

Par la interpretación de resultados con respecto de Jitter, se tomó la Media, del Pre-test y Post-test, del cuadro estadístico descriptivo.

Tabla 5.2: Nivel de Jitter para la mejora de datos

	Pre-Test	Post-Test	Mejora	% de mejora
Media	35.53	17.31	18.22	51.2%

Con respecto al nivel de Jitter en la Tabla 5.2, se confirma que la implementación de infraestructura de redes ha reducido la latencia en un 18.22%. En el Pre-test sin la implementación la implementación de infraestructura de redes, el tiempo de latencia eran de 35.53%, sin embargo, luego de la implementación de infraestructura de redes este se redujo al 17.31%, influyendo la mejora por medio de la implementación de una nueva infraestructura de redes.

Variable especifica Y3

Par la interpretación de resultados con respecto índice de detección de intrusiones, se tomó la Media, del Pre-test y Post-test, del cuadro estadístico descriptivo.

Tabla 5.3: Índice de detección de intrusiones para la mejora de datos

	Pre-Test	Post-Test	Reducción	% de reducción
Media	**78.17**	**44.03**	**34.14**	**43.67**

Con respecto al índice de detección de intrusiones en la Tabla 5.3 se confirma que la implementación de infraestructura de redes ha reducido índice de detección de intrusiones en un 34.14%. En el Pre-test sin la implementación de infraestructura de redes, el índice de detección de intrusiones era de 78.17%, sin embargo, luego de la implementación de infraestructura de redes este se redujo a 44-03. Esto nos da una mejora en la detección de intrusiones de 43.67%, influyendo en la mejora en la seguridad de la red en la UGEL Huanca Sancos.

Variable general X

La interpretación de la hipótesis general se basa en los resultados obtenidos por cada uno de sus dimensiones, determinando el rechazo la hipótesis nula (Ho).

Para comparación de hipótesis, se mide la variable comunicación y seguridad de datos de acorde a sus dimensiones, obteniendo los siguientes resultados por cada dimensión, según las tablas 5.1, 5.2 y 5.3.

Tabla 5.4 Comunicación y Seguridad De Datos

Comunicación y Seguridad De Datos				
	Y1 Nivel de Latencia	**Y2** Nivel de Jitter	Y3 Índice de Intrusiones	**Promedio (%)**
% De Mejora Post-test Pre-Test	**62.00**	**51.20**	**43.67**	**52.29**

En la Tabla 5.4, puede verificar que las dimensiones de la variable, Comunicación y Seguridad de datos han mejorado con La implementación de infraestructura de redes, el nivel

de Latencia se obtuvo una reducción del 62.10% en el Nivel de Jitter, una reducción del 51,20% y en la seguridad de datos el Índice de Intrusiones una mejora del 43.67%. Obteniendo un porcentaje de 52.29% de mejora mediante la implementación de infraestructura de redes de comunicación y seguridad de datos en la UGEL Huanca Sancos.

Confirmando que la implementación de infraestructura de redes permite mejorar la comunicación y seguridad de datos en la UGEL Huanca Sancos. De esta manera es confirmada la hipótesis del presente estudio.

CONCLUSIONES

Se logró los objetivos de la investigación adquiriendo nuevos conocimientos el cual hace un aporte importante a la UGEL Huanca Sancos.

1. En nuestra investigación se ha logrado el objetivo principal, que ha sido Determinar cómo la implementación de infraestructura de redes mejora la comunicación y seguridad de datos en la UGEL Huanca Sancos. Mediante la medición y validación de las hipótesis, se alcanzaron nuestros objetivos que nos habíamos planteados.

2. Con respecto a nuestro objetivo específico, que era Determinar en qué medida la implementación de infraestructura de redes influirá en el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos. Podemos decir que este objetivo se ha cumplido porque mejora la comunicación de la red y el nivel de latencia se redujo de 74.17 ms (100%) a 28.07 ms (37.84%). Esto dio lugar a una reducción del nivel de latencia de 46.10 ms (62.15%).

3. Del mismo modo en cuanto al nivel de Jitter, se redujo de 35.53 ms (100%) a 17.31 ms (48.71%). Esto dio lugar a una reducción del nivel de latencia de 18.22 ms (51.28%), logrando la meta de nuestro estudio.

4. Por ultimo con respecto a nuestro objetivo específico, que era establecer como la implementación de infraestructura de redes influirá en la seguridad de la red en la UGEL Huanca Sancos. Sin la implementación de la infraestructura de redes el Pre-Test dio un resultado de 78.17% y con la implementación de infraestructura de redes para el proceso estudiado se redujo al 44.03%, mostrando una reducción del 34.14%. La mejora en cuanto al índice de intrusiones se logró un porcentaje de 43.67% para el proceso actual, confirmando la hipótesis que la implementación de infraestructura de redes mejora la comunicación y seguridad de datos en la UGEL 312 Huanca Sancos.

RECOMENDACIONES

- Mantener el registro constante de los datos y valores del comportamiento de la transmisión de información, para poder realizar un comparativo mensual de los resultados obtenidos y así poder mejorar la toma decisiones.
- Dar un mantenimiento periódico del cableado para poder garantizar su estabilidad y calidad.
- Plasmar una capacitación a todos los trabajadores de la UGEL Huanca Sancos sobre el uso adecuado de las nuevas tecnologías que se implementara de tal forma que familiaricen de forma apropiada y se aproveche al máximo sus capacidades.
- Realizar investigaciones sobre la implementación una red convergente para mejorar los servicios internet y comunicación en la UGEL Huanca Sancos.
- Se recomienda no saturar la red con descargas masivas o uso que no sea necesario para el manejo de información de la UGEL Huanca Sancos.

REFERENCIAS BIBLIOGRAFICAS

[1] J. Galdos Guizado y Y. I. Benites Sosa. Tesis de Pregrado. “Diseño y simulación de la implementación de una red convergente para mejorar los servicios de comunicación de la municipalidad distrital de Manta 2015”, Facultad de ingeniería electrónica – sistemas, UNH, Huancavelica, Perú, 2018 [En línea] Disponible: http://repositorio.unh.edu.pe/handle/UNH/1970

[2] V. C. Poma Torres. Tesis de Pregrado. “rediseño de redes mediante la metodología top down network design para mejora de la red de datos de los equipos de tic en la DIRESA Junín, Facultad de ingeniería sistemas y computación, UPLA, Huancayo, Perú, 2017 [En línea] Disponible: https://hdl.handle.net/20.500.12848/303

[3] L. A. Guerra Menéndez, H. G Maquera Quispe y M. G. del Carmen Delgado. (2017) Mejoramiento en el uso de internet en la escuela profesional de contabilidad de la universidad nacional de Huancavelica. Revista [En línea] Vol. (2) pp. 130-140. Disponible: https://revistas.unjbg.edu.pe/index.php/cyd/article/download/739/751/1386

[4] R. E. de la Cruz Vargas. Tesis de pregrado. “Propuesta de políticas, basadas en buenas practicas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita 2016”. Universidad Católica Los Ángeles Chimbote, Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistemas. Piura, 2016 [En línea] Disponible: https://hdl.handle.net/20.500.13032/890

[5] UGARTE L. Implementación de un sistema de administración de redes usando plataformas de software libre para mejorar el servicio de internet inalámbrico en la ciudad de tayabamba-pataz. Universidad Señor de Sipán. 2016

[6] Rojas M. Diseño y Simulación de una red basada en VLAN’s para mejorar la comunicación de datos en la empresa Grupo El Saber S.A.C. Universidad César Vallejo. 2018

[7] Chavez D. Diseño de la red de comunicaciones para mejorar la transmisión de datos de la municipalidad distrital de chavín de huántar, provincia de huari – Ancash 2018. Universidad nacional santiago antúnez de mayolo. 2018

[8] Morón P. Implementación de un centro de operaciones de red para la empresa Redycom Solutions bajo el marco de trabajo ITILv4 en la ciudad de Lima - 2019. Universidad Tecnológica del Perú. 2020

[9] Fuerte R. Diseño de un sistema de monitoreo de red LAN para una empresa Pyme, para mejorar la disponibilidad y la gestión de red, tomando como referencia el modelo de gestión de red en OSI. Universidad Nacional Mayor de San Marcos. 2021

[10] Valladares G. Influencia del cableado estructurado en la plataforma de comunicaciones de voz - Programa Juntos Cerro de Pasco. Universidad nacional Daniel Alcides Carrión. 2019

[11] L. P. Zheng Huang. Tesis de pregrado. “Diseño e implementación de una red LAN para la empresa Palinda”. Colegio de Ciencias e Ingeniería, USFQ, Quito,2017 [En línea] Disponible: http://repositorio.usfq.edu.ec/handle/23000/6383

[12] X.F. López Andrade. Tesis de pregrado. “rediseño de la red con calidad de servicios para datos y tecnología de voz sobre IP en el ilustre Municipio de Ambato. Departamento de investigación, postgrados y autoevaluación. Ambato, Ecuador, 2008 [En línea] Disponible: https://repositorio.pucesa.edu.ec/bitstream/123456789/645/1/85008.PDF

[13] J. Marugán Merinero. Tesis de pregrado. “Diseño de infraestructura de red y soporte informático para un centro público de educación infantil y educación”. Escuela Universitaria de Informática Universidad Politécnica de Madrid, 2010 [En línea] Disponible: https://oa.upm.es/4976/3/PFC_JUAN_MARUGAN_MERINEROx.pdf

[14] S. A. Espinosa Silva. Tesis de pregrado. “Proyecto de reingeniería de la infraestructura de la red LAN de SYC S.A”. Universidad Pontificia Bolivariana. Escuela de Ingeniería y Administración, Facultad de Ingeniería Electrónica Bucaramanga.2008 [En línea] Disponible: http://hdl.handle.net/20.500.11912/350

[15] L.A. Herrera Lara. Tesis de pregrado. “Implementacion de un centro de operaciones de seguridad de redes (NSOC) usando herramientas open source para la infraestructura industrial de la empresa eléctrica Quito”. Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica. Quito.2008 [En línea] Disponible: http://bibdigital.epn.edu.ec/handle/15000/22864

[16] N. A. Altamirano López y F. R. Sequeira Jiménez Tesis de Master. “Análisis de amenazas relacionadas a los metadatos y correo electrónico, e implementación de un aplicativo como herramienta para disminuir el riesgo de un ataque en el que se empleen estos elementos”. Universidad Nacional de Ingeniería, Facultad de Ciencias y Sistemas, Maestría en Gestión de la seguridad de la Información. Nicaragua. 2016 [En línea] Disponible: https://core.ac.uk/download/pdf/250144002.pdf

[17] Cordero P, Marcillo E. Propuesta de diseño del Data center y reestructuración de la red de datos de la universidad estatal de bolívar. Universidad Politécnica Salesiana sede Quito. 2018

[18] Olivas C. Aplicación de metodología para el diseño e implementación de redes de Campus Universitario. Universidad de Chile. 2019

[19] Iturralde P, Lazo V. Implementación de un Laboratorio de Redes de Telecomunicaciones utilizando Infraestructura Mikrotik. Universidad del Azuay. 2017

[20] Orozco P. Instalación de una red 802.11n de largo alcance que provea servicios de Internet a la Escuela Telesecundaria: “María Montessori”, y servicios de Telemedicina a localidades del Municipio de Ometepec, Gro. Instituto tecnológico de Acapulco. 2019

[21] M. Lederkremer, “Redes Informáticas” 1ra edición Buenos Aires Argentina, 2019 [En Línea] Disponible:

https://books.google.com.pe/books?id=7frADwAAQBAJ&printsec=frontcover&dq=redes+informaticas&hl=es&sa=X&redir_esc=y#v=onepage&q&f=false

[22] IBM. Seguridad de datos [En línea] Disponible: https://www.ibm.com/es-es/topics/data-security

[23] M. Soriano. Seguridad en redes y seguridad de la información 1ra Edicion. Czech Republic, 2013 [En línea] Disponible: https://psm.fei.stuba.sk/pages/47/Seguridad_de_Red_e_Informacion.pdf

[24] P.H. Escobar C. J.L Bilnao R. "Investigación y educación superior" 2da edición Universidad Libre – Colombia. 2020 [en linea] Disponible: https://books.google.com.pe/books?id=W67WDwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[25] L.Birolli, J.Natwichai y T. Enokido. "Advances in internet data and web technologies" Tailand 2021 [en línea] Disponible: https://link.springer.com/book/10.1007/978-3-030-70639-5

[26] E. Salustio S. "Advances in internet, data and web technologies", 2021 [en línea] Disponible: http://saludpublica.cucs.udg.mx/cursos/medicion_exposicion/Hern%C3%A1ndez-Sampieri%20et%20al,%20Metodolog%C3%ADa%20de%20la%20investigaci%C3%B3n,%202014,%20pp%20194-267.pdf

[27] M.I.Romero Castro, G.L. Figueroa Morán y otros "Introducción a la seguridad informática y el análisis de vulnerabilidades" 1ra. Edición, Alcoy (Alicante), 2018

ANEXOS

Anexo 1: Matriz de consistencia

"IMPLEMENTACION DE INFRAESTRUCTURA DE REDES PARA MEJORAR LA COMUNICACIÓN Y SEGURIDAD DE DATOS EN LA UGEL 312 HUANCA SANCOS – AYACUCHO 2022"

AUTOR: RONALD APAICO MENDOZA

PROBLEMA DE INVESTIGACIÓN	OBJETIVOS	MARCO TEORICO	HIPOTESIS	VARIABLE	METODOLOGIA
PROBLEMA GENERAL ¿Cómo la implementación de infraestructura de redes mejorará la comunicación y seguridad de datos en la UGEL Huanca Sancos? PROBLEMA ESPECIFICO - ¿En qué medida la implementación de infraestructura de redes influirá en el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos? - ¿En qué medida la implementación de infraestructura de redes influirá en la seguridad de la red en la UGEL Huanca Sancos? - ¿Cómo implementar la infraestructura de redes, para mejorar la comunicación y seguridad en la UGEL Huanca Sancos?	OBJETIVO GENERAL Determinar cómo la implementación de infraestructura de redes mejora la comunicación y seguridad de datos en la UGEL Huanca Sancos. OBJETIVO ESPECIFICO Determinar en qué medida la implementación de infraestructura de redes influirá en el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos Establecer como la implementación de infraestructura de redes influirá en la seguridad de la red en la UGEL Huanca Sancos. Implementar una infraestructura de redes que mejora la comunicación y seguridad de la red en la UGEL Huanca Sancos.	ANTECEDENTES J. Galdos Guizado y Y.I. Benites Sosa UNH Huancavelica (2018) "diseño simulación de la implementación de una red convergente para mejorar los servicios de comunicación de la municipalidad de Manta,2015" L.A. Guerra Menendez y otros UNJBG Tacna (2017) "mejorando el uso de internet en la escuela profesional de contabilidad de la UNH" V.C. Poma Torres y otros UPLA Huancayo (2017) "rediseño de redes mediante la metodología top down network design para mejora de la red de los equipos tic en la Diresa Junín" X.F. López Andrade. PUCE Ambato. Ecuador (2008) "Rediseño de la red con calidad de servicio para datos y tecnología de voz sobre ip en el ilustre municipio de Ambato"	HIPOTESIS GENERAL La implementación de infraestructura de redes permite mejorar la comunicación y seguridad de datos en la UGEL Huanca Sancos. HIPOTESIS ESPECIFICO La implementación de infraestructura de redes mejora el tráfico o desempeño de red en la comunicación de datos en la UGEL Huanca Sancos. La implementación de infraestructura de redes mejora la seguridad de la red en la UGEL Huanca Sancos. La implementación de infraestructura de redes, mejora la comunicación y seguridad de la red en la UGEL Huanca Sancos. Esto se realizó en base a los requerimientos de la institución en estudio.	VARIABLES INDEPENDIENTES IMPLEMENTACION DE INFRAESTRUCTURA DE REDES DIMENCIONES - Confiabilidad de redes. - Capacidad de red. INDICADORES - Frecuencia de fallas. - Capacidad de transmisión. VARIABLES DEPENDIENTES COMUNICACIÓN Y SEGURIDAD DE DATOS DIMENSIONES - Tráfico o desempeño de red. - Seguridad de la red. INDICADORES - Latencia. - Retraso de envió de paquetes. - Índice de detección de intrusiones.	**METODOLOGIA DE INVESTIGACION** Experimental **TIPO DE INVESTIGACION** Cuantitativo tecnológico. **NIVEL DE INVESTIGACION** Explicativo. **DISEÑO DE LA INVESTIGACIÓN** Diseños Experimentales **POBLACION DE INVESTIGACION** Todos los usuarios que laboran en los diferentes ambientes de la UGEL Huanca Sancos. **TECNICAS E INSTRUMENTOS DE RECOLECCION DE DATOS.** Observación. Encuesta. Entrevista. **TECNICA DE PROCESAMIENTOS Y ANALISIS DE DATOS:** Técnicas descriptivas, inferenciales y de caso.

Anexo 2 Matriz de Operacionalización de Variables

VARIABLES	DEFINICION	DIMENSIONES	INDICADORES	INSTRUMENTOS
VARIABLE INDEPENDIENTE **(Implementación de infraestructura de redes)**	Es el proceso que permite la descripción formal de los elementos de hardware y software de la red, incluyendo su arquitectura en modo de operación para la productividad de la UGEL Huanca Sancos.	Confiabilidad	Frecuencia de fallas	Ficha de recolección de datos
		Capacidad	Capacidad de transmisión	Ficha de recolección de datos
VARIABLE DEPENDIENTE **(Comunicación y seguridad de datos)**	Es el proceso que permite que se pueda compartir datos entre los usuarios autorizados conectados a la red garantizando la integridad e inviolabilidad de los mismos.	Trafico de la red	- Latencia - Retraso de envio de paquetes (jitter)	Ficha de recolección de datos
		Seguridad de la red	Detección de intrusiones	Ficha de recolección de datos

Anexo 3: Ficha de Evaluación por criterio expertos

UPLA
UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDACIÓN POR CRITERIO EXPERTO

1. DATOS DEL EXPERTO

Nombre y Apellidos:	EYNER ORLANDINI GUERRERO PINEDA
Grado Académico:	INGENIERO DE SISTEMAS E INFORMÁTICA
Lugar y Fecha:	CARAZ-HUAYLAS-ANCASH 15/02/2023

2. FICHA DE RECOLECCIÓN DE DATOS.

Recomendaciones: marque con una (x) la opción que mejor le parezca.

		Criterios	Deficiente	Aceptable	Bueno
N°	**Indicadores**	**Descripción de los indicadores**	**01**	**03**	**05**
01	Claridad	El instrumento está formulado con lenguaje apropiado, es decir libre de ambigüedades.		X	
02	Objetividad	El instrumento permitirá mostrar la variable de estudio en toda su dimensión e indicador en su aspecto conceptual y operacional.			X
03	Actualidad	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal inherente de atención al cliente.			X
04	Organización	El instrumento induce organicidad lógica en concordancia con la definición operacional y conceptual de las variables y sus dimensiones e indicadores de manera que permitieran hacer abstracciones e inferencias en función a las hipostasis, problemas y objetivos de la investigación.			X
05	Suficiencia	Los ítems del instrumento expresan suficiencia en cantidad y calidad en la redacción.			X
06	Pertinencia	El instrumento responde al momento oportuno o más adecuado.		X	
07	Consistencia	La información que se obtendrá mediante los instrumento, permitirá analizar, describir y explicar la realidad motivo de la investigación.			X
08	Coherencia	El instrumento expresa coherencia entre las variables, dimensiones e indicadores.			X
09	Metodología	Los procedimientos insertados en el instrumento responden al propósito de la investigación.			X
10	Aplicación	Los datos permiten un tratamiento estadístico pertinente.			X
		Conteo total de marcas:	**A**	**B**	**C**
			0	2	8

3. FORMULA:

Coeficiente de validez = $\frac{1xA + 3xB + 5xC}{50}$ $= \frac{46}{50} = 0.92$

3. OPINIÓN DE APLICABILIDAD:

Intervalo	Categoría	
[0.20 - 0.40]	No válido, reformular	○
<0.41 - 0.60]	No válido, modificar	○
<0.61 - 0.80]	Válido, mejorar	○
<0.81 - 1.00]	Válido, aplicar	⊗

COLEGIO DE INGENIEROS DEL PERU
CONSEJO DEPARTAMENTAL ANCASH - HUARAZ
EYNER ORLANDINI GUERRERO PINEDA
INGENIERO DE SISTEMAS E INFORMATICA
CIP. 267696

Firma del Experto
DNI: 70670575

5. RECOMENDACIONES:

Anexo 4: Ficha de Evaluación por criterio expertos

UPLA
UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDACIÓN POR CRITERIO EXPERTO

1. DATOS DEL EXPERTO

Nombre y Apellidos:	LOURDES ROSMERY FIGUEROA MIRANDA
Grado Académico:	INGENIERO EN INFORMATICA Y DE SISTEMAS
Lugar y Fecha:	09 DE FEBRERO 2023

2. FICHA DE RECOLECCIÓN DE DATOS.

Recomendaciones: marque con una (x) la opción que mejor le parezca.

		Criterios	Deficiente	Aceptable	Bueno
Nº	**Indicadores**	**Descripción de los indicadores**	**01**	**03**	**05**
01	Claridad	El instrumento está formulado con lenguaje apropiado, es decir libre de ambigüedades.		X	
02	Objetividad	El instrumento permitirá mostrar la variable de estudio en toda su dimensión e indicador en su aspecto conceptual y operacional.			X
03	Actualidad	El instrumento evidencia vigencia acorde con el conocimiento científico, tecnológico y legal inherente de atención al cliente.		X	
04	Organización	El instrumento induce organicidad lógica en concordancia con la definición operacional y conceptual de las variables y sus dimensiones e indicadores de manera que permitieran hacer abstracciones e inferencias en función a las hipostasis, problemas y objetivos de la investigación.			X
05	Suficiencia	Los ítems del instrumento expresan suficiencia en cantidad y calidad en la redacción.			X
06	Pertinencia	El instrumento responde al momento oportuno o más adecuado.			X
07	Consistencia	La información que se obtendrá mediante los instrumento, permitirá analizar, describir y explicar la realidad motivo de la investigación.			X
08	Coherencia	El instrumento expresa coherencia entre las variables, dimensiones e indicadores.		X	
09	Metodología	Los procedimientos insertados en el instrumento responden al propósito de la investigación.			X
10	Aplicación	Los datos permiten un tratamiento estadístico pertinente.			X
			A	**B**	**C**
		Conteo total de marcas:	0	3	7

3. FORMULA:

Coeficiente de validez = $\frac{1xA + 3xB + 5xC}{50}$ $= \frac{44}{50} = 0.88$

3. OPINIÓN DE APLICABILIDAD:

Intervalo	Categoría	
[0.20 - 0.40]	No válido, reformular	○
<0.41 - 0.60]	No válido, modificar	○
<0.61 - 0.80]	Válido, mejorar	○
<0.81 - 1.00]	Válido, aplicar	⊗

Ing. Lourdes R. Figueroa Miranda
CIP N° 191438
DNI: 42104433

Firma del Experto
DNI : 42104433

5. RECOMENDACIONES:

Anexo 5: Ficha de recolección de datos Nivel de latencia Test retest

Ficha de Registro				
Investigadores	Roland apaico Mendoza	**Tipo de Prueba**		TEST
Empresa investigada	UGEL 312 Huanca Sancos - Ayacucho			
Fecha Inicio	**01 Agosto**	**Fecha fin**	**30 Agosto**	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de latencia**	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio del nivel de latencia (Ms)**
1	1-Ago	7280	92	79.13
2	1-Ago	7400	92	80.43
3	1-Ago	6800	92	73.91
4	1-Ago	8900	92	96.74
5	1-Ago	6700	92	72.83
6	4-Ago	9400	92	102.17
7	4-Ago	5400	92	58.70
8	4-Ago	6544	92	71.13
9	4-Ago	7400	92	80.43
10	4-Ago	6300	92	68.48
11	5-Ago	5600	92	60.87
12	5-Ago	7345	92	79.84
13	5-Ago	5300	92	57.61
14	5-Ago	8400	92	91.30
15	5-Ago	7220	92	78.48
16	6-Ago	6540	92	71.09
17	6-Ago	6780	92	73.70
18	6-Ago	8432	92	91.65
19	6-Ago	6780	92	73.70
20	6-Ago	6540	92	71.09
21	7-Ago	5200	92	56.52
22	7-Ago	6100	92	66.30
23	7-Ago	7200	92	78.26
24	7-Ago	8100	92	88.04
25	7-Ago	6100	92	66.30
26	8-Ago	5300	92	57.61
27	8-Ago	6100	92	66.30
28	8-Ago	8100	92	88.04
29	8-Ago	6200	92	67.39
73	21-Ago	7920	92	86.09
74	21-Ago	5820	92	63.26
75	21-Ago	4560	92	49.57
76	22-Ago	8130	92	88.37
77	22-Ago	5560	92	60.43
78	22-Ago	6910	92	75.11
79	22-Ago	5490	92	59.67
80	25-Ago	8460	92	91.96
81	25-Ago	5600	92	60.87
82	25-Ago	7510	92	81.63
83	25-Ago	5510	92	59.89
84	26-Ago	7530	92	81.85
85	26-Ago	8450	92	91.85
86	26-Ago	7300	92	79.35
87	27-Ago	6050	92	65.76
88	27-Ago	5420	92	58.91
89	27-Ago	5860	92	63.70
90	27-Ago	6810	92	74.02
91	28-Ago	7830	92	85.11
92	28-Ago	8190	92	89.02

Anexo 6: Ficha de recolección de datos Nivel de Jitter Test Retest

Ficha de Registro 03				
Investigadore	Roland apaico Mendoza	**Tipo de Prueba**		TEST
Empresa investigada	UGEL 312 Huanca Sancos - Ayacucho			
Fecha Inicio	**01 Agosto**	**Fecha**	**30 Agosto**	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de Jitter**	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio de nivel de jitter**
1	1-Ago	3450	92	37.50
2	1-Ago	3800	92	41.30
3	1-Ago	4120	92	44.78
4	1-Ago	4200	92	45.65
5	1-Ago	4134	92	44.93
6	4-Ago	4323	92	46.99
7	4-Ago	3989	92	43.36
8	4-Ago	3678	92	39.98
9	4-Ago	3545	92	38.53
10	4-Ago	4213	92	45.79
11	5-Ago	3908	92	42.48
12	5-Ago	3897	92	42.36
13	5-Ago	4212	92	45.78
14	5-Ago	3556	92	38.65
15	5-Ago	3212	92	34.91
16	6-Ago	3456	92	37.57
17	6-Ago	4908	92	53.35
18	6-Ago	4569	92	49.66
19	6-Ago	3456	92	37.57
20	6-Ago	3455	92	37.55
21	7-Ago	2340	92	25.43
22	7-Ago	1783	92	19.38
23	7-Ago	2890	92	31.41
24	7-Ago	1820	92	19.78
25	7-Ago	2520	92	27.39
26	8-Ago	1520	92	16.52
27	8-Ago	3510	92	38.15
28	8-Ago	1620	92	17.61
29	8-Ago	1230	92	13.37
30	8-Jul	2610	92	28.37
31	11-Ago	3530	92	38.37
32	11-Ago	1530	92	16.63
33	11-Ago	2450	92	26.63
34	11-Ago	1850	92	20.11
35	11-Ago	2760	92	30.00
36	12-Ago	3941	92	42.84
37	12-Ago	2613	92	28.40
38	12-Ago	1400	92	15.22
39	12-Ago	3845	92	41.79
40	12-Ago	3210	92	34.89
41	13-Ago	2510	92	27.28
42	13-Ago	3601	92	39.14
43	13-Ago	3950	92	42.93
44	13-Ago	2840	92	30.87
45	13-Ago	3761	92	40.88
46	14-Ago	1843	92	20.03
47	14-Ago	3460	92	37.61
48	14-Ago	2640	92	28.70
49	14-Ago	1760	92	19.13
50	14-Ago	2850	92	30.98
51	15-Ago	1630	92	17.72
52	15-Ago	2480	92	26.96
53	15-Ago	3915	92	42.55
54	15-Ago	2913	92	31.66
55	15-Ago	3200	92	34.78

Anexo 7: Ficha de recolección de datos índice de intrusiones Test Retest

Ficha de Registro 03				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**TEST**
Institución investigada	**UGEL 312 Huanca Sancos – Ayacucho**			
Fecha Inicio	01 Agosto	**Fecha fin**	30 Agosto	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	Índice de detección de intrusiones	**MS**	IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)	
Item	**Area**	**Intrusiones detectadas**	**Intrusiones totales**	**IDI**
1	1-Ago	5	10	50.00
2	1-Ago	4	12	33.33
3	1-Ago	4	11	36.36
4	1-Ago	4	12	33.33
5	1-Ago	3	12	25.00
6	4-Ago	4	10	40.00
7	4-Ago	5	11	45.45
8	4-Ago	4	10	40.00
9	4-Ago	3	11	27.27
10	4-Ago	4	12	33.33
11	5-Ago	3	9	33.33
12	5-Ago	4	9	44.44
13	5-Ago	6	10	60.00
14	5-Ago	4	11	36.36
15	5-Ago	5	12	41.67
16	6-Ago	4	10	40.00
17	6-Ago	4	9	44.44
18	6-Ago	4	8	50.00
19	6-Ago	4	10	40.00
20	6-Ago	4	10	40.00
21	7-Ago	5	10	50.00
22	7-Ago	6	12	50.00
23	7-Ago	4	11	36.36
24	7-Ago	4	12	33.33
25	7-Ago	7	12	58.33
26	8-Ago	4	10	40.00
27	8-Ago	5	11	45.45
28	8-Ago	4	10	40.00
29	8-Ago	3	11	27.27
30	8-Jul	4	12	33.33
31	11-Ago	3	9	33.33
32	11-Ago	4	9	44.44
33	11-Ago	6	10	60.00
34	11-Ago	4	11	36.36
35	11-Ago	6	12	50.00
36	12-Ago	4	10	40.00
37	12-Ago	4	9	44.44
38	12-Ago	4	8	50.00
39	12-Ago	4	10	40.00
40	12-Ago	4	10	40.00
41	13-Ago	5	10	50.00
42	13-Ago	4	12	33.33
43	13-Ago	4	11	36.36
44	13-Ago	4	12	33.33
45	13-Ago	5	12	41.67
46	14-Ago	4	10	40.00
47	14-Ago	5	11	45.45
48	14-Ago	4	10	40.00
49	14-Ago	3	11	27.27

Anexo 8: Ficha de recolección de datos 01 Nivel latencia Pre-test

Ficha de Registro				
Investigadores	Roland apaico Mendoza	**Tipo de Prueba**		Pre test
Empresa investigada	UGEL 312 Huanca Sancos - Ayacucho			
Fecha Inicio	01 Julio	**Fecha**		30 Julio
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	Nivel de latencia	MS	Sumatoria de ms / Número de equipos evaluados	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio del nivel de latencia (Ms)**
1	1-Jul	7280	92	79.13
2	1-Jul	7400	92	80.43
3	1-Jul	6800	92	73.91
4	1-Jul	8900	92	96.74
5	1-Jul	6700	92	72.83
6	4-Jul	9400	92	102.17
7	4-Jul	5400	92	58.70
8	4-Jul	6544	92	71.13
9	4-Jul	7400	92	80.43
10	4-Jul	6300	92	68.48
11	5-Jul	5600	92	60.87
12	5-Jul	7345	92	79.84
13	5-Jul	5300	92	57.61
14	5-Jul	8400	92	91.30
15	5-Jul	7220	92	78.48
16	6-Jul	6540	92	71.09
17	6-Jul	6780	92	73.70
18	6-Jul	8432	92	91.65
19	6-Jul	6780	92	73.70
20	6-Jul	6540	92	71.09
21	7-Jul	5200	92	56.52
22	7-Jul	6100	92	66.30
23	7-Jul	7200	92	78.26
24	7-Jul	8100	92	88.04
25	7-Jul	6100	92	66.30
26	8-Jul	5300	92	57.61
27	8-Jul	6100	92	66.30
28	8-Jul	8100	92	88.04
29	8-Jul	6200	92	67.39
88	27-Jul	5420	92	58.91
89	27-Jul	5860	92	63.70
90	28-Jul	6810	92	74.02
91	28-Jul	7830	92	85.11
92	28-Jul	8190	92	89.02

Anexo 9: Ficha de recolección de datos 01 Nivel latencia PostTest

Ficha de Registro 01				
es	Roland apaico Mendoza	Tipo de Prueba		Post test
Empresa investigada	UGEL 312 Huanca Sancos - Ayacucho			
Fecha Inicio	01 Diciembre	fin		30 Diciembre
Variable	Indicador	Medida	Fórmula	
Comunicación y Seguridad	Nivel de latencia	MS	Sumatoria de ms / Número de equipos evaluados	
Item	Area	Sumatoria de ms	Número de equipos	Promedio del nivel de latencia (Ms)
1	1-Dic	2500	92	27.17
2	1-Dic	2200	92	23.91
3	1-Dic	2100	92	22.83
4	1-Dic	2450	92	26.63
5	1-Dic	1340	92	14.57
6	4-Dic	2500	92	27.17
7	4-Dic	3200	92	34.78
8	4-Dic	2870	92	31.20
9	4-Dic	3120	92	33.91
10	4-Dic	2130	92	23.15
11	5-Dic	1450	92	15.76
12	5-Dic	3240	92	35.22
13	5-Dic	3120	92	33.91
14	5-Dic	2670	92	29.02
15	5-Dic	3245	92	35.27
16	6-Dic	2890	92	31.41
17	6-Dic	3130	92	34.02
18	6-Dic	2340	92	25.43
19	6-Dic	1783	92	19.38
20	6-Dic	2890	92	31.41
21	7-Dic	1820	92	19.78
22	7-Dic	2520	92	27.39
23	7-Dic	1520	92	16.52
24	7-Dic	3510	92	38.15
25	7-Dic	1620	92	17.61
26	8-Dic	1230	92	13.37
27	8-Dic	2610	92	28.37
28	8-Dic	3530	92	38.37
29	8-Dic	1530	92	16.63
30	8-Dic	2450	92	26.63
31	11-Dic	1850	92	20.11
32	11-Dic	2760	92	30.00
33	11-Dic	3941	92	42.84
84	26-Dic	1873	92	20.36
85	26-Dic	1740	92	18.91
86	26-Dic	1460	92	15.87
87	27-Dic	2540	92	27.61
88	27-Dic	3891	92	42.29
89	27-Dic	1786	92	19.41
90	28-Dic	2841	92	30.88
91	28-Dic	3401	92	36.97
92	28-Dic	1254	92	13.63

Anexo 10: Ficha de recolección de datos 02 Nivel de Jitter Pre test

Ficha de Registro 02				
Investigadores	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Empresa investigada	UGEL 312 Huanca Sancos - Ayacucho			
Fecha Inicio	01 Julio	**fin**		30 Julio
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de Jitter**	**MS**	**Sumatoria de ms / Número de equipos evaluados**	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio de nivel de jitter**
1	1-Jul	3450	92	37.50
2	1-Jul	3800	92	41.30
3	1-Jul	4120	92	44.78
4	1-Jul	4200	92	45.65
5	1-Jul	4134	92	44.93
6	4-Jul	4323	92	46.99
7	4-Jul	3989	92	43.36
8	4-Jul	3678	92	39.98
9	4-Jul	3545	92	38.53
10	4-Jul	4213	92	45.79
11	5-Jul	3908	92	42.48
12	5-Jul	3897	92	42.36
13	5-Jul	4212	92	45.78
14	5-Jul	3556	92	38.65
15	5-Jul	3212	92	34.91
16	6-Jul	3456	92	37.57
17	6-Jul	4908	92	53.35
18	6-Jul	4569	92	49.66
19	6-Jul	3456	92	37.57
20	6-Jul	3455	92	37.55
21	7-Jul	2340	92	25.43
22	7-Jul	1783	92	19.38
23	7-Jul	2890	92	31.41
24	7-Jul	1820	92	19.78
25	7-Jul	2520	92	27.39
26	8-Jul	1520	92	16.52
27	8-Jul	3510	92	38.15
28	8-Jul	1620	92	17.61
29	8-Jul	1230	92	13.37
30	8-Jul	2610	92	28.37
31	11-Jul	3530	92	38.37
32	11-Jul	1530	92	16.63
33	11-Jul	2450	92	26.63
34	11-Jul	1850	92	20.11
35	11-Jul	2760	92	30.00
36	12-Jul	3941	92	42.84
37	12-Jul	2613	92	28.40
38	12-Jul	1400	92	15.22
39	12-Jul	3845	92	41.79
40	12-Jul	3210	92	34.89
41	13-Jul	2510	92	27.28
42	13-Jul	3601	92	39.14
43	13-Jul	3950	92	42.93
44	13-Jul	2840	92	30.87
45	13-Jul	3761	92	40.88
46	14-Jul	1843	92	20.03

Anexo 11: Ficha de recolección de datos 02 Nivel de Jitter PostTest

Ficha de Registro				
Investigadores	**Roland apaico Mendoza**	**Tipo de Prueba**		**Post test**
Empresa investigada	UGEL 312 Huanca Sancos - Ayacucho			
Fecha Inicio	01 Diciembre	**Fecha fin**		30 Diciembre
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Nivel de Jitter**	MS	Sumatoria de ms / Número de equipos evaluados	
Item	**Area**	**Sumatoria de ms**	**Número de equipos**	**Promedio de nivel de jitter**
1	1-Dic	1749	92	19.01
2	1-Dic	1821	92	19.79
3	1-Dic	1540	92	16.74
4	1-Dic	1659	92	18.03
5	1-Dic	1430	92	15.54
6	4-Dic	1340	92	14.57
7	4-Dic	1234	92	13.41
8	4-Dic	1434	92	15.59
9	4-Dic	1533	92	16.66
10	4-Dic	1367	92	14.86
11	5-Dic	1558	92	16.93
12	5-Dic	1789	92	19.45
13	5-Dic	1120	92	12.17
14	5-Dic	1230	92	13.37
15	5-Dic	1123	92	12.21
16	6-Dic	1300	92	14.13
17	6-Dic	1324	92	14.39
18	6-Dic	1432	92	15.57
19	6-Dic	1593	92	17.32
20	6-Dic	1890	92	20.54
21	7-Dic	1640	92	17.83
22	7-Dic	1840	92	20.00
23	7-Dic	1945	92	21.14
24	7-Dic	1640	92	17.83
25	7-Dic	1750	92	19.02
26	8-Dic	1460	92	15.87
27	8-Dic	1940	92	21.09
28	8-Dic	1620	92	17.61
29	8-Dic	1450	92	15.76
30	8-Dic	1350	92	14.67
31	11-Dic	1460	92	15.87
32	11-Dic	1480	92	16.09
33	11-Dic	1945	92	21.14
34	11-Dic	1750	92	19.02
35	11-Dic	1451	92	15.77
36	12-Dic	1231	92	13.38
37	12-Dic	1642	92	17.85
38	12-Dic	1513	92	16.45
39	12-Dic	1346	92	14.63
40	12-Dic	1513	92	16.45
41	13-Dic	1240	92	13.48
42	13-Dic	1346	92	14.63
43	13-Dic	1621	92	17.62
44	13-Dic	1031	92	11.21
45	13-Dic	1842	92	20.02
46	14-Dic	1945	92	21.14
47	14-Dic	1430	92	15.54
48	14-Dic	1752	92	19.04

Anexo 12: Ficha de recolección de datos 03 Índice de intrusiones Pretest

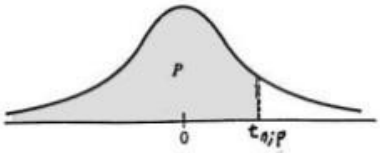
Ficha de Registro 03				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Pre test**
Institución investigada	**UGEL 312 Huanca Sancos – Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	Índice de detección de intrusiones	**MS**	IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)	
Item	**Area**	**Intrusiones detectadas**	**Intrusiones totales**	**IDI**
1		5	10	50.00
2		4	12	33.33
3		4	11	36.36
4		4	12	33.33
5		3	12	25.00
6		4	10	40.00
7		5	11	45.45
8		4	10	40.00
9		3	11	27.27
10		4	12	33.33
11		3	9	33.33
12		4	9	44.44
13		6	10	60.00
14		4	11	36.36
15		5	12	41.67
16		4	10	40.00
17		4	9	44.44
18		4	8	50.00
19		4	10	40.00
20		4	10	40.00
21		5	10	50.00
22		6	12	50.00
23		4	11	36.36
24		4	12	33.33
25		7	12	58.33
26		4	10	40.00
27		5	11	45.45
28		4	10	40.00
29		3	11	27.27
30		4	12	33.33
31		3	9	33.33
32		4	9	44.44
33		6	10	60.00
34		4	11	36.36
35		6	12	50.00
36		4	10	40.00
37		4	9	44.44
38		4	8	50.00
39		4	10	40.00
40		4	10	40.00
41		5	10	50.00
42		4	12	33.33
43		4	11	36.36
44		4	12	33.33
45		5	12	41.67
46		4	10	40.00

Anexo 13: Ficha de recolección de datos 03 Índice de intrusiones PostTest

Ficha de Registro				
Investigador	Roland apaico Mendoza	**Tipo de Prueba**		**Post Test**
Institución investigada	**UGEL 312 Huanca Sancos – Ayacucho**			
Fecha Inicio	01 Julio	**Fecha fin**	30 Julio	
Variable	Indicador	**Medida**	**Fórmula**	
Comunicación y Seguridad	**Índice de detección de intrusiones**	**MS**	**IDI = (Intrusiones detectadas y respondidas) / (Intrusiones totales)**	
Item	**Area**	**Intrusiones detectadas**	**Intrusiones totales**	**IDI**
1		6	7	85.71
2		5	8	62.50
3		7	7	100.00
4		6	6	100.00
5		5	7	71.43
6		6	8	75.00
7		6	7	85.71
8		6	6	100.00
9		5	6	83.33
10		6	7	85.71
11		6	6	100.00
12		5	7	71.43
13		5	6	83.33
14		5	7	71.43
15		4	5	80.00
16		5	6	83.33
17		5	5	100.00
18		4	5	80.00
19		4	6	66.67
20		4	6	66.67
21		6	7	85.71
22		5	8	62.50
23		7	7	100.00
24		6	6	100.00
25		5	7	71.43
26		6	8	75.00
27		6	7	85.71
28		6	6	100.00
29		5	6	83.33
30		6	7	85.71
31		6	6	100.00
32		5	7	71.43
33		5	6	83.33
34		5	7	71.43
35		4	5	80.00
36		5	6	83.33
37		5	5	100.00
38		4	5	80.00
39		4	6	66.67
40		4	6	66.67
41		6	7	85.71
42		5	8	62.50
43		7	7	100.00
44		6	6	100.00
45		5	7	71.43
46		6	8	75.00
47		6	7	85.71
48		6	6	100.00
49		5	6	83.33

Anexo 14: Tabla de la distribución T de student.

Distribución t de Student

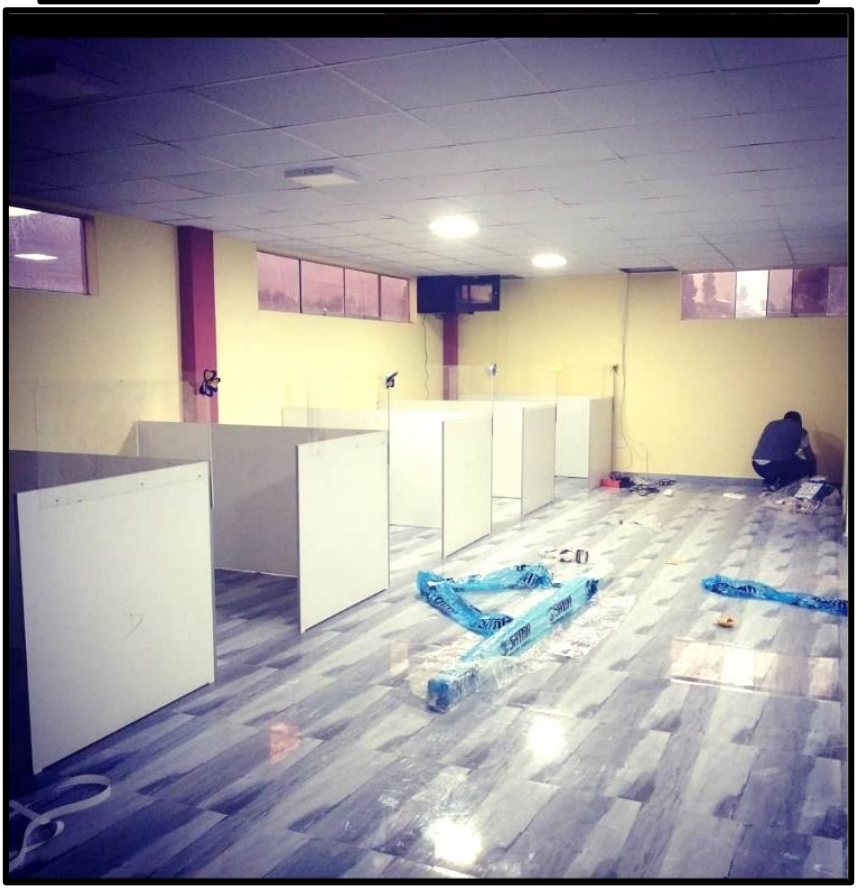


La tabla A.4 da distintos valores de la función de distribución en relación con el número de grados de libertad; concretamente, relaciona los valores p y $t_{n;p}$ que satisfacen

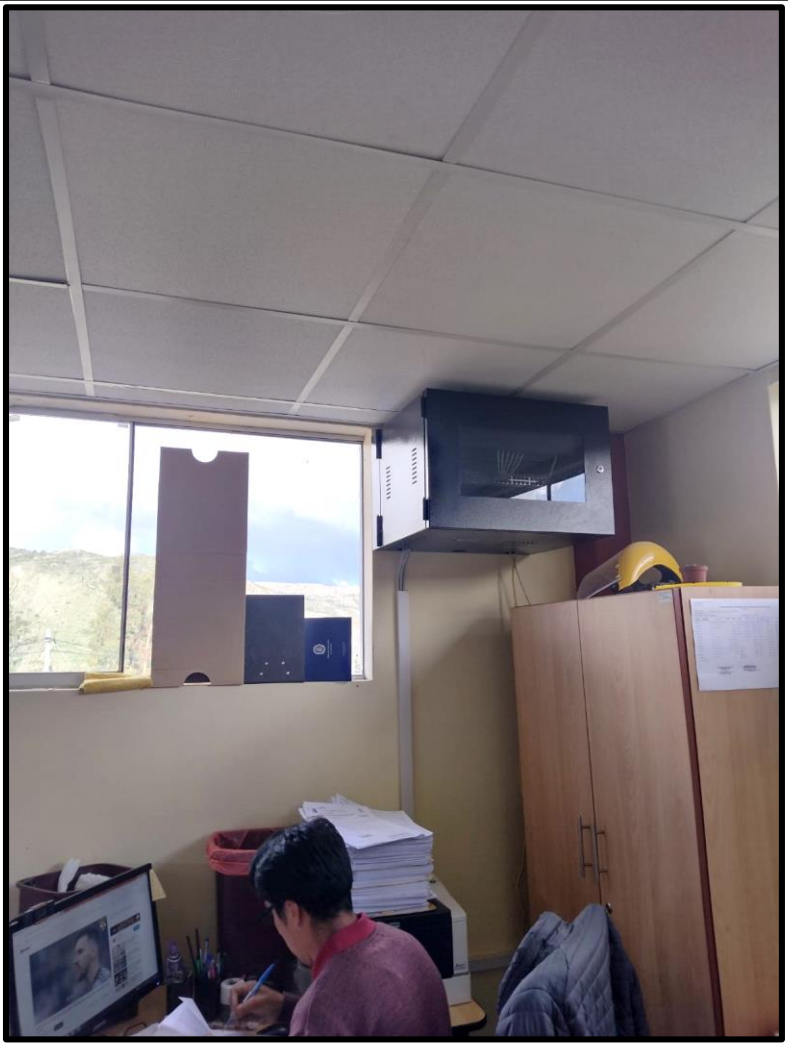
$$P(t_n \leq t_{n;p}) = p.$$

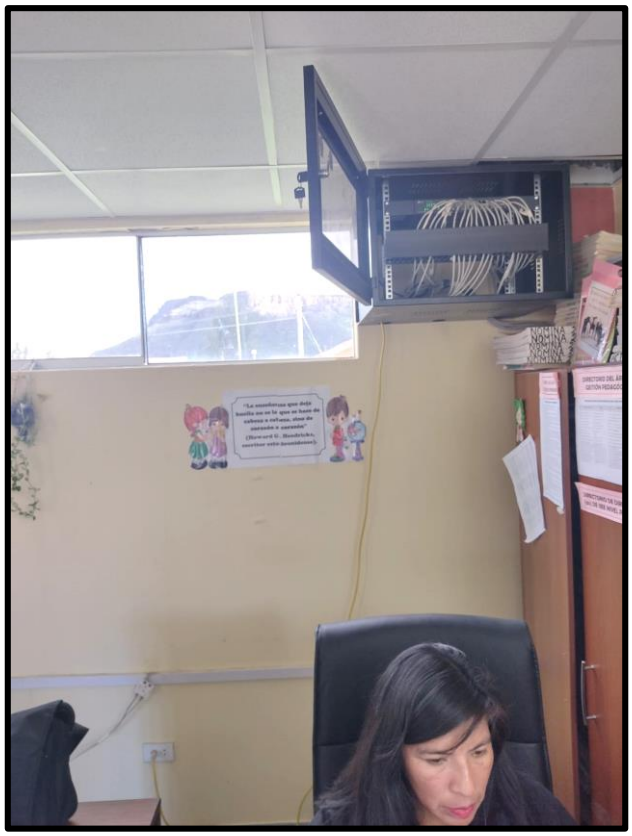
n	$t_{0,55}$	$t_{0,60}$	$t_{0,70}$	$t_{0,80}$	$t_{0,90}$	$t_{0,95}$	$t_{0,975}$	$t_{0,99}$	$t_{0,995}$
1	0,1584	0,3249	0,7265	1,3764	3,0777	6,3138	12,7062	31,8205	63,6567
2	0,1421	0,2887	0,6172	1,0607	1,8856	2,9200	4,3027	6,9646	9,9248
3	0,1366	0,2767	0,5844	0,9785	1,6377	2,3534	3,1824	4,5407	5,8409
4	0,1338	0,2707	0,5686	0,9410	1,5332	2,1318	2,7764	3,7469	4,6041
5	0,1322	0,2672	0,5594	0,9195	1,4759	2,0150	2,5706	3,3649	4,0321
6	0,1311	0,2648	0,5534	0,9057	1,4398	1,9432	2,4469	3,1427	3,7074
7	0,1303	0,2632	0,5491	0,8960	1,4149	1,8946	2,3646	2,9980	3,4995
8	0,1297	0,2619	0,5459	0,8889	1,3968	1,8595	2,3060	2,8965	3,3554
9	0,1293	0,2610	0,5435	0,8834	1,3830	1,8331	2,2622	2,8214	3,2498
10	0,1289	0,2602	0,5415	0,8791	1,3722	1,8125	2,2281	2,7638	3,1693
11	0,1286	0,2596	0,5399	0,8755	1,3634	1,7959	2,2010	2,7181	3,1058
12	0,1283	0,2590	0,5386	0,8726	1,3562	1,7823	2,1788	2,6810	3,0545
13	0,1281	0,2586	0,5375	0,8702	1,3502	1,7709	2,1604	2,6503	3,0123
14	0,1280	0,2582	0,5366	0,8681	1,3450	1,7613	2,1448	2,6245	2,9768
15	0,1278	0,2579	0,5357	0,8662	1,3406	1,7531	2,1314	2,6025	2,9467
16	0,1277	0,2576	0,5350	0,8647	1,3368	1,7459	2,1199	2,5835	2,9208
17	0,1276	0,2573	0,5344	0,8633	1,3334	1,7396	2,1098	2,5669	2,8982
18	0,1274	0,2571	0,5338	0,8620	1,3304	1,7341	2,1009	2,5524	2,8784
19	0,1274	0,2569	0,5333	0,8610	1,3277	1,7291	2,0930	2,5395	2,8609
20	0,1273	0,2567	0,5329	0,8600	1,3253	1,7247	2,0860	2,5280	2,8453
21	0,1272	0,2566	0,5325	0,8591	1,3232	1,7207	2,0796	2,5176	2,8314
22	0,1271	0,2564	0,5321	0,8583	1,3212	1,7171	2,0739	2,5083	2,8188
23	0,1271	0,2563	0,5317	0,8575	1,3195	1,7139	2,0687	2,4999	2,8073
24	0,1270	0,2562	0,5314	0,8569	1,3178	1,7109	2,0639	2,4922	2,7969
25	0,1269	0,2561	0,5312	0,8562	1,3163	1,7081	2,0595	2,4851	2,7874
26	0,1269	0,2560	0,5309	0,8557	1,3150	1,7056	2,0555	2,4786	2,7787
27	0,1268	0,2559	0,5306	0,8551	1,3137	1,7033	2,0518	2,4727	2,7707
28	0,1268	0,2558	0,5304	0,8546	1,3125	1,7011	2,0484	2,4671	2,7633
29	0,1268	0,2557	0,5302	0,8542	1,3114	1,6991	2,0452	2,4620	2,7564
30	0,1267	0,2556	0,5300	0,8538	1,3104	1,6973	2,0423	2,4573	2,7500
40	0,1265	0,2550	0,5286	0,8507	1,3031	1,6839	2,0211	2,4233	2,7045
50	0,1263	0,2547	0,5278	0,8489	1,2987	1,6759	2,0086	2,4033	2,6778
60	0,1262	0,2545	0,5272	0,8477	1,2958	1,6706	2,0003	2,3901	2,6603
80	0,1261	0,2542	0,5265	0,8461	1,2922	1,6641	1,9901	2,3739	2,6387
100	0,1260	0,2540	0,5261	0,8452	1,2901	1,6602	1,9840	2,3642	2,6259
120	0,1259	0,2539	0,5258	0,8446	1,2886	1,6577	1,9799	2,3578	2,6174
∞	0,126	0,253	0,524	0,842	1,282	1,645	1,960	2,327	2,576

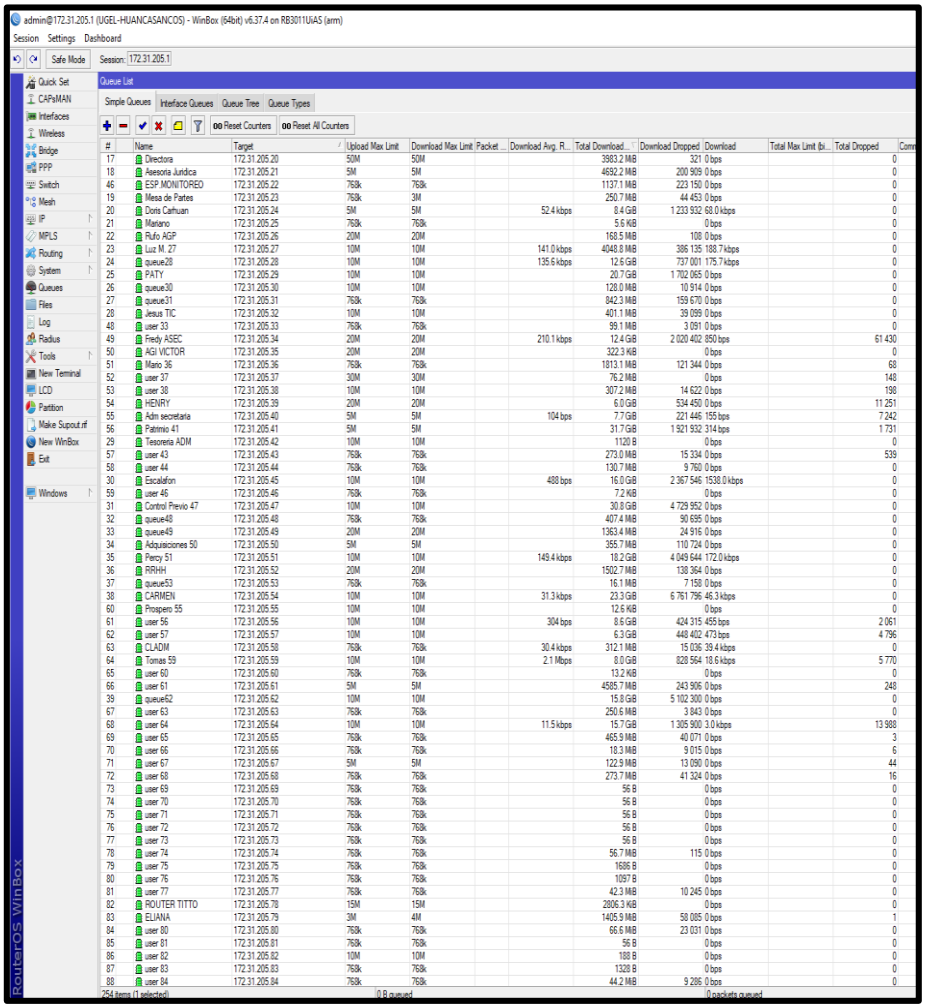
Anexo 15: Evidencias de la implementación de redes en la UGEL Huanca Sancos.



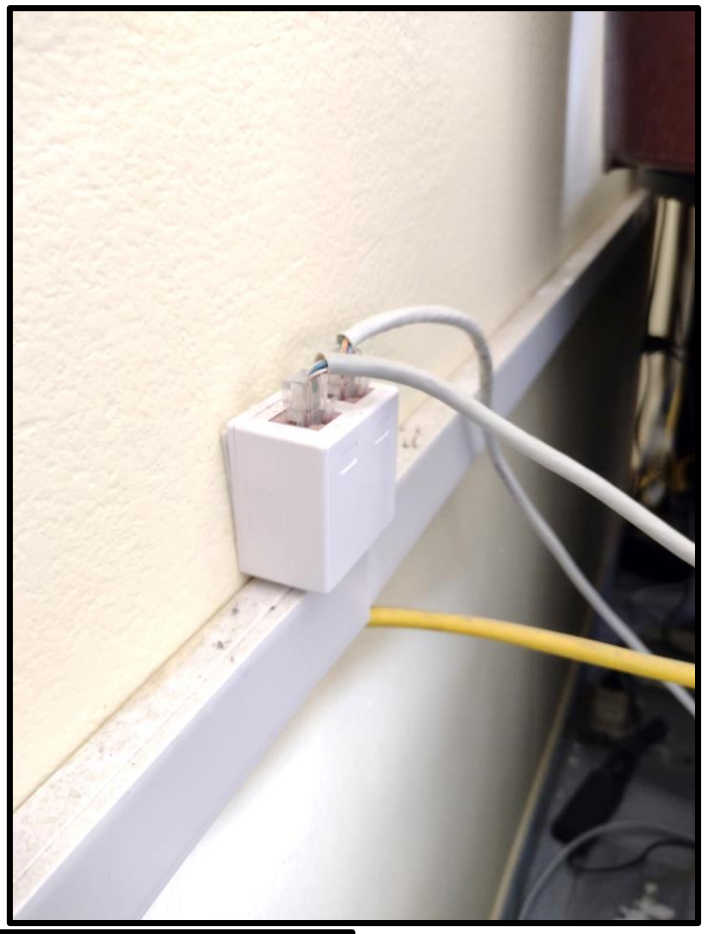

WALON

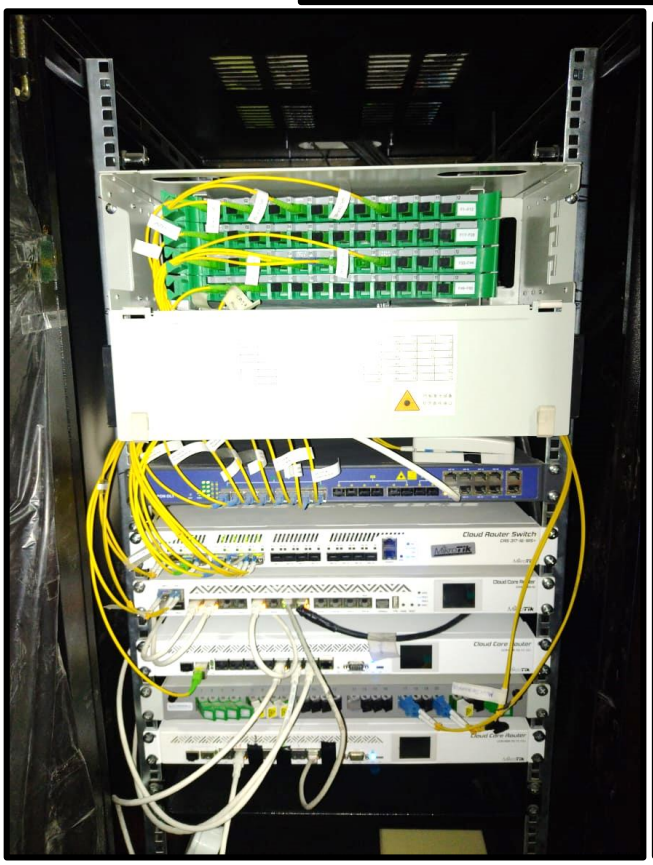





admin@172.31.205.1 (UGEL-HUANCASANCOS) - WinBox (64bit) v6.37.4 on RB3011UiAS (arm)
Session Settings Dashboard
Safe Mode
Session: 172.31.205.1
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
00 Reset Counters
00 Reset All Counters
RouterOS WinBox


NOMINA
NOMINA
NOMINA
NOMINA
NOMINA




Cloud Router Switch