UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creada por Ley N° 25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA - SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"DISEÑO DE INFRAESTRUCTURA DE RED DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UN GOBIERNO LOCAL, 2021"

LÍNEA DE INVESTIGACIÓN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTADO POR:

Bach. ESCOBAR LANDEO, Rubén

Bach. VILCA RAMOS, Ivan

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

HUANCAVELICA, PERÚ

2022

UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creada por Ley N ° 25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA - SISTEMA

ACTA DE SUSTENTACIÓN DE TESIS

Mediante el aplicativo Google Meet: meet.google.com/ran-tsdw-xmu; (PE) +51 1 6449188 PIN: 710 834 463 4552#, habilitado por Secretaría Docente de la Facultad de Ingeniería Electrónica - Sistemas, en mérito a la **Resolución de Consejo de Facultad N° 0169-2022-FIES-UNH,** de fecha 28 de junio del 2022**,** a los 13 días del mes de julio del año 2022, a horas 12:00 m., se reunieron; el Jurado Calificador, conformado de la siguiente manera:

1.	**PRESIDENTE**	:	Dr. Luis Enrique PACHECO MOSCOSO
	ORCID	:	*https://orcid.org/0000-0002-7818-1724*
	DNI N°	:	20103301
2.	**SECRETARIO**	:	Dr. Freddy Toribio HUAYTA MEZA
	ORCID	:	*https://orcid.org/0000-0001-9606-6343*
	DNI N°	:	20024900
3.	**VOCAL**	:	Dr. John Fredy ROJAS BUJAICO
	ORCID	:	*https://orcid.org/0000-0001-6614-9615*
	DNI N°	:	10730857
4.	**ASESOR**	:	Dr. John Fredy ROJAS BUJAICO
	ORCID	:	*https://orcid.org/0000-0001-6614-9615*
	DNI N°	:	10730857

Designados con Resolución de Consejo de Facultad N° 058-2022-FIES-UNH de fecha 30 de marzo de 2022 del proyecto de investigación, Titulado:

"DISEÑO DE INFRAESTRUCTURA DE RED DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UN GOBIERNO LOCAL, 2021"

Cuyo autor es el (los) graduado (s): Bachilleres:
Rubén ESCOBAR LANDEO con DNI N°: 71909501
Ivan VILCA RAMOS con DNI N°: 71929216,

A fin de proceder con la evaluación y calificación de la sustentación del proyecto de investigación **POR PRIMERA VEZ**, antes citado.

Se dio inicio a la sustentación del proyecto de investigación en mención, a horas 12 con 05 minutos, concluyendo a horas 12 con 30 minutos.

Finalizado la sustentación; se invitó al público presente y al sustentante abandonar la sala de actos; y, luego de una amplia deliberación y calificación por parte del jurado, se llegó al siguiente resultado:

APROBADO POR: UNANIMIDAD

Dr. Luis Enrique PACHECO MOSCOSO
Presidente

Dr. Freddy Toribio HUAYTA MEZA
Secretario

Dr. John Fredy ROJAS BUJAICO
Vocal

TÍTULO

"DISEÑO DE INFRAESTRUCTURA DE RED DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UN GOBIERNO LOCAL, 2021"

AUTORES

BACH. ESCOBAR LANDEO RUBEN

BACH. VILCA RAMOS IVAN

ASESOR

DR. ROJAS BUJAICO JOHN FREDY

https://orcid.org/0000-0001-6614-9615

DNI Nº: 10730857

AGRADECIMIENTO

A Dios, por ser nuestra guía y brindarnos la dicha de la salud y bienestar físico y espiritual.

A nuestros familiares, padres y hermanos quienes son la fuente de inspiración y superación, por su apoyo incondicional durante nuestra formación profesionales.

A la Escuela Profesional de Ingeniería de Sistemas, durante nuestros estudios realizados obtuvimos los conocimientos y habilidades necesarias de los diferentes docentes de la especialidad, lo cual nos facilita enormemente en nuestro desempeño laboral en los diferentes campos de trabajo.

De igual manera, queremos agradecer a nuestro asesor al Dr. John Rojas Bujaico, quien con sus conocimientos nos guió a través de cada una de las etapas de este proyecto de tesis para alcanzar los resultados que buscamos.

Los autores

TABLA DE CONTENIDO

TABLA DE CONTENIDOS DE TABLAS

TABLA DE CONTENIDOS DE FIGURAS

RESUMEN

La presente investigación titulada: “DISEÑO DE INFRAESTRUCTURA DE RED DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UN GOBIERNO LOCAL, 2021” Su surgimiento se debe a la importancia de la información en la actualidad, es el recurso más importante en la organización, y toma en cuenta las diversas vulnerabilidades que existen debido a los avances en tecnología y comunicaciones.

El problema de la investigación: ¿De qué manera el diseño de infraestructura de red de datos mejora la seguridad de la información en el Gobierno Local de Paucará?, que actualmente se cuenta con una infraestructura de red de datos que no cumple con las funciones para el que fue implementado.

La investigación tiene como objetivo diseñar una infraestructura de red de datos que integre la actual infraestructura de red de voz completamente independiente y la infraestructura de red de datos para proporcionar una mejor transmisión de datos y mejorar la seguridad de la información en el gobierno local de Paucará.

La investigación se basa en el método Top Down de Cisco. Identifica y analiza el estado actual de la infraestructura, tratando de identificar las necesidades y dificultades en la gestión de la red de datos, la falta de seguridad y los riesgos que enfrenta la red. Obtener información de diversas fuentes, como documentos internos y observaciones de la organización.

Palabras clave: Vlan, seguridad de la información, infraestructura de red.

ABSTRACT

This research entitled: "DATA NETWORK INFRASTRUCTURE DESIGN FOR INFORMATION SECURITY IN A LOCAL GOVERNMENT, 2021" Its emergence is due to the importance of information today, it is the most important resource in the organization, and takes into account the various vulnerabilities that exist due to advances in technology and communications.

The research problem: How does the design of the data network infrastructure improve information security in the Local Government of Paucará? There is currently a data network infrastructure that does not fulfill the functions for the one that was implemented.

The research aims to design a data network infrastructure that integrates the current completely independent voice network infrastructure and the data network infrastructure to provide better data transmission and improve information security in the local government of Paucará.

The research is based on Cisco's Top Down method. Identify and analyze the current state of the infrastructure, trying to identify the needs and difficulties in managing the data network, the lack of security and the risks faced by the network. Obtain information from various sources, such as internal documents and observations of the organization.

Keywords: Vlan, information security, network infrastructure.

INTRODUCCIÓN

La Tesis “DISEÑO DE INFRAESTRUCTURA DE RED DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UN GOBIERNO LOCAL, 2021” se basó en el diseño de una Infraestructura de red de datos para mejorar la seguridad de la información de la entidad local que es el Gobierno Local de Paucara, utilizando los elementos básicos requeridos para su funcionamiento optimizado. La red debe soportar completamente las comunicaciones de datos, VoIP, video y audio, y la red debe tener seguridad, esta es una característica de cualquier sistema, que nos dice que no tiene ningún peligro, daño o riesgo que afecte su funcionamiento directo o sus resultados.

En el trabajo de investigación se realizó el diseño de la infraestructura de la red de datos en la presente gestión del gobierno local de Paucara, el trabajo integral se dividió en cuatro capítulos que son descritos uno por uno seguidamente.

El primer capítulo, muestra los aspectos generales del trabajo, como las preguntas, los objetivos y los supuestos en la metodología de la investigación.

El segundo capítulo, presenta las bases teóricas, el marco teórico, los antecedentes de la investigación, las bases teóricas, las hipótesis y las variables de investigación que ayudan a reconocer y comprender el desarrollo del trabajo.

El tercer capítulo, presenta la metodología de investigación, aclara el alcance de la investigación, el tipo de investigación, el nivel de investigación, el método de investigación y el diseño de la investigación. Asimismo, población, muestras, muestreo, técnicas y herramientas de recolección de datos, procedimientos de recolección de datos y técnicas de procesamiento.

El cuarto capítulo, cubren los resultados y discusión de cada hipótesis, con base en sus respectivos indicadores para medir las variables de investigación. Finalmente, expone las conclusiones y recomendaciones utilizadas en la investigación, bibliografía y enlaces correspondientes.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

Hoy en día en la era de la informática para todas las organizaciones a nivel internacional la información es el recurso activo más importante para la toma de decisiones y es necesario que este recurso sea manejado de manera muy organizada y con seguridad en bien de la organización.

Esto corrobora **Chiavenato I.** (2006) donde manifiesta que la información "es un conjunto de datos significativos, es decir, para reducir la incertidumbre o aumentar la comprensión de algo. De hecho, la información es un tipo de información significativa en un contexto específico, que se puede utilizar de inmediato y reducir la incertidumbre de nuestra decisión". En esta definición, es importante enfatizar que la información que se transmite tiene un significado según el contexto, pero está destinada a tomar una decisión.

Las redes y telecomunicaciones, en nuestro país y en el mundo están en gran crecimiento, aquellas con mayor proporción de todos los servicios de comunicación de voz y datos están en constante desarrollo, lo que beneficia a las personas y organizaciones al utilizar diferentes servicios, por ejemplo; transmisión en tiempo real, enviar mensajes de voz, datos, envío de archivos grandes, descarga de archivos, música, videos, etc., esto nos ha beneficiado mucho en todos los ámbitos, sin embargo muchas instituciones aun no cuentan con estos servicios, como es el caso del Gobierno Local de Paucará.

La seguridad de la información es un conjunto de medidas preventivas y de respuesta para organizaciones y sistemas tecnológicos que pueden

proteger y resguardar la información para mantener la confidencialidad, la disponibilidad y la integridad de los datos.

En referencia a ello, **Vergara G.** (2017) en su tesis sobre Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016, se cree que la seguridad de la información tiene un impacto muy importante en la calidad del servicio, porque la información oportuna y segura es un recurso muy importante para la toma de decisiones organizacionales y el logro de metas.

El proceso del flujo de información pasa de oficina en oficina de manera regular; dicha información documentaria que se manipula ya sea física o digitalmente muchas veces son de carácter reservado, confidencial y secreto, y no solo los aspectos documentarios, también la información que considera al software, los aplicativos, herramientas y servicios indirectos que engloba; los cuales requieren implementar controles en el hardware de la computadora, en sus aplicaciones y sistemas de información que utilizan en cada una de sus oficinas administrativas.

La red LAN del Gobierno Local de Paucará tiene una antigüedad de 10 años, al cual no se le dio el respectivo mantenimiento encontrándose en el presente en mal estado, lo que significa que en su momento no se halla diseñado la red con los estándares y normativas necesarias. El gobierno local de Paucará cuenta con un proveedor de servicio de internet con capacidad de descarga de 69.01 Mbps y carga de 19.84 Mbps, la entidad cuenta con un total de 75 usuarios que hacen uso de la red de datos e internet, siendo en estas actividades donde se muestran los problemas de seguridad de la información teniendo como causas la mala administración del ancho de banda, la lentitud y latencia en la transmisión y distribución de información, perdida de información, cableado de la red sin un diseño lógico, todo ello causando malestar y quejas de los usuarios al responsable de la Oficina de Computación e Informática.

Figura 1

Incremento de Host en el Gobierno Local de Paucará

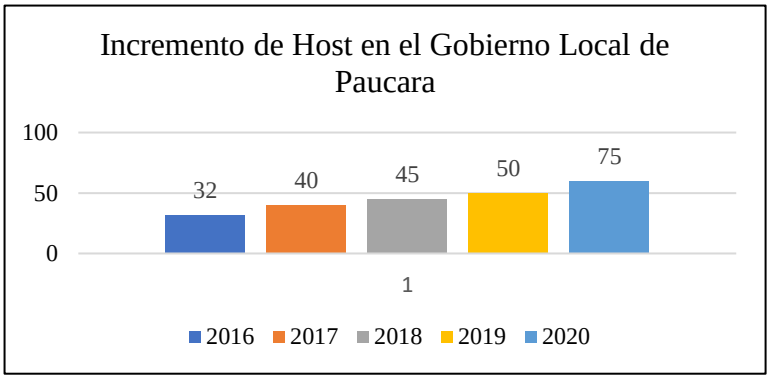
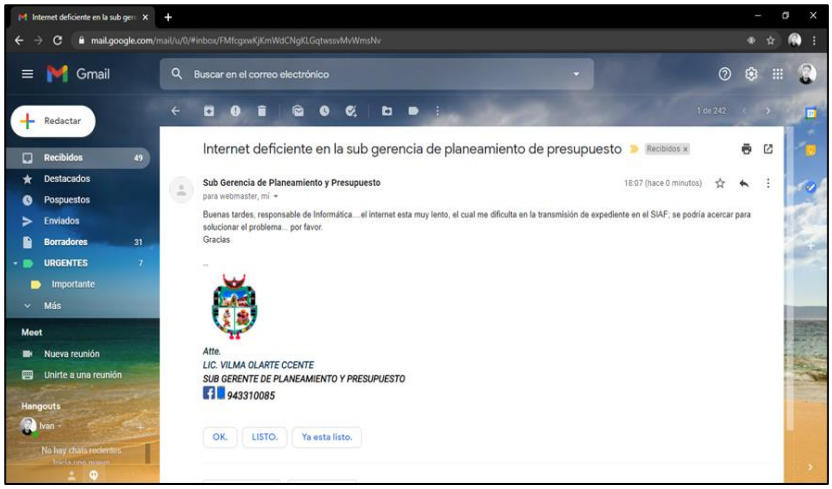


Figura 2

Situación Actual del Cableado de red.

Figura 3

Queja de usuarios con respecto al servicio de internet.



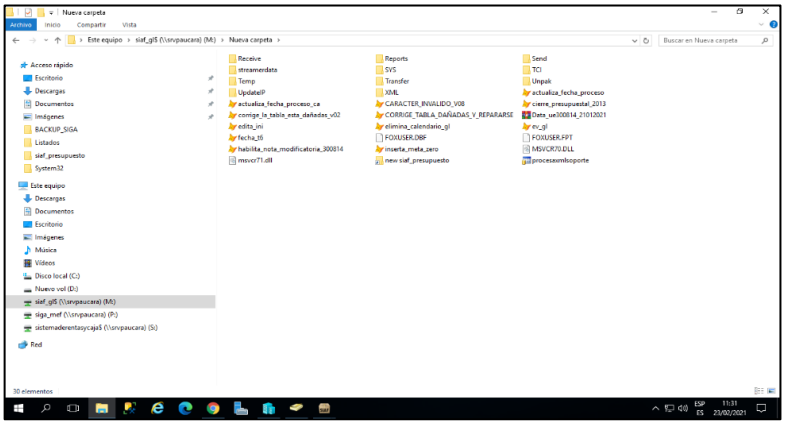
Así mismo, la seguridad se ha vulnerado en relación con la información que se maneja dentro de la institución, existiendo un riesgo muy alto de que la información se vulnere o se pierda ya que la mayor parte de la información fluye en los sistemas informáticos tales como Sistema Integrado de Administración Financiera (SIAF), Sistema Integrado de Gestión Administrativa (SIGA) y otros sistemas del Gobierno Local de Paucará. Estos sistemas ya mencionados no se encuentran con la seguridad necesaria como debería ser, la Red LAN se encuentra configurada de manera libre, no existe administración de los usuarios, esto hace que cualquier usuario se podría conectar a la red y así acceder a la información que fluye en la red. Los sistemas informáticos con que cuenta la entidad se encuentran compartido en la red LAN sin seguridad por lo que los usuarios pueden acceder como clientes a la raíz de cada sistema, y es allí donde por desconocimiento eliminan los componentes del sistema SIGA, SIAF y otros sistemas retrasando el trabajo diario de los usuarios en general.

Figura 4

Eliminación de componentes del SIGA.

Figura 5

Eliminación de componentes del SIAF.



A razón de que los sistemas informáticos están compartidos en la red, cualquier usuario conectado a la red puede acceder a los recursos compartidos y es allí donde acceden y vulneran la información y sobre todo la molestia de los altos funcionarios de la entidad.

Figura 6

Queja de los usuarios sobre accesos no autorizados al SIAF.

La investigación se desarrolló en el Gobierno Local de Paucará, el cual propone un diseño de infraestructura de red de datos para mejorar la seguridad de la información, enmarcados en los estándares de ISO27001:2013, contextualizado para una entidad pública. Para el proceso de experimentación se tomó el total de host conectados en la red. Se propone una forma diferente de gestionar la seguridad de la información en la red de datos de la entidad en mención.

El propósito de la presente investigación fue proponer un diseño de infraestructura de la red de datos con las nuevas tecnologías y estándares para contribuir en la mejora de la seguridad de la información en el Gobierno Local de Paucará, además para contribuir en la investigación y ser aplicado a instituciones para solucionar problemas similares.

1.2. Formulación del problema

1.2.1. Problema General

¿De qué manera el diseño de infraestructura de red de datos influye en la seguridad de la información en el Gobierno Local de Paucará?

1.2.2. Problemas Específicos

a) ¿Cómo el diseño de infraestructura de red de datos influye en la Integridad de la Información del Gobierno Local de Paucará?
b) ¿Cómo el diseño de infraestructura de red de datos influye en la Disponibilidad de la Información del Gobierno Local de Paucará?
c) ¿Cómo el diseño de infraestructura de red de datos influye en la Confidencialidad de la Información del Gobierno Local de Paucará?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar de qué manera el diseño de infraestructura de red de datos influye en la seguridad de la información en el Gobierno Local de Paucará.

1.3.2. Objetivos específicos

a) Demostrar la influencia del diseño de infraestructura de red de datos en la Integridad de la Información en el Gobierno Local de Paucará.
b) Demostrar la influencia del diseño de infraestructura de red de datos en la Disponibilidad de la Información en el Gobierno Local de Paucará.

c) Demostrar la influencia del diseño de infraestructura de red de datos en la Confidencialidad de la Información en el Gobierno Local de Paucará.

1.4. Justificación

1.4.1. Justificación Social o práctica

Las organizaciones dependen del desarrollo tecnológico, por eso esta investigación permitió diseñar una infraestructura de red teniendo un conocimiento amplio de las redes, que depende del desarrollo tecnológico, la calidad de transmisión, la seguridad de la información y el buen uso del ancho de banda interno y externo son características que sirven al buen uso de la red y la transmisión de información.

Este documento permitirá a las organizaciones mejorar la transmisión de información, la seguridad de la información y lograr una gestión técnica centralizada para garantizar el uso completo de los recursos técnicos disponibles.

1.4.2. Justificación Metodológica

Esta tesis es factible porque brindará soluciones a problemas organizacionales, como el ahorro de dinero, la facilidad de comunicación y el poder compartir información, se hizo uso de la metodología Top Down de cisco, que costa de 4 fases. Además, se tomará como guía el ISO27001:2013 para la gestión de la seguridad de la información.

1.4.3. Justificación Teórica o Científica.

Esta investigación es teóricamente razonable, pues las variables "modelo de infraestructura de red de datos" y "seguridad de la información" muestran la confiabilidad del conocimiento relacionado con la teoría propuesta en el marco teórico, lo que permite evaluar la importancia de las variables reflexionar y debatir, afrontar o verificar la teoría propuesta para comprobar su utilidad. Por tanto, los resultados

obtenidos ayudan a ampliar los conocimientos sobre el tema. También servirá como base para futuras investigaciones.

1.5. Importancia de la investigación

Muchas de las organizaciones, cuentan con recursos tecnológicos que promueven el desarrollo de diferentes actividades internas. Generalmente, los recursos se comparten a través de medios de transmisión, es decir, se configuran las redes informáticas.

La propuesta de esta investigación es diseñar un modelo de infraestructura de red de datos que permita compartir programas y archivos almacenados en servidores a los que puedan acceder muchos usuarios de la red al mismo tiempo. Comparta recursos de red, como impresoras, escáneres, dispositivos de almacenamiento, sistemas informáticos, etc. Permitió la conexión de estaciones de trabajo que permitieron el intercambio de información y el desarrollo de actividades de optimización salvaguardando la seguridad de la información y los recursos compartidos en el Gobierno Local de Paucará. El modelo servirá para que otras instituciones de similar infraestructura lo utilicen y puedan referenciar en sus distintas aplicaciones. En la presente investigación se realizó el diseño de la infraestructura de red, no así la implementación del diseño desarrollado.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación.

2.1.1. Antecedentes Internacionales

Castrizano Y. (2019); en su tesis de maestría titulado**:** ***"Configuración de la Red de Datos para los servicios de Acceso a la red por Suscripción de ETECSA"***. Investigación realizada en la Universidad Central Marta Abregú de la Villas de Santa Clara Cuba, tuvo como objetivo principal proponer una Configuración de la Red de Datos para el Servicio de Acceso a la Red por Suscripción de ETECSA, bajo el método de acceso PPPoEv6, de tal forma que se logre aumentar las capacidades de conectividad de la Red y disminuir el uso de las direcciones públicas IPv4 y el de las licencias CGN, la investigación primero analiza el estado actual del servicio de acceso a la red por suscripción, su arquitectura de servicio y sus componentes funcionales. También evaluó el estado actual del agotamiento de direcciones IPv4 y discutió técnicas para mitigarlo. La investigación concluye que las Redes de Datos que soportan los Servicios de Acceso a Internet por Suscripción pueden ser analizadas usando un Modelo de Red que divide la Infraestructura en Capas. Cada una de las capas está compuesta por dispositivos de red y las funciones que estos realizan. Las funciones relacionadas con los Servicios de Acceso por Suscripción pueden ser agrupadas en: (i) Reenvío de Tramas, (ii) Traducción de Direcciones, (iii) Métodos de Acceso y (iv) Enrutamiento.

Esta investigación guarda relación con este proyecto, ya que considera los niveles de acceso a la red y su aplicación del método

PPPoEv6 para un mejor funcionamiento y aprovechamiento de los recursos.

Vidal J. (2016); en su tesis de maestría titulado: ***"Diseño una propuesta de mejoramiento en la infraestructura de red de datos en la ESPAM MFL con calidad de servicio".*** Investigación realizada en la Pontificia Universidad Católica del Ecuador, el cual tuvo como objetivo principal diseñar la infraestructura de red con calidad de servicio para mejorar el funcionamiento del flujo de información de la red de datos ESPAM MF, todo ello desarrollado bajo la metodología de James McCabe y el enfoque Inductivo - Deductivo, llegando a concluir que la tecnología inalámbrica de cuarta generación, como IEEE 802.11n, tiene una frecuencia de 2,4 GHz, pero el estándar 802.11n puede mostrar su capacidad real y lograr la velocidad de transmisión de datos más alta a una frecuencia de 5 GHz. Cualquiera que diseñe una nueva WLAN debe elegir la banda de 5 GHz.

Este antecedente guarda relación con la presente investigación por que se hizo un estudio de la red actual de la organización y posterior a ello se plantea un diseño integrado más optimo basado en Vlan y la metodología de James McCabe que permite mejorar la calidad de servicio, seguridad a ataques externos, seguridad interna de usuarios y sobre todo tiene la similitud en el desarrollo de la red.

Galarza C. (2018); en su artículo científico titulado: ***"Diseño e implementación de una red de datos segura para la Pontificia Universidad Católica del Ecuador, Santo Domingo"***, con el propósito de realizar la recolección de información, se analizan e identifican las vulnerabilidades de los equipos de conmutación de dos capas, luego se implementan las medidas correctivas y se realizan las pruebas de desempeño correspondientes. El método utilizado en el diseño de la red es CISCO. Al implementar configuraciones de seguridad correctivas en la infraestructura de red de datos de capa 2, el nivel de seguridad se puede aumentar como medida preventiva contra el acceso no autorizado a diferentes recursos, y se puede reducir el uso de vulnerabilidades de

capa 2, mejorando así la integridad, la disponibilidad y la confidencialidad. de información.

Este artículo científico, guarda relación con este proyecto, ya que contribuye con los métodos de levantamiento de la situación actual de la red además de los métodos de desarrollo de red como es el CISCO y los VLANS.

Espinosa O. (2015) en su artículo científico titulado: ***"Implementación de Arquitectura de Redes Seguras"***, se realizó esta investigación desde el punto de vista de los pilares de la seguridad informática como son: la integridad, la disponibilidad y la confidencialidad de los muchos tipos de organizaciones, como son las de tipo financiero o las gubernamentales que tienen el problema de la seguridad de la información y es imprescindible proteger los activos, también, por reglamentación se deben cumplir ciertas normas basadas en estándares de seguridad, por lo que es necesario que estas enfoquen sus esfuerzos en la implementación arquitecturas de redes seguras. A razón de ello se elaboró un prototipo de arquitectura con los estándares de seguridad y Vlan bajo la metodología CISCO y los métodos adicionales de Clúster, llegando a la conclusión de que una correcta implementación desde el punto de vista técnico, se puede mejorar la seguridad de las organizaciones, con unas correctas políticas de seguridad, compromiso de la alta dirección y la conciencia de seguridad del recurso humano.

Este artículo científico, guarda relación con este proyecto, en el sentido de que justifica y evidencia los pilares de la seguridad de la información como son: integridad, disponibilidad y la confidencialidad en red de toda organización.

2.1.2. Antecedentes Nacionales

Pacheco L. (2013); en su tesis de maestría titulado: ***"Diseño de un modelo de sistema integrado de infraestructura de red de datos para mejorar la gestión de la información en la municipalidad***

distrital de Mariscal Cáceres". Investigación realizada en la Universidad Nacional del Centro del Perú. La investigación fue cuantitativa, de tipo descriptiva – propositiva de nivel explicativo. El objetivo principal de la investigación fue diseñar un Modelo de Sistema Integrado de Infraestructura de Red de datos para Mejorar la Gestión de la Información en la Municipalidad Distrital de Mariscal Cáceres, con el cual busca integrar la comunicación de Voz y Datos y la optimización de las actividades dentro de la organización el cual fue desarrollada mediante la metodología de TOP-DOW con la guía de Cisco. Llegando a la conclusión que El modelo de sistema integrado proporciona una mayor seguridad de los datos y evita el acceso no autorizado de terceros, lo que se logra a través de redes virtuales y listas de control de acceso.

Esta investigación es importante ya que guarda una relación en el diseño de un modelo de sistema integrado basado en la metodología de Top – Dow de CISCO para la optimización de los trabajos diarios de la organización, además contribuye para la formulación de objetivo de la investigación.

Maldonado H. (2018); en su tesis de posgrado titulado: ***"Tecnología IP para la mejora de la gestión administrativa de la Municipalidad Distrital de Perene"***, realizada en la Universidad Nacional del Centro del Perú. La investigación desarrollada tuvo el enfoque cuantitativo, el tipo fue aplicada y el nivel de investigación explicativo, tuvo como objetivo reducir el tiempo de atención a los usuarios con el diseño de la Tecnología IP para la mejora de la gestión administrativa de la Municipalidad Distrital de Perene, todo ello desarrollado bajo la metodología de James McCabe y CISCO. Concluye que la implementación de tecnología IP puede mejorar el servicio a los usuarios en el distrito y ciudad de Perene. Según análisis estadístico de satisfacción, la tasa de aceptación del proyecto es del 0,84%, y permite la integración en la misma red con tecnología IP las comunicaciones de datos y voz, por lo que los servicios internos de cada área de la Municipalidad distrital de Perene están más optimizados.

Este antecedente guarda relación con el presente proyecto en el desarrollo el modelo de infraestructura de red con la metodología de James McCabe y CISCO, en donde detalla específicamente los procesos a desarrollar y la influencia en la mejora de atención de los usuarios de la institución. También resaltar que en esta investigación se diseña la red mediante Vlan que tiene mejor rendimiento y además considera que la tecnología IP es muy importante en la gestión de información.

Coras J. (2013); en su tesis de posgrado titulado: ***"Rediseño de la red de comunicaciones basado en tecnologías de alta disponibilidad de gestión de tráfico para mejorar la comunicación de la Municipalidad Provincial de Churcampa - Huancavelica"***, realizada en la Universidad Nacional del Centro del Perú, el cual como objetivo principal fue determinar la influencia del rediseño de la red de comunicaciones basadas en tecnología de alta disponibilidad de gestión de tráfico en la comunicación de la Municipalidad Provincial de Churcampa – Huancavelica todo ello basado en la metodología de TOP – DOWN de Cisco. La investigación desarrollada tuvo el enfoque cuantitativo, el tipo fue aplicada y el nivel de investigación explicativo. La investigación concluye que mediante la aplicación de tecnología de alta disponibilidad en el rediseño de la red de comunicaciones se asegura la alta eficiencia, seguridad y disponibilidad del sistema, el cual debe ser aprovechado al máximo por los empleados del Gobierno Provincial y Municipal de Churcampa.

Esta investigación guarda relación con este proyecto donde detalla la implementación de la tecnología de alta disponibilidad bajo me metodología de Top-Down a base de un análisis muy detallado de la situación actual para luego establecer una mejor comunicación en la red de datos y el cual se ha aplicado en una Municipalidad, en ese sentido considera muchos aspectos con respecto a la eficiencia, seguridad y disponibilidad de la información.

Guzman G. (2015); en su tesis de maestría titulado: ***"Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega"***, desarrollado en la ciudad de Huancayo, el cual tuvo como objetivo principal determinar el nivel de importancia de la metodología de seguridad de tecnologías de información y comunicaciones que permita la continuidad de procesos de la clínica Ortega, todo ello desarrollado mediante las normas y estándares de ISO 27002, COBIT, ITIL. Esta investigación nace para salvaguardar su seguridad consiste en mantener la calidad del servicio y garantizar la eficacia y eficiencia de los procesos comerciales y el valor de sus activos. La conclusión es que el modelo de seguridad propuesto consta de varias áreas, cada una de las cuales tiene implementados controles de seguridad. De esta forma se mejora el nivel de seguridad, que se mide por asignación, y el valor inicial es 16 y el valor final es 50.

Este antecedente guarda relación con respecto a este proyecto por la aplicación el estándar de gestión de riesgos (serie ISO/IEC 27.000) y el (ISM3) como una metodología para gestionar la seguridad de la información.

2.2. Bases teóricas

2.2.1. Que es una red

Como menciona **Molero** (2013) y **Gunter** (1998), definen una red, como "estructura de conexión de computadoras, que permite a la visión del mundo compartir recursos como: transmisión de datos, aplicaciones, video, voz e imágenes. La conexión de dichas computadoras también se realiza en el mismo entorno o en países vecinos"

Por otro lado, Pérez (2008), hace referencia que una red es un grupo de computadoras interconectadas y otros dispositivos que permiten a los usuarios compartir información. Se basan en su alcance (red de área personal o PAN, red de área local o LAN, red de área metropolitana o

MAN, red de área amplia o WAN, etc.), su forma de conexión (mediante cable coaxial, fibra óptica, radio, microondas, infrarrojos) o relación funcional (client-server, person to person), etc.

2.2.1.1.Características

Según, **Juliá** (2013), menciona las 5 características de una buena red que nos permite definir su funcionalidad:

a) **Velocidad**

Se denomina velocidad a los datos transferidos (bytes y bits) a través de la red por segundo. Por lo general, se miden mediante pruebas de velocidad. La velocidad de carga y descarga de datos variará, según el estándar que usemos y el tipo de red o medio (inalámbrico, fibra óptica, teléfono o cable coaxial) utilizado para transmitir los datos.

b) **Seguridad de red**

Este es uno de los aspectos más peligrosos que rodean a las redes inalámbricas. Los intrusos ocupan nuestro ancho de banda es una de las razones que hacen que estas redes sean más vulnerables a los ataques.

Por otro lado, las redes cableadas pueden verse interferidas por el uso de otros equipos (como microondas). A diferencia de estos, la fibra óptica tiene una excelente seguridad.

c) **Confiabilidad**

Mide la probabilidad de que un nodo de la red falle y, por tanto, causen fallos. Esto depende en parte de la topología de red que instalamos y la ubicación del componente defectuoso. Cuando uno de los componentes no funciona, afectará al funcionamiento de toda la red y viceversa, planteando un problema local.

d) Escalabilidad

La red no puede seguir agregando nuevos componentes y esperar que funcione a la misma velocidad. Cuando agregamos nuevos nodos y se están ejecutando al mismo tiempo, la conexión a Internet se reduce, la velocidad de transmisión de datos es generalmente menor y la posibilidad de errores es mayor.

e) Disponibilidad

Es la capacidad de la red de estar disponible y completamente activa cuando la necesitamos. Estamos discutiendo el tiempo posible para que los nodos cumplan con las condiciones de rendimiento necesarias dentro de nuestra empresa. El objetivo es hacer que la red esté disponible de acuerdo con las necesidades de uso de la red instalada.

2.2.1.2.Ventajas y Desventajas

Según, **Gilberto J.** (2012):

Ventajas

- Seguridad.
- Los periféricos comparten recursos.
- Base de datos compartida.
- Mejora de la organización de la empresa.
- Interconexión.

Desventajas

- La vida útil de los equipos periféricos es corta.
- Dividir los conflictos entre el acceso ilegal y la transmisión simultánea.
- Entrada de malware.
- Información perdida y robada.

2.2.1.3.Clasificación de redes por alcance

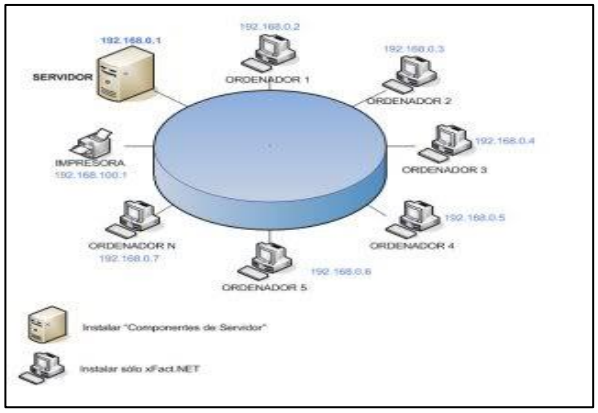
Según, **Porto & Ana** (2008) y **Juliá** (2015) Suelen existir muchas redes, y teniendo en cuenta que cada una de ellas tiene propiedades distintas, es muy común verlas aceptadas las que a continuación se detallan:

Red de área personal (PAN)

Son redes informáticas que se extienden hasta los 10 metros, similar a la distancia Bluetooth de los dispositivos móviles. Son muy básicos y se pueden utilizar en salas de reuniones. Se utiliza para comunicar dispositivos de información en computadoras con diferentes tecnologías cercanas a las personas.

Figura 7

Red de área personal.

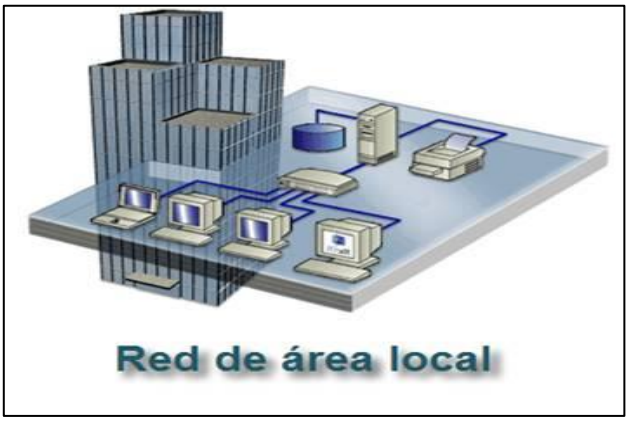


Red de área local (LAN)

Son grupos de computadoras y dispositivos que comparten líneas o enlaces inalámbricos a través de servidores. LAN incluye computadoras, impresoras, escáneres, fotocopiadoras, etc., que están conectados a servidores instalados en edificios o empresas con las que la mayoría de nosotros estamos familiarizados. La red LAN tiene un rango de cobertura de 200 metros a 1 kilómetro y su velocidad de transmisión es de 10 a 100 Mbps (megabits por segundo).

Figura 8

Red de área Local.



Red de área amplia (WAN)

Son desarrollados por una organización o empresa para su uso Privado, proporcionando conexiones a sus clientes a través de un proveedor de Internet. La velocidad de transmisión está entre 1 Mbps y 1 Gbps, oscilando entre 100 kilómetros y 1000 kilómetros, es decir, estas redes se utilizan para conectar diferentes regiones geográficas o países.

Figura 9

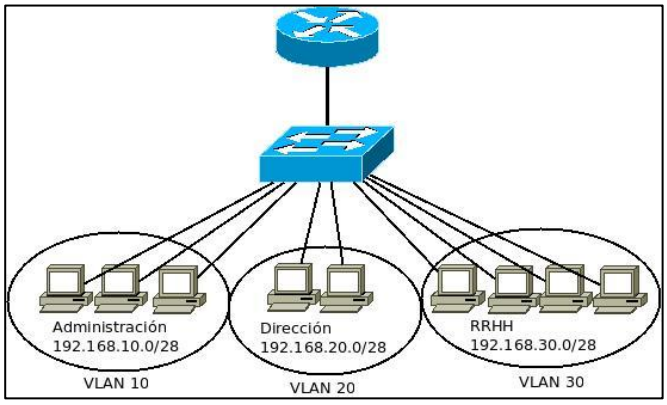
Red de área Amplia.

Red de área local virtual (VLAN)

Las VLAN están vinculadas lógicamente (a través de protocolos, puertos, etc.) para reducir el tráfico de red y mejorar la seguridad. Si una empresa tiene varios departamentos y desea que utilicen redes independientes utilizan las VLAN.

Figura 10

Red de Área Local Virtual.



2.2.2. Infraestructura de red de datos

Según **Behrouz A.** (2007) La infraestructura de red nombra todos estos elementos básicos y esenciales para cualquier organización pública o privada (empresa, oficina o industria) que necesite todo o parte de los siguientes servicios de telecomunicaciones: teléfono, fax, computadora, escáner, impresora, TPV, cámaras de control y vigilancia, control de acceso, teléfono de datos, aire acondicionado, extinción de incendios.

Con base en lo anterior, la construcción de una infraestructura de red, no sólo permitirá a la organización reducir los gastos de funcionamiento y el personal técnico. Sino que, a su vez, mejorará la capacidad de gestión de la infraestructura de tecnología de la información y reducirá la dependencia de los flujos de información.

2.2.3. Dimensiones de la Infraestructura de red de datos

Según **Cisco S.** (2004) los pilares fundamentales de infraestructura de red son los siguientes.

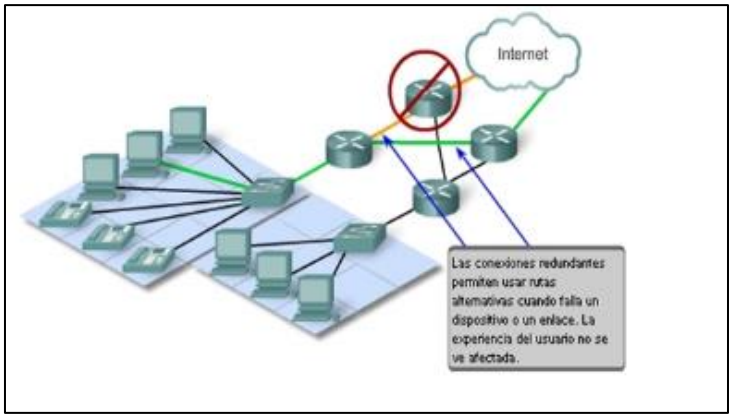
a) Tolerancia a fallas

La expectativa de que Internet siempre estará disponible para millones de usuarios confiables requiere el diseño y la construcción de arquitecturas de red tolerantes a fallas. Las redes tolerantes a

fallas pueden limitar el impacto de fallas de hardware o software y pueden recuperarse rápidamente cuando ocurren tales fallas. Estas redes se basan en enlaces o rutas redundantes entre el origen y el destino de los mensajes. Si el enlace o el enrutamiento falla, el proceso garantiza que el mensaje se pueda enrutar inmediatamente a un enlace diferente, que sea transparente para los usuarios en ambos extremos. Tanto la infraestructura física como el proceso lógico de enrutamiento de mensajes a través de la red están diseñados para adaptarse a esta redundancia. Esta es la premisa básica de la arquitectura de red actual.

Figura 11

Tolerancia a Fallas.



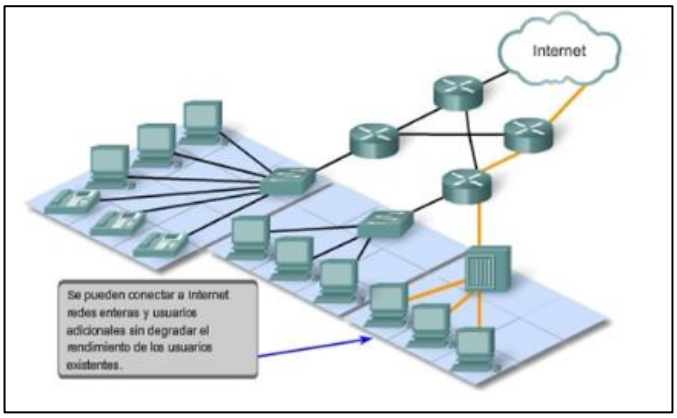
b) Escalabilidad

Las redes escalables se pueden expandir rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento de los servicios proporcionados a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicios se conectan a Internet cada semana. La capacidad de la red para soportar estas nuevas interconexiones depende del diseño jerárquico de la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios conectarse sin interrumpir toda la red. El desarrollo tecnológico continúa mejorando las capacidades de mensajería y el rendimiento

de cada capa de componentes de la estructura física. Estos desarrollos, así como los nuevos métodos de identificación y localización de usuarios individuales dentro de Internet, permiten que Internet se adapte a las necesidades de los usuarios.

Figura 12

Escalabilidad.

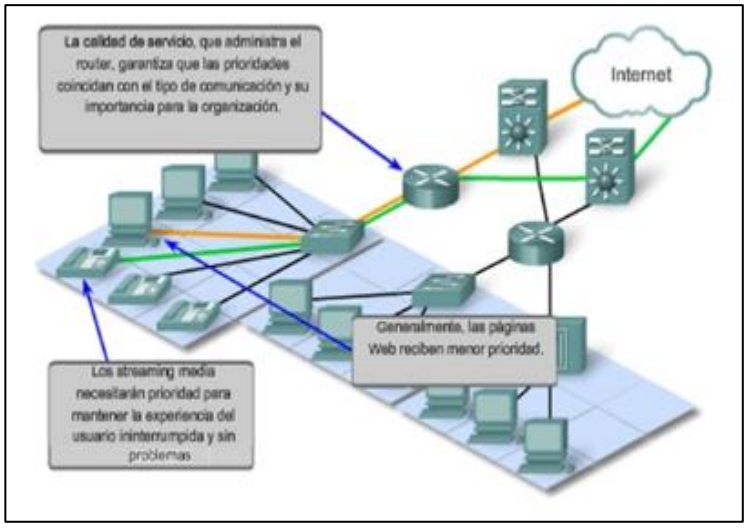


c) Calidad de Servicio (QoS)

Actualmente, Internet ofrece a sus usuarios niveles aceptables de tolerancia a fallos y escalabilidad. Pero las nuevas aplicaciones disponibles para los usuarios en Internet han creado mayores expectativas sobre la calidad de los servicios prestados. La transmisión de voz y video en tiempo real requiere un nivel constante de calidad y transmisión ininterrumpida, lo cual es innecesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide experimentando personalmente la calidad de las mismas presentaciones de audio y video. Las redes tradicionales de voz y video están diseñadas para admitir un solo tipo de transmisión y, por lo tanto, pueden producir niveles aceptables de calidad. Los nuevos requisitos para respaldar esta calidad de servicio en redes convergentes han cambiado el diseño y la implementación de las arquitecturas de red.

Figura 13

Calidad de Servicio.

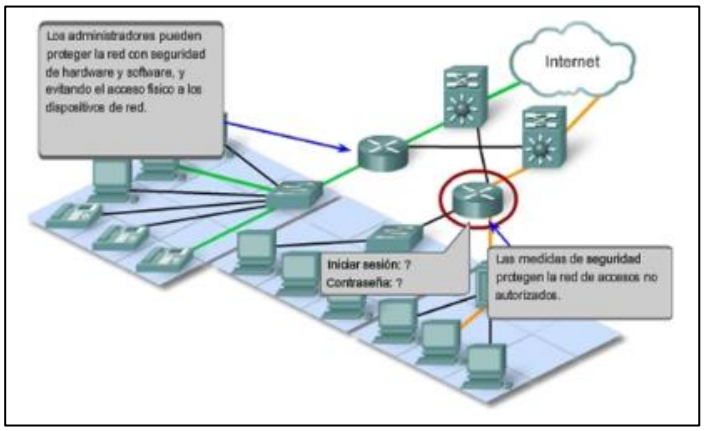


d) Seguridad

Internet ha evolucionado de una Internet de organización educativa y gubernamental estrictamente controlada a un medio de transmisión de comunicación personal y comercial ampliamente accesible. Por lo tanto, los requisitos de seguridad de la red han cambiado. Las expectativas de privacidad y seguridad que surgen del uso de Internet para intercambiar información comercial sensible y crítica están más allá de lo que puede proporcionar la arquitectura actual. La rápida expansión del campo de las comunicaciones donde las redes de datos tradicionales no pueden proporcionar servicios ha aumentado la necesidad de incorporar seguridad en la arquitectura de la red. Por lo tanto, se ha realizado un gran esfuerzo en este campo de investigación y desarrollo. Al mismo tiempo, se están implementando muchas herramientas y procedimientos para contrarrestar las fallas de seguridad inherentes a la arquitectura de la red.

Figura 14

Seguridad.



e) Acceso a recursos compartidos

Compartir permite a los usuarios acceder a archivos y carpetas a través de la red. Los usuarios pueden conectarse a recursos compartidos a través de la red y acceder al contenido que contiene: aplicaciones y datos públicos o de usuario. Esta función nos permite compartir recursos, archivos, etc. con personas de la misma red. Para que podamos conectarnos en la misma red y transferir archivos y compartirlos entre nosotros.

Figura 15

Acceso a recursos compartidos.

2.2.4. LAN Virtuales (VLAN)

2.2.4.1.Definición de VLAN

Una Red virtual local más conocido como VLAN, es una manera de generar redes lógicas que trabajen de forma independiente en una misma infraestructura de red física.

Diferentes redes virtuales pueden existir en un mismo dispositivo de comunicación conocido como el switch o en una infraestructura de red física. Podemos decir que son necesarios para aminorar el tamaño de dominio de broadcast y es ventajoso en la administración de la red de datos, dividiendo en segmentos más pequeños de una red local. (Cisco Networking Academy, 2009).

A. Uso de las VLAN

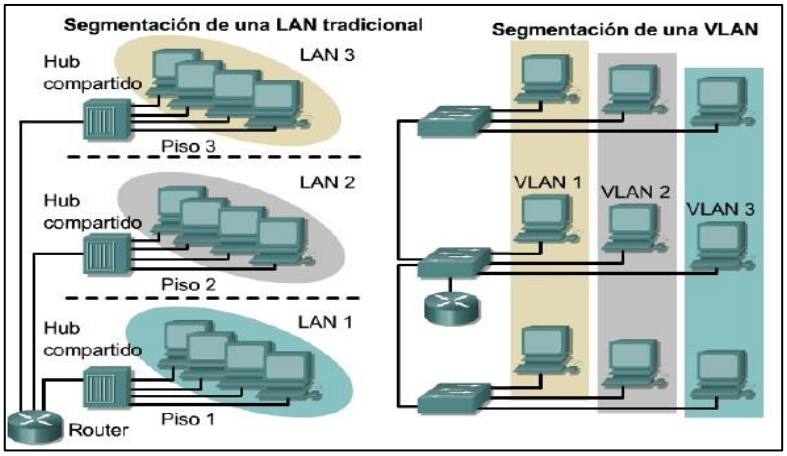
En una infraestructura de red de área local más conocido como LAN, todos los hosts que pertenecen a un mismo switch o grupo de switch conectados entre sí, comparten el mismo dominio de broadcast. Esto hace que, paquetes que llegan a una LAN será replicado a todos los puertos del switchs o grupo de switchs. Esto hace que se reduzca el rendimiento de la red por el uso excesivo del ancho de banda en el envío de mensajes. (Pergandon, 2015).

Es usual que en una misma red de área local existan usuarios que pertenecen a diferentes grupos de trabajo. Habitualmente los mensajes de difusión solo corresponden a los dispositivos que pertenecen a un mismo grupo de trabajo, a cada host llegan mensajes de diferentes grupos de trabajo que no le corresponden, y de esta manera hacen uso de un ancho de banda que pudiera ser aprovechado en el envió de otros datos. Como podemos ver en la gráfica, hay dos formas de dar solución. (Pergandon, 2015).

- **Utilizar routers**: El router o enrutador es un dispositivo que permite dividir dominios de broadcast, eso nos quiere decir que los mensajes que se envían en una LAN no son enviados a otras redes locales. (Pergandon, 2015).

Figura 16

Segmentación utilizando router y redes virtuales.



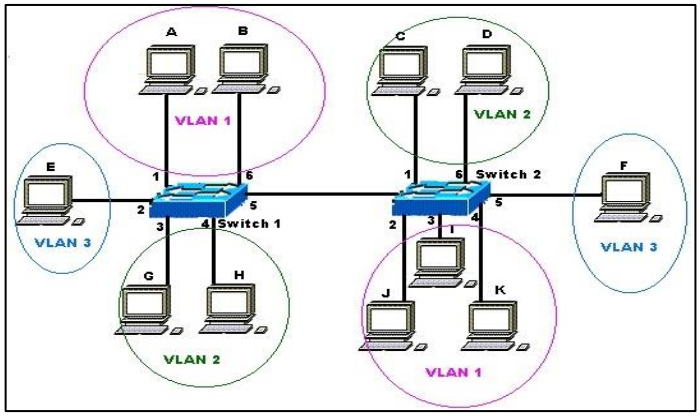
Fuente: (Pergandon, 2015)

- **Implementar redes de área local virtual (VLAN)**

  Una VLAN está conformada por un conjunto lógico de hosts, de forma física están conectadas a uno o más equipos switchs, estos pueden ser administrados como una subred. Cada host se comunicará solamente con otros hosts de su grupo, pese a que un host de otro grupo esté conectado en el mismo switch. (Pergandon, 2015).

  Figura 17

  Segmentación de una red en VLAN.



Fuente: (Pergandon, 2015)

B. Tipos de Vlan

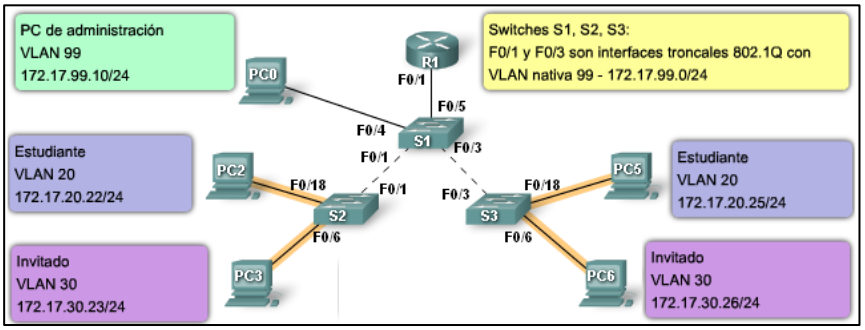
Existen varias formas de establecer una VLAN dependiendo de la forma de agrupar los nodos de la red:

Vlan de datos

Una VLAN de datos es una red lógica cuya configuración sirve para enviar tráfico de datos que es generado por los usuarios. Esta VLAN puede mandar tráfico basado en voz o tráfico que es utilizado para gestionar el switch, este tráfico de datos no formaría parte de una VLAN de datos, es una forma común de los administradores de red apartar el tráfico generado por voz y del tráfico generado en la gestión de los equipos de comunicación. La importancia de dividir los datos de tráfico de voz y el de la gestión de los equipos de comunicación, radica en que esos datos se envíen en ese mismo segmento, ya sea en el segmento de voz o datos. (Cisco Networking Academy, 2009).

Figura 18

Vlan de Datos.



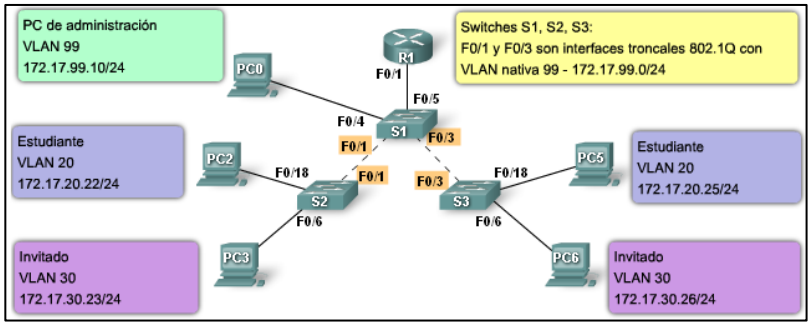
Fuente: (Cisco Networking Academy, 2009)

Vlan predeterminada

Luego que el switch entre en funcionamiento todos los puertos pertenecen a la vlan predeterminada que por defecto es la VLAN 1, esto hace que todos esos puertos pertenezcan al mismo dominio de difusión, como es una Vlan predeterminada esta no se puede renombrar o eliminar. (Cisco Networking Academy, 2009).

Figura 19

Vlan Predeterminada.



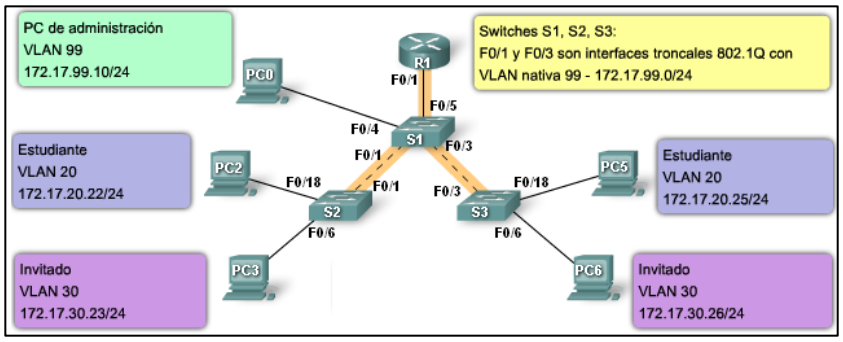
Fuente: (Cisco Networking Academy, 2009)

Vlan nativa

La Vlan nativa están asignados a los puertos troncales 802.1Q, son puertos que admiten el tráfico que llegan de diferentes Vlan con un tráfico etiquetado, como también de otras Vlan con tráfico no etiquetado.

Figura 20

Vlan nativa.



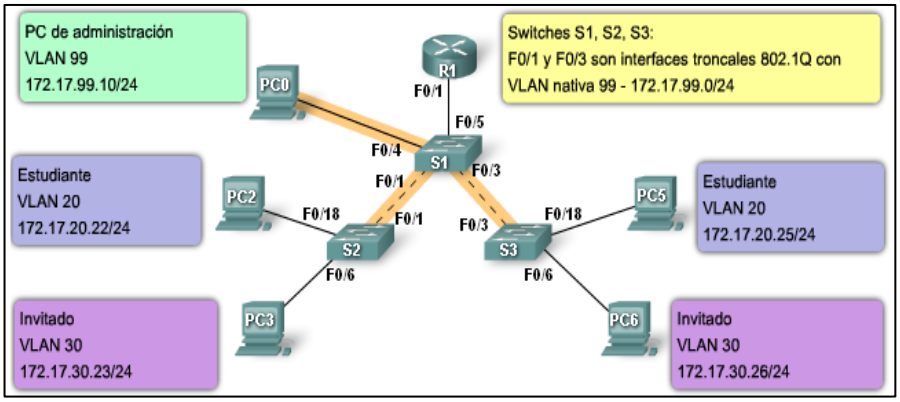
Fuente: (Cisco Networking Academy, 2009)

Vlan de administración

La Vlan de administración puede ser cualquier Vlan que puede ser asignado que tenga la capacidad de ser administrado a los dispositivos de comunicación, por defecto si una Vlan determinada no ha sido asignado como Vlan de administración se puede hacer uso de la Vlan 1, para esto se tendría que asignar una dirección IP seguido de su mascara de subred a la Vlan de administración. (Cisco Networking Academy, 2009).

Figura 21

Vlan de administración.



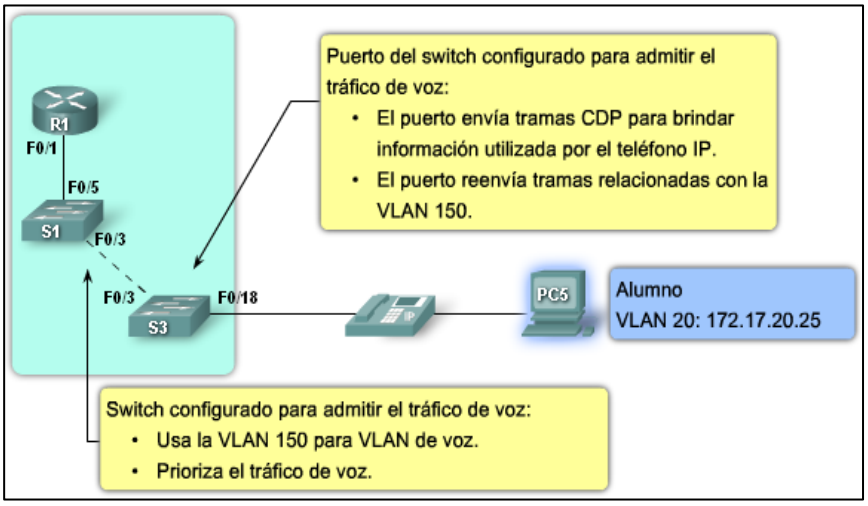
Fuente: (Cisco Networking Academy, 2009)

Vlan de voz

La Vlan de voz es un segmento de red destinada únicamente para el tráfico de voz generada por los usuarios, esta forma de segmentación asegura la calidad del flujo de voz, dando prioridad al momento que se esté generando la comunicación. (Cisco Networking Academy, 2009).

Figura 22

Vlan de voz.



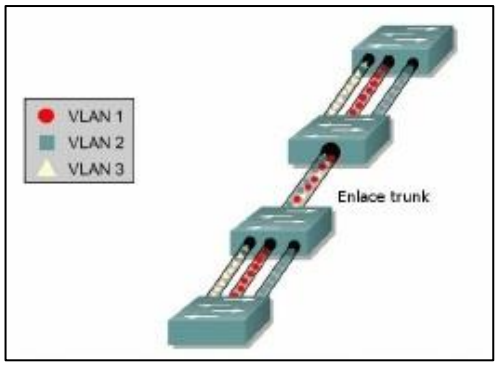
Fuente: (Cisco Networking Academy, 2009)

C. Dispositivos para crear Vlans

a. **Enlace trunk**: Es un enlace entre dos dispositivos que van a soportar diferentes redes virtuales, los enlaces trunk o enlaces troncales son utilizados en conexiones de switch a switch, los dispositivos que admiten Vlan son denominados como VLAN-aware. (Pergandon, 2015).

Figura 23

Enlace troncal.



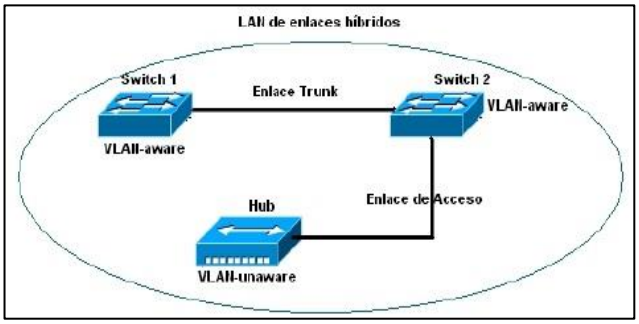
Fuente: (Pergandon, 2015)

b. **Enlace de acceso**: Este tipo de enlace comunica un dispositivo Vlan-aware que son los dispositivos que contienen Vlans, con otro Vlan-unaware que son dispositivos que no admiten Vlans. Los dispositivos finales conectados los puertos del switch son conocidos también como enlaces de acceso. (Pergandon, 2015).

En una red local cuando existen enlaces troncales y enlaces de acceso, también es conocido como enlaces híbridos. (Pergandon, 2015).

Figura 24

Enlaces híbridos.



Fuente: (Pergandon, 2015)

D. Pautas para la configuración de Vlans

Ahora presentamos, los distintos pasos que se realiza al momento de configurar Vlans en una Lan:

1. De acuerdo a su criterio identifique el número de Vlan, recuerde que el primero no se puede utilizar.
2. Según requerimiento identifique los dispositivos finales que integrarán a cada Vlan.
3. según requerimiento identifique que puertos serán usados como enlace troncal.
4. Enlazar de forma física los dispositivos finales e intermediarios a la red.
5. Arrancamos el witch utilizando el cable de consola para realizar las acciones siguientes:
   a. Implementar políticas de seguridad: Creando para usuarios diferentes.
   b. Asignar direcciones IP al switch: Esto va permitir que el administrador acceda de forma remota utilizando Telnet, SSH, etc.)
6. Configurar Vlans en el switch:
   a. Según necesidad podemos ir añadiendo o modificando como también eliminando redes virtuales locales, teniendo presente que si no se crean todos los dispositivos finales e intermediarios estarán conectados la Vlan 1, eso quiere decir que todos los puertos del switch o grupo de switchs pertenecen a la Vlan 1.
   b. Se sabe que todos los puertos de los switchs de la Lan están unidos a la Vlan 1, si se están creando nuevas Vlans, los dispositivos presentes en la Lan se tienen que distribuir a las diferentes Vlans creadas.
   c. Si se pretende comunicar las diferentes redes virtuales creadas, se tiene que hacer uso de un Router, que estará conectado a un puerto troncal del switch.
7. Configurar las redes virtuales en el router:

a. Configurar un puerto del switch como puerto troncal que se enlazará al router.
b. Según la cantidad de redes virtuales creadas, se crean subinterfaces en el router una para cada Vlan, que serán puertos lógicos por donde se conectarán las distintas Vlans.

8. Configurando los dispositivos que pertenecen a cada Vlan:
   a. Dirección IP. La dirección IP debe pertenecer a la subred que la dirección IP de la puerta de enlace que fue creado como subinterfaz en el router.
   b. La máscara de subred.
   c. La puerta de enlace debe ser el mismo que la subinterfaz en el router.

E. **Comprobando la configuración de las Vlan:**

- Dos dispositivos como PCs conectados a una misma Vlan, si hacemos ping deben responder de manera satisfactoria.

2.2.5. Elementos del Cableado Estructurado

Según, **Stallings W.** (2004), El cableado estructurado es una infraestructura de medio físico que puede brindar comunicación en un área limitada, está compuesto por elementos pasivos que cumplen con ciertas características, como transparencia de la aplicación, vida útil larga y flexible y soporte para el cambio y crecimiento en el futuro. Asimismo, debe cumplir con ciertas normas o regulaciones locales e internacionales.

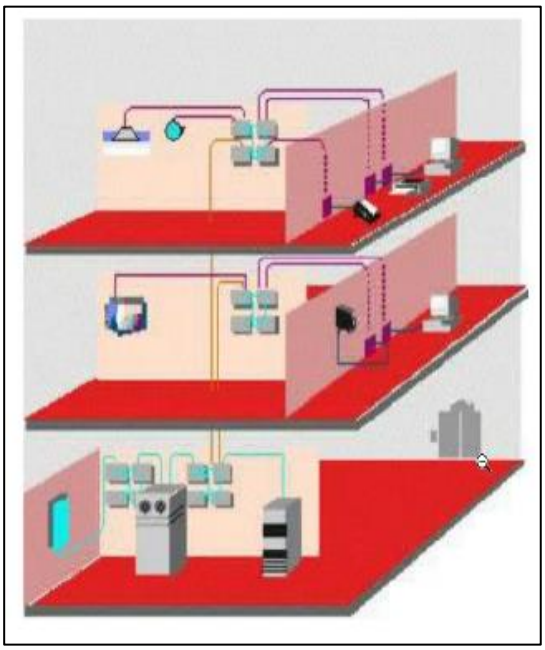
Guía de construcción: Un sistema de cableado estructurado completo se puede dividir en subsistemas independientes, cada subsistema proporciona modularidad y flexibilidad, lo que permite cambios y reubicación. Los diferentes tipos de conexiones, nuevas aplicaciones o nuevas configuraciones estándar varían según la solución seleccionada y los productos instalados.

Elija la configuración de la conexión de red según el tipo de conexión, la distancia entre puntos, el tipo de cable que se utilizará, la cantidad de dispositivos y otras consideraciones para este tipo.

A veces, se utiliza una combinación de configuraciones cuando las condiciones necesarias de diseño y construcción lo permiten, debido a costos, adiciones y otras condiciones de la red que no se consideraron al principio, o debido a consideraciones del cliente o errores en el diseño profesional.

Figura 25

Conexión de Cableado Estructurado.

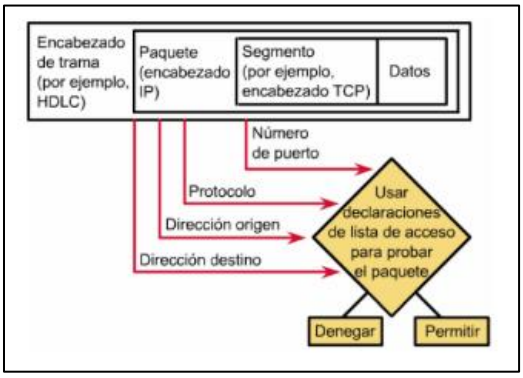


2.2.6. Listas de Control De Acceso (ACL)

Según, **Molina F.** (2006). ACL es una lista de comandos aplicables a las interfaces del enrutador. Estas listas le dicen al enrutador qué tipos de paquetes aceptar y qué tipos de paquetes rechazar. La aceptación y el rechazo pueden basarse en determinadas especificaciones, como la dirección de origen, la dirección de destino y el número de puerto. Cualquier tráfico que pase a través de la interfaz debe cumplir con ciertas condiciones como parte de la ACL. Se pueden crear ACL para todos los protocolos de red de enrutamiento (como IP e IPX) para filtrar los paquetes de datos a medida que pasan por el enrutador.

Figura 26

ACL.



a) Funcionamiento de las ACLs

ACL es un conjunto de declaraciones que se utilizan para definir paquetes:

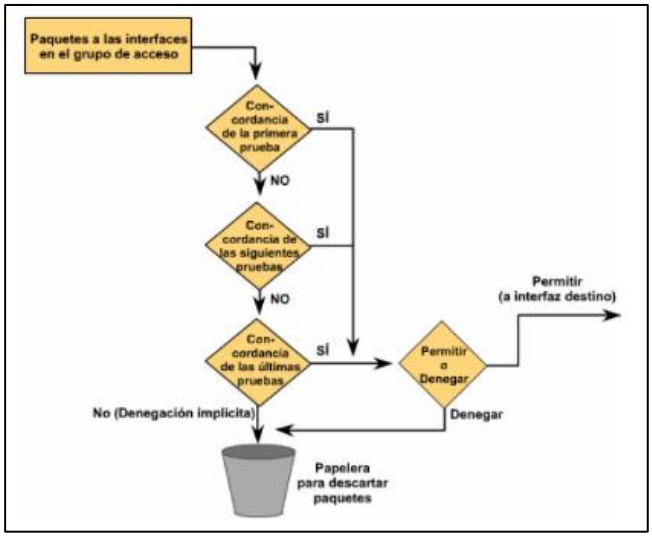
- Ingrese a la interfaz de entrada
- Se reenvían a través del enrutador
- Salen de la interfaz de salida del enrutador.

No importa si se usa ACL o no, el principio del proceso de comunicación es el mismo. Cuando un paquete de datos ingresa a la interfaz, el enrutador verifica si el paquete de datos es enrutable o puenteado. Ahora el enrutador verifica si la interfaz entrante tiene una ACL. Si existe, verifique que el paquete cumpla con las condiciones de la lista. Si se permite el paquete, se compara con la entrada de la tabla de enrutamiento para determinar la interfaz de destino. Luego, el enrutador verificará si la interfaz de destino tiene una ACL. De lo contrario, puede enviar el paquete de datos directamente a la interfaz de destino.

Las sentencias de ACL se ejecutan en orden lógico. Si se cumple una determinada condición, el paquete se permite o deniega y las declaraciones de ACL restantes no se verifican. Si la declaración de ACL no se valida, se aplica una declaración implícita "denegar cualquier". Esto significa que, aunque la declaración "denegar cualquier" no se ve claramente en la última línea de la ACL, sí existe.

Figura 27

Diagrama de Flujo de una ACL.



2.2.7. Metodología de Diseño de Redes

Metodología Top-Down Network Design

De acuerdo a (Oppenheimer, Top-Down Network Design Third Edition, 2011) esta metodología se basa en un diseño "top-down", haciendo referencia al modelo OSI, se parte del nivel superior y pasa al nivel inferior del modelo anterior.

Este método se enfoca en la red empresarial, comenzando desde la capa de aplicación, capa de presentación, capa de sesión y capa de transporte, y luego en las capas inferiores (red, enlace de datos, capa física), porque el siguiente contenido se analiza en estas capas: el estado actual de la red, la demanda, la imitación y su estructura lógica que se deben tener en cuenta a la hora de desarrollar la metodología.

El método se despliega en cuatro etapas bien estructuradas, describiendo los pasos a seguir en el diseño e implementación de la red, y se da su ciclo de ejecución. Estas etapas son:

- Fase I: Análisis de requerimientos
- Fase II: Diseño Lógico de red
- Fase III: Diseño Físico de red
- Fase IV: Probar, Optimizar y Documentar el diseño de la red

Fase I: Análisis de Requerimientos

Esta etapa se enfoca en analizar las metas propuestas por la empresa: requisitos, metas y restricciones. Para obtener esta información se utiliza como fuente de consulta a las personas que trabajan en la empresa y sus usuarios. En cuanto a la red, su infraestructura debe ser analizada y descrita a nivel lógico y físico, para comprender claramente el área a intervenir. (Oppenheimer, Identificación de necesidades de los clientes y metas, 2011).

Fase II: Diseño Lógico de Red

En esta fase se cubre el diseño de topología de red que se desea implementar o mejorar dentro de su empresa, además se especifica el direccionamiento lógico que se implementará en la nueva red, ya sea IPv4, IPv6 o la coexistencia de los dos protocolos. Analice y seleccione los protocolos de conmutación y enrutamiento que utilizarán los dispositivos de red para comunicarse. Esta fase también incluye planes de seguridad y mecanismos de gestión y mantenimiento de redes. (Oppenheimer, Diseño Lógico de Red, 2011).

Fase III: Diseño Físico de Red

Esta etapa se centra en la selección de equipos y tecnología para que se pueda implementar el diseño lógico propuesto. Para seleccionar el equipo correcto, se deben comparar los diferentes equipos y marcas en el mercado, en función de su rendimiento, seguridad, escalabilidad y los factores económicos más importantes. (Oppenheimer, Diseño Físico de Red, 2011).

Fase IV: Probar, Optimizar y Documentar el Diseño de Red

En esta etapa, la red se prueba mediante la implementación de pilotos. Esto se hace para monitorear su rendimiento, disponibilidad y uso de ancho de banda. A partir de los datos obtenidos, sacar conclusiones sobre el funcionamiento de la red para proponer estrategias de optimización.

En esta etapa también se desarrolla la documentación de diseño, lo que significa compilar todas las configuraciones lógicas de la red (direccionamiento, enrutamiento, etc.), así como la identificación del equipo y su cableado estructurado. (Oppenheimer, Probar, Optimizar y Documentar el diseño de Red, 2011).

Metodología de Diseño propuesto por James Mccabe.

Esta metodología fue propuesta por James McCABE en su libro "Practical Computer Network analysis and desing" en el año de 1998. Esta metodología divide el diseño de la red de computadoras en fases y procesos con el fin de realizar cambios futuros sin dañar la estructura.

a) Etapa de diagnóstico

- Una descripción detallada del estado actual de la red.
- Verificar que la infraestructura física y lógica de la red esté documentada y evaluar si cumple con los estándares internacionales.

b) Fase de análisis

- Enumere el área y la cantidad de hosts que posee y describa su funcionamiento.
- Definición de requisitos.
- Definición de la ubicación del host.

c) Fase de diseño

- Diseño físico. - Evaluar y diseñar la estructura física de la red de datos. (La velocidad de megabit soportada por el medio seleccionado, la determinación del dispositivo de comunicación).
- Diseño lógico. - Evaluar y diseñar la infraestructura lógica de la red de datos.

d) Fase de implementación

- Construir y configurar la red según el diseño simulado.

e) Fase de operación

- La red está operativa y monitoreada. Esta etapa es la prueba de diseño máximo.

f) Etapa de optimización

- En esta etapa, los errores se detectan y corrigen.

2.2.8. Seguridad de la Información

2.2.8.1. Definición de la seguridad de la información

Según, **Godoy R.** (2014). La seguridad de la información tiene como objetivo proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizados. La seguridad es un concepto relacionado con la certeza, sin riesgo o contingencia. El estado de cualquier sistema o tipo de información (computadora o no) que indique que el sistema o la información no es peligroso, dañado o riesgoso puede entenderse como seguro. Comprenda todo lo que pueda afectar su funcionamiento directo o los resultados obtenidos como peligro o daño. Al mismo tiempo, cree que la seguridad de la información es un conjunto de medidas preventivas y de respuesta para las organizaciones y los sistemas técnicos que pueden proteger la información, y se esfuerzan por mantener su confidencialidad, disponibilidad e integridad.

Por su lado **Soriano M.** (2014), define el concepto de seguridad de la información como "proteger la información y los sistemas de información del acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados".

Además, la Norma **ISO 27001 (2013**) define que la seguridad de la información puede evitar que la información provenga de diversas amenazas para garantizar la continuidad del negocio, minimizar las pérdidas comerciales y maximizar el retorno de la inversión y las nuevas posibilidades. Asimismo,

considera la existencia de diversas formas de información, por ejemplo; impresa o escrita en papel, recopilada electrónicamente, transmitida electrónicamente, presentada en forma de imagen o expuesta en una conversación. Independientemente de la forma de la información, o la manera en que se distribuya o concentre (almacene), siempre debe estar protegida y asegurada de manera adecuada para mantener la confidencialidad, integridad y disponibilidad, términos que forman la base de la información y el edificio de seguridad de la información.

Figura 28

Sistema de gestión de seguridad de información.

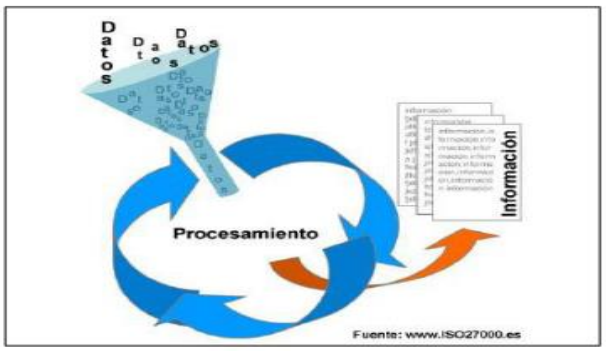


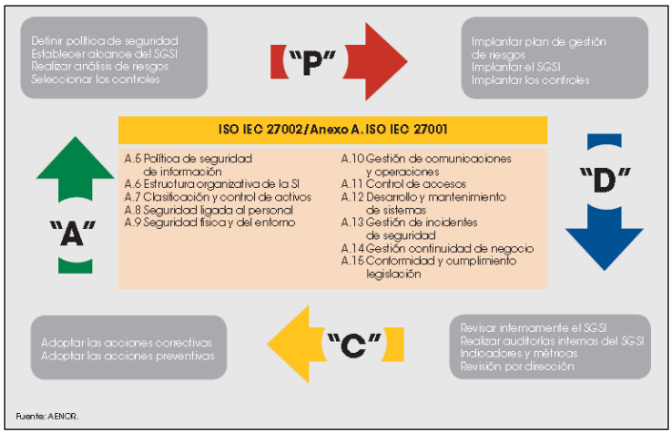
Figura 29

Procedimientos y controles de seguridad basados en una evaluación de riesgo.

Según, **Fernández C.** (2012). La información es tan importante para la organización como lo es el sistema circulatorio de la propia organización. En realidad, las organizaciones se enfrentan actualmente a una gran cantidad de amenazas de diferentes fuentes, incluidas nuevas herramientas comerciales y de TIC (tecnología de la información y la comunicación). El CEO (Directores generales) y el CIO (Directores de informática) deben aplicar a la información como activo principal de cualquier empresa por lo que se debe implementar, mantener y mejorar las medidas de seguridad para lograr sus objetivos comerciales y garantizar que el cumplimiento legal, la reputación y la imagen de la empresa estén protegidos.

Figura 30

Sistema de gestión de la seguridad de la in formación ISO 27001.



2.2.9. Dimensiones de la seguridad de la información

Según, **Godoy R.** (2014), consideró pilares de la Seguridad de la información a las siguientes características.

a) Confidencialidad: para garantizar que solo las personas debidamente autorizadas puedan acceder a la información.

b) Integridad: Esforzarse por mantener la integridad de los datos y evitar modificaciones no autorizadas.

c) Disponibilidad: acceso al sistema e información en el momento requerido por personal autorizado.

Por su parte tambien **Camacho R.** (2008), indicó las siguientes propiedades de la Seguridad de información.

a) Confidencialidad: para asegurar que la información solo pueda ser accedida por aquellos que estén autorizados a acceder a ella.

b) Integridad: para asegurar la exactitud e integridad de la información y los métodos de procesamiento.

c) Disponibilidad: para asegurar que los usuarios autorizados puedan acceder a la información y los recursos relacionados cuando sea necesario.

También considera las siguientes características:

- Autenticidad: Asegúrese de que la información provenga de una fuente real.
- No repudio: para asegurar que el autor de una transacción electrónica no niegue posteriormente que la transacción ha sido ejecutada.
- Identificación: Identificar correctamente a la persona cuando solicita el acceso.
- Control de uso: procedimientos y políticas que restringen el control de uso.
- Auditabilidad: Auditoría a través del historial de eventos (logs).

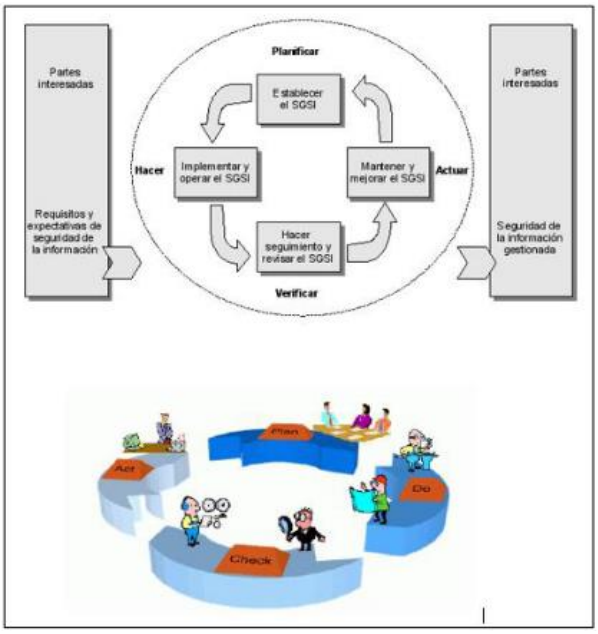
2.2.10. Teorías y modelos de la seguridad de la información

Según la norma **ISO 27001** (2013); se etableció que la información es uno de los activos más importantes de cualquier organización, y necesita ser adecuadamente protegida junto con los procesos y sistemas que la manejan, de amenazas que puedan poner en

peligro la competitividad, rentabilidad y continuidad de los niveles de cumplimiento legal necesarios para alcanzar las metas de la organización. La seguridad de la información consiste en proteger la información a través de un sistema de gestión de seguridad de la información basado en las directrices de buenas prácticas de seguridad de la información UNE-ISO / IEC 27002, para que esté siempre disponible, integrado y distribuido solo al personal autorizado. El modelo en el que se basa el SGSI se denomina modelo PDCA (Planificar-Hacer-Verificar-Actuar).

Figura 31

Modelo PDCA (Plan-Do-Check-Act).

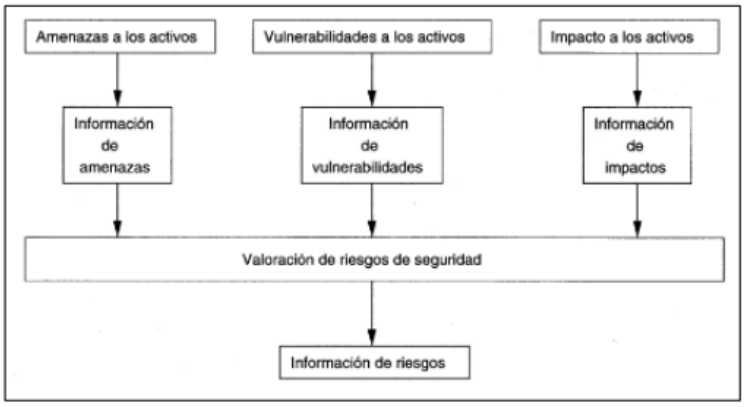


También **Areitio J.** (2008); consideró que todo modelo de seguridad se divide en tres áreas principales, estas áreas trabajan juntas para garantizar que el proceso de seguridad logre sus objetivos.

- Proceso de riesgo: Identificar y priorizar peligros inherentes en el desarrollo de productos, sistemas u organizaciones, ser responsable de identificar y cuantificar la posibilidad de amenazas y establecer niveles de riesgo aceptables para la organización, tomando en cuenta eventos de impacto potencial indeseable.

Figura 32

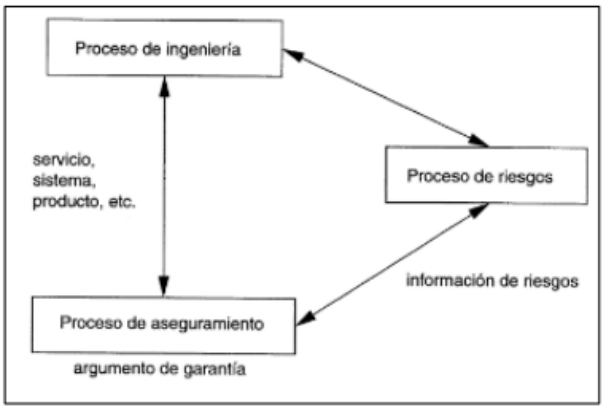
Componentes del proceso de riesgos.



- **Proceso de ingeniería:** Identificar e implementar soluciones a los problemas ocasionados por amenazas y peligros, desde el concepto, diseño, implementación, verificación, despliegue, operación y mantenimiento hasta las diferentes etapas de desarrollo. El equipo de ingenieros de seguridad trabaja con los consumidores (altos directivos, empleados, usuarios, socios comerciales o entidades externas) para determinar todos los requisitos de seguridad.

Figura 33

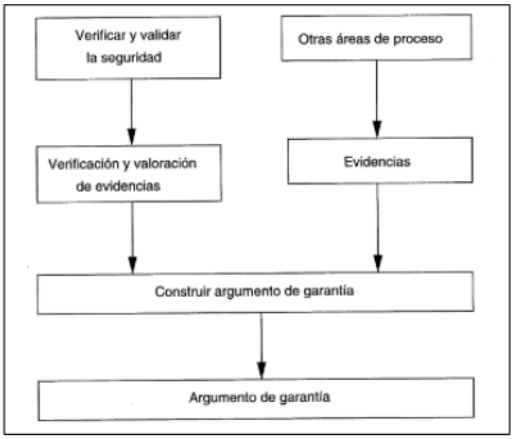
Áreas de proceso de la seguridad de información.



- **Proceso de aseguramiento:** determinar la confianza en que se cumplen los requisitos de seguridad; exactitud, eficiencia, solidez y verificación.

Figura 34

Componentes del proceso de aseguramiento.



- **Servicios de seguridad:** Permiten la implementación de la política de seguridad de la organización que establece computadoras, personal, equipos, etc. en el sistema de información. El propósito es proteger todas las entidades identificables.

Figura 35

Modelo de servicio de seguridad.

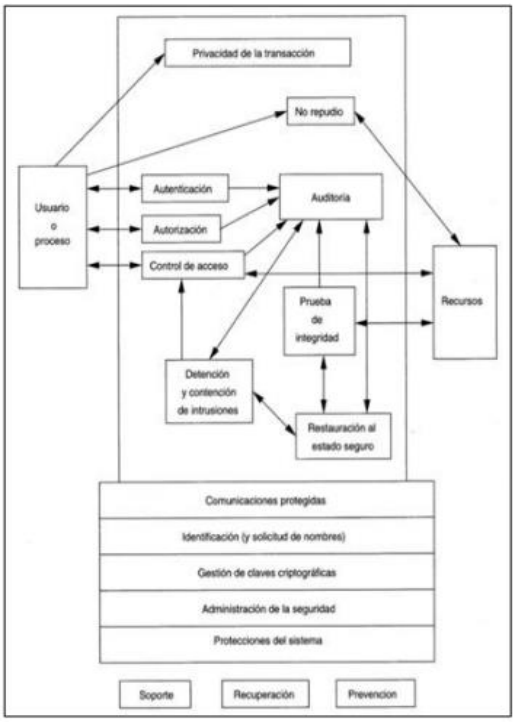


Figura 36

Modelo de servicios de confidencialidad.

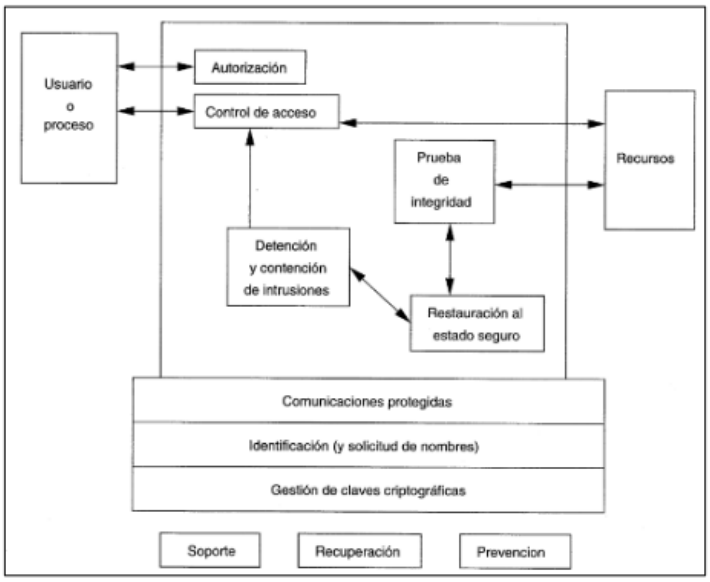


Figura 37

Modelo de servicios de integridad.

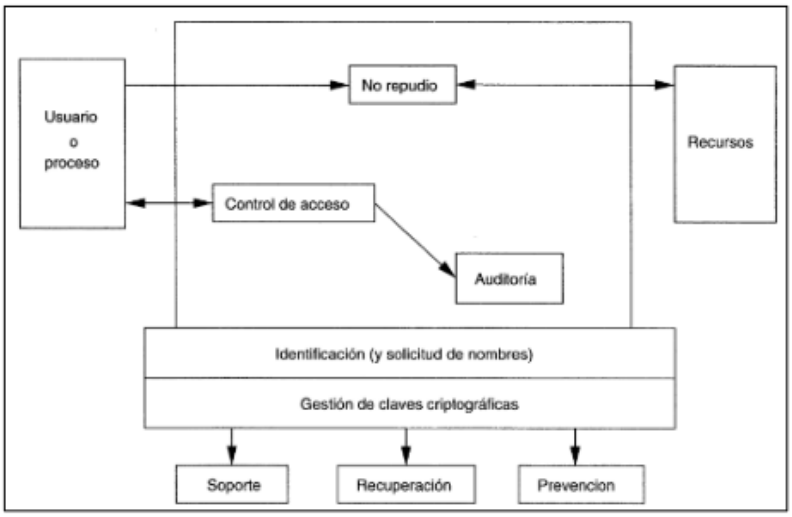
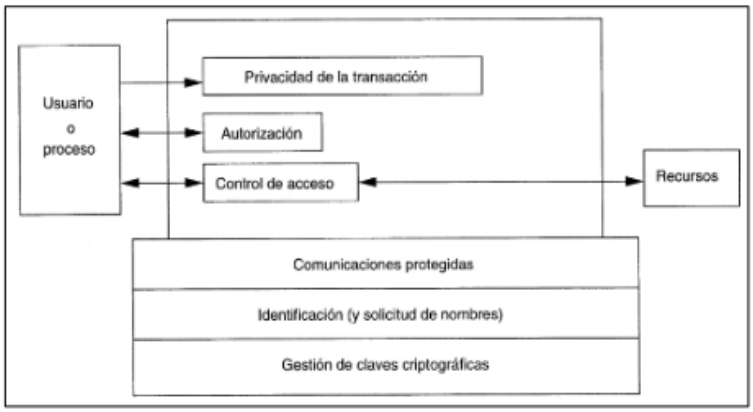


Figura 38

Modelo de servicios de disponibilidad.



Por su parte **Burgos J.** (2008), considera que el modelo PDCA es un estándar ISO formal. Está construido sobre una base que no es necesariamente aplicable a todas las organizaciones, especialmente cuando no están involucradas en el proceso relacionado con el estándar ISO. Por lo tanto, el siguiente es un modelo con una base práctica, que no omite ni restringe las actividades indicadas en el modelo formal, sino que las utiliza para apoyar las formas reales de actividades que deben cubrirse para lograr un nivel suficiente de seguridad de la información en el dominio de las TIC en cualquier tipo de organización.

2.3. Formulación de hipótesis

2.3.1. Hipótesis General

El diseño de infraestructura de red de datos influye significativamente en la seguridad de la información en el Gobierno Local de Paucará.

2.3.2. Hipótesis específicas

a) El diseño de infraestructura de red de datos influye significativamente en la Integridad de la Información en el Gobierno Local de Paucará.

b) El diseño de infraestructura de red de datos influye significativamente en la Disponibilidad de la Información en el Gobierno Local de Paucará.

c) El diseño de infraestructura de red de datos influye significativamente en la Confidencialidad de la Información en el Gobierno Local de Paucará.

2.4. Definición de términos

2.4.1. Información

Según, **Chiavenato I.** (2006) (Idalberto, 2006)La información es: “Es un conjunto de datos significativos, que es para reducir la incertidumbre o aumentar la comprensión de algo”.

2.4.2. Red de Datos

Según, **Behrouz A.** (2007). La red de datos es un sistema compuesto por equipos terminales, equipos intermedios y equipos de conexión de medios, que proporciona una plataforma para la red interpersonal.

2.4.3. Seguridad

Según, **Godoy R.** (2014)**.** El estado de cualquier sistema o tipo de información (computadora o no), que indica que el sistema o la información no es peligroso, dañado o riesgoso

2.4.4. Seguridad de la Información

Según, **Soriano M.** (2014). Cómo proteger la información y los sistemas de información del acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.

2.4.5. Calidad de Servicio (Qos)

Según, **Fontalvo & Vergara** (2010). La calidad de los bienes o servicios, como un conjunto de factores internos para satisfacer las necesidades de los usuarios (clientes), y que es como la "aplicabilidad" de los productos o servicios, que se caracteriza por brindarles la capacidad a los clientes para satisfacer sus necesidades.

2.4.6. Disponibilidad

Según, **Camacho R.** (2008). Asegúrese de que los usuarios autorizados puedan acceder a la información y los recursos relacionados cuando sea necesario.

2.4.7. Integridad

Según, **Godoy R.** (2014). Se esfuerza por mantener la integridad de los datos y evitar modificaciones no autorizadas.

2.4.8. Confidencialidad

Según, **Camacho R. (2008).** Asegurarse de que solo las personas autorizadas a acceder a ella puedan acceder a la información.

2.5. Identificación de variables

2.5.1. Variable Independiente

Infraestructura de red de datos: Según **Behrouz A.** (2007) Son sistemas compuestos por equipos terminales, equipos intermedios y medios que conectan los equipos y proporcionan una plataforma para redes humanas.

La infraestructura de la red de datos respalda la forma en que vivimos, estudiamos, trabajamos y jugamos. Proporcionan una plataforma de servicio que nos permite conectarnos con familiares y amigos y con nuestro trabajo e intereses a nivel local y global. Esta plataforma admite el uso de texto, gráficos, video y voz.

2.5.2. Variable Dependiente

Seguridad de la Información: Con respecto a ello **Godoy R.** (2014) menciona que la seguridad de la información tiene como objetivo proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizados; la seguridad es un concepto relacionado con la certeza, libre de riesgos o contingencia; la seguridad puede entenderse como cualquier sistema o tipo de información (Computadora o no) estado, que indica que el sistema o la información no es peligrosa, dañada o peligrosa. Se

entiende como un peligro o destrucción de todo aquello que pueda afectar su funcionamiento directo o los resultados obtenidos. También menciona que es un conjunto de medidas preventivas y de respuesta para las organizaciones y sistemas técnicos que pueden proteger la información buscando la confidencialidad, disponibilidad e integridad.

2.6. Operacionalización de variables

Tabla 1

Operacionalización de variables

VARIABLE INDEPENDIENTE	DIMENSIÓN	INDICADORES
X: Infraestructura de red de datos	X1: Tolerancia a fallas	• N° de enlaces redundancia de datos a nivel LAN • N° de diversidad de datos a nivel LAN
	X2: Escalabilidad	• N° de sub redes a nivel LAN • N° de equipos conectados a la red LAN
	X3: Calidad de Servicio (QoS)	• N° de servicios ofrecidos por la red. • Tiempos de respuesta de las aplicaciones a nivel LAN.
VARIABLE DEPENDIENTE	**DIMENSIÓN**	**INDICADORES**
Y: Seguridad de la Información	Y1: Disponibilidad de la Información	• Tiempos de respuesta de las aplicaciones informáticas a nivel LAN. • Velocidad de carga y descarga
	Y2: Integridad de la Información	• % de accesos a servicios no autorizados a nivel LAN.
	Y3: Confidencialidad de la Información	• %de usuarios identificados en la red.

Fuente: Elaboración propia.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. Tipo de investigación

La presente investigación es aplicada, porque utiliza conocimientos y métodos establecidos para analizar y explicar los fenómenos de seguridad de la información que ocurren en el Gobierno Local de Paucará.

A esto **Murillo W.** (2008) menciona que la investigación aplicada se denomina "investigación práctica o empírica", y su característica es buscar la aplicación o uso de los conocimientos adquiridos después de la implementación y práctica de la investigación sistemática, mientras se obtienen otros conocimientos.

3.2. Nivel de investigación

La investigación es explicativa, responsable de encontrar las causas de los hechos mediante el establecimiento de relaciones causales y la obtención de resultados mediante la prueba de hipótesis.

Según, **Hernández, Fernández & Baptista** (2006), mencionan que "las investigaciones explicativas consideran la manipulación de la variable independiente (VI) que es la causa sobre las variables dependientes (VD) que es el efecto, en una realidad especifica determinada".

3.3. Métodos de investigación

3.3.1. Método General

El método general es el método científico, que nos permite formular y verificar hipótesis a partir del planteamiento del problema en estudio y la construcción teórica en la que se fundamenta.

Según, **Pino G.** (2019). El método científico es un "proceso destinado a explicar fenómenos, establecer relaciones entre los hechos y enunciar leyes que expliquen los fenómenos físicos del mundo y obtener, con estos conocimientos, aplicaciones útiles al hombre".

3.3.2. Método Especifico

Es **Deductivo – Inductivo** donde **Bastar S.** (2012) menciona que:

Método deductivo: Es un proceso racional de general a particular.

Método inductivo: Es un proceso racional de lo individual a lo general. Este método se aplica en procesos de orden intelectual, porque es un procedimiento de sistematización en el que a partir de resultados particulares se buscan las relaciones generales que las expliquen.

3.4. Diseño de investigación

El presente proyecto muestra un diseño experimental de tipo pre-experimental debido a que se realizará una evaluación de la infraestructura de redes actual (pre test) y luego se implementaran redes privadas virtuales para evaluar la seguridad de la información (post test). El esquema es:

GE: 0_1 ------- X -----0_2

Donde:

G.E. Grupo experimental

0_1: Pre Test: La seguridad de la información sin el uso de las Redes Virtuales privadas.

0_2: Post Test: La seguridad de la información con el uso de las Redes Virtuales privadas.

X: Manipulación de variables Independiente (Infraestructura de red de datos)

3.5. Población, muestra y muestreo

3.5.1. Población

La población general con la que trabajamos consiste en cada host conectado a la red actual y el host no conectado.

3.5.2. Muestra

La muestra es de 26 host que se toman del Gobierno Local de Paucará lo cual fue tomada por conveniencia.

3.5.3. Muestreo

En esta investigación, se consideró el muestreo por conveniencia.

3.6. Técnicas e instrumentos de recolección de datos

En el proceso de recolección de información, es necesario adoptar tecnologías que apoyen las necesidades de investigación, para obtener información confiable, directa y fácil de interpretar.

3.6.1. Técnicas de recolección de datos

- **Observación directa:** esta técnica es la que nos ayuda a comprender directamente cómo se manejan las tecnologías de la información y la comunicación (TIC) a nivel del Gobierno Local de Paucará.

  Utilice tablas de observación y listas de verificación para recopilar información antes y después.

  A esto **Hernández, Fernández & Baptista** (2006), expresan que: "la observación directa consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta".

3.6.2. Instrumentos de recolección de datos

- **Ficha de Observación:** En este trabajo, utilizamos registros de observación como herramienta de recopilación porque existen múltiples herramientas y técnicas de recopilación de datos.

3.7. Técnicas de procesamiento y análisis de datos

3.7.1. Técnicas de procesamiento de datos

Para el propósito de esta investigación, las herramientas mencionadas en el anexo se utilizan para el procesamiento de datos. Ingresamos los datos recolectados en un software que permite operaciones estadísticas. En nuestro caso, Microsoft Excel 2019 e IBM SPSS Statistics. Es fácil de operar y tiene la ventaja de obtener información estadística.

3.7.2. Técnicas de análisis de datos

El análisis de datos tiene como objetivo determinar un conjunto de estadísticas o medidas estadísticas, como medidas de tendencia central y medidas de dispersión. En el análisis y discusión de datos se trabajó con la técnica de la triangulación de autores y teorías respectivamente.

3.8. Descripción de la prueba de hipótesis

Como menciona **Oseda D.** (2018) "se ha podido verificar los planteamientos de diversos autores y cada uno de ellos con sus respectivas características y peculiaridades, motivo por el cual era necesario decidir por uno de ellos para ser aplicado en la investigación".

Ahora bien, respecto a la prueba de hipótesis general, se utilizaron el estadígrafo rho de Spearman. Ahora bien, teniendo como referencia a dicho investigador se tiene la siguiente secuencia lógica:

a) Planteamiento de hipótesis estadísticas.

   Hipótesis nula: **Ho**

   Hipótesis alterna: **H1**

b) Nivel de significancia o riesgo, que viene a ser el 5%.
c) Cálculo del estadístico de prueba, que para nuestro caso será la prueba t de Student.
d) Decisión estadística, condicionado por el p-valor.
e) Conclusión estadística, según el error tipo I o error tipo Alfa.

CAPÍTULO IV

DISCUSIÓN DE RESULTADOS

4.1. Presentación de resultados

4.1.1. Diseño de la solución

Para el diseño de la plataforma de red de datos del Gobierno Local de Paucará, se utilizó la metodología Top-Down de Cisco, metodología que nos ofrece cuatro fases, y que para cada fase se hizo un análisis minucioso para tener como resultado la solución al problema.

4.1.1.1. Análisis de los requerimientos

- ***Objetivos institucionales***

  Entre los objetivos instituciones del Gobierno Local de Paucará podemos citar lo siguiente:

  - ✓ Planificar, ejecutar y promover, una serie de medidas necesarias, encaminadas a brindar a la población un clima socioeconómico y cultural apropiados para brindar una buena atención a las necesidades primordiales en lo que respecta a vivienda, salud, seguridad, educación entre otros, dando prioridad los gastos con total transparencia, fomentando actividades, proyectos, todo ello enmarcado en el presupuesto de la institución.
  - ✓ Impulsar la cooperación comprometida de la ciudadanía del pueblo de Paucará en la administración municipal, promoviendo el trabajo comunitario en beneficio de la sociedad.

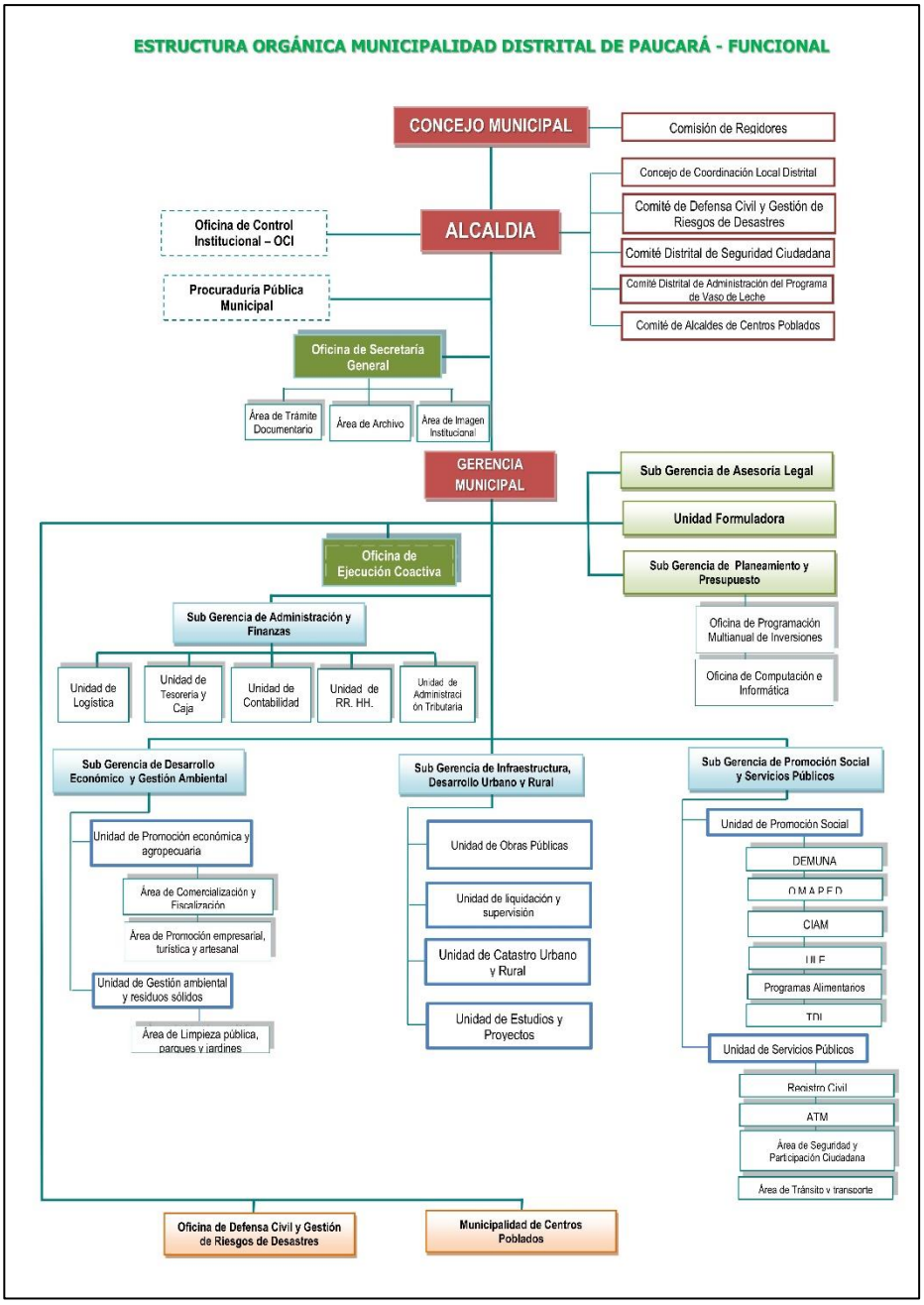
- ✓ Asegurar la asistencia de los servicios de la institución hacia la población, a través de los sofisticados métodos de trabajo, con el propósito de alcanzar los mejores estándares de calidad.

Organigrama de la municipalidad

Es vital conocer la organización del Gobierno Local de Paucará, para de esa manera visualizar la distribución para luego segmentar la cantidad de usuarios, así como el tráfico de datos.

Figura 39

Organigrama del Gobierno Local de Paucará.



Fuente: ROF del Gobierno local de Paucará.

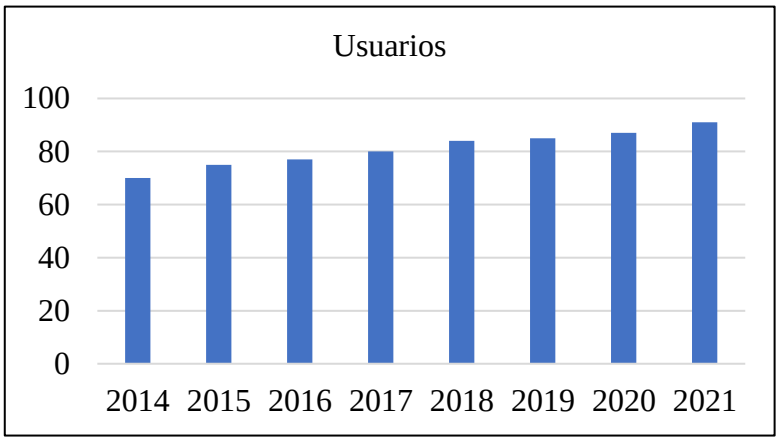
Evolución de la organización

La plataforma de red del Gobierno Local de Paucará inicio su funcionamiento en los años 2004, solo para acceso a Internet, y la cantidad de empleados era reducido, luego se fueron implementando

más áreas y con el avance de las nuevas tecnologías, y la utilización de aplicativos de gestión pública, desde el año 2010 hasta la actualidad se ha ido ampliando la red con dispositivos de comunicación, servidores, y dispositivos terminales, y que actualmente se cuenta con 91 terminales.

Figura 40

Crecimiento de usuarios de la red LAN.



Fuente: Elaboración propia.

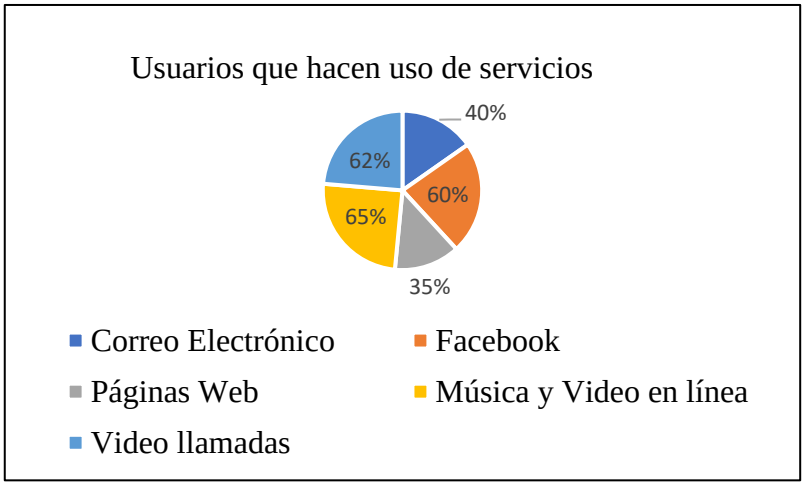
- ***Objetivos técnicos***

Los servicios que brinda actualmente la plataforma de red, me permiten establecer una segmentación, en función a los servicios o aplicaciones que hacen uso durante el día.

Los aplicativos que hacen mayor uso son los softwares de gestión como SIAF, SIGA; también hace uso de aplicativos como son videos en línea, música en línea, video llamadas, esto hace que la plataforma del Gobierno Local de Paucará tenga un uso exagerado de la red, también el personal que labora en la Municipalidad hace un uso exagerado de correo electrónico, redes sociales y acceso a portales web.

Figura 41

Usuarios que hacen uso de servicios.



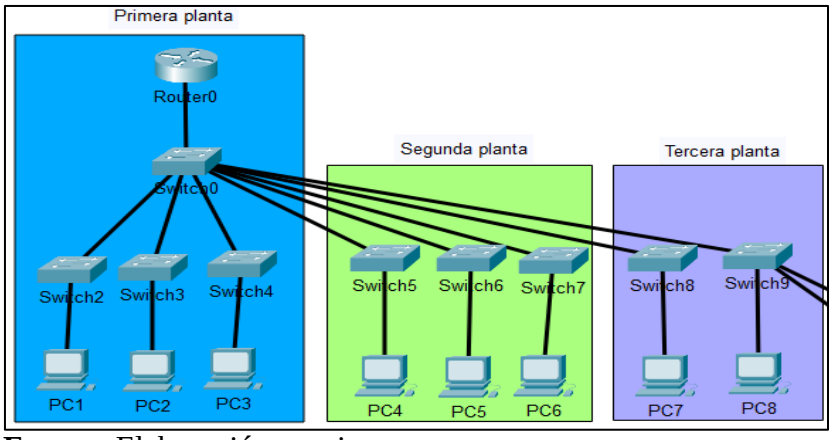
Fuente: Elaboración propia.

- ***Analizando la red Existente***

La plataforma actual del Gobierno Local de Paucará está formado por un Router para el Acceso al Servicio de internet, este está conectado a un Switch que sirve de concentración de ocho Switchs distribuidos para atender a las diferentes áreas de la entidad, esto Switch son equipos de acceso para los dispositivos terminales, todo esto en una mismo edificio de cuatro plantas y es aquí donde se genera la mayor cantidad de tráfico, accediendo a los servicios y aplicaciones teniendo y mayor consumo de la red.

Figura 42

Red existente.



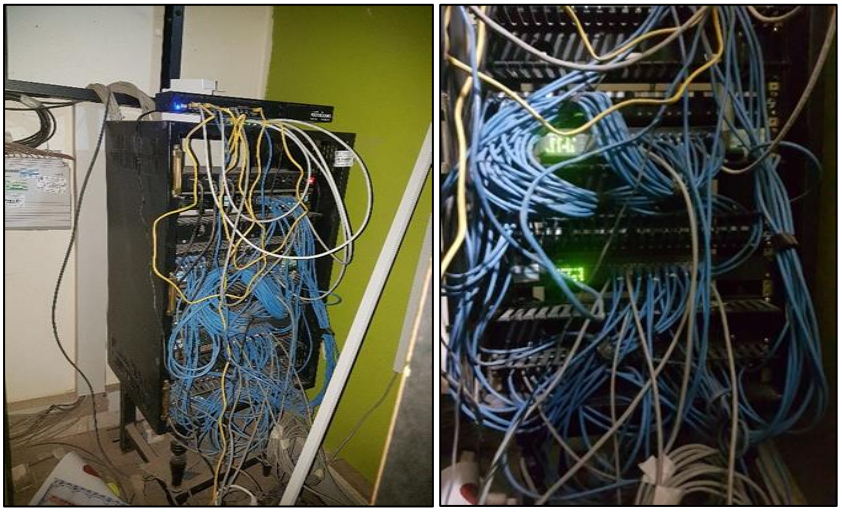
Fuente: Elaboración propia.

Resultado del diagnóstico Físico

En cuanto al cableado estructurado, se observa que no está diseñado de acuerdo a normas establecidas, los cables están tendidos de manera artesanal y no es el adecuado, y podemos observar que su distribución no cuenta con una instalación de manera correcta, en algunos casos no se cuenta con canaletas y en algunos casos si cuentan con ductos, para la instalación de los equipos de comunicación, se adecuo un sitio y es el lugar donde se encuentran en este momento los equipos, los equipos de comunicación en algunos casos no se encuentran en gabinetes.

Figura 43

Cableado de la red.



Fuente: Elaboración propia.

Los equipos con que cuenta actualmente del Gobierno Local de Paucara podemos visualizar en la siguiente tabla, con algunas características como la cantidad de puertos, su velocidad, cantidad, y si son equipos administrables.

Tabla 2

Equipos de comunicación con que cuenta el Gobierno Local de Paucará

Equipos	Cantidad	Administrable
Router: BOARD RB3011UIAS-RM	**1**	**No**
Switch: GIGABIT L2 TP-LINK T2600G-28TS 24 PUERTOS 10/100/1000	**9**	**No**

Fuente: Elaboración propia.

4.1.1.2. Desarrollo del diseño lógico

En esta fase se ha analizado la cantidad de toma datas para los equipos terminales con que cuenta el Gobierno Local de Paucara, que cuenta con 25 áreas u oficinas, con 91 toma datas para los dispositivos finales, lo que se pretende es que cada Área u oficina sea una red independiente.

Tabla 3

Total de equipos por Áreas u Oficinas del Gobierno Local de Paucará.

N°	Áreas/Oficinas	Laptop	Comp.	Tota_Host
1	Alcaldía	1	2	3
2	Oficina de Secretaria General	3	4	7
3	Oficina de Imagen Institucional	1	1	2
4	Gerencia Municipal	4	1	5
5	Sub Gerencia de Asesoría Legal	3	1	4
6	Sub Gerencia de Planeamiento y Presupuesto	4	2	6
7	Sub Gerencia de Administración y Finanzas	2	1	3
8	Unidad de Logística	3	2	5
9	Oficina de Patrimonio	1	2	3
10	Unidad de Tesorería	2	2	4
11	Unidad de Contabilidad	2	1	3
12	Unidad de Recursos Humanos	1	1	2
13	Unidad de Administración Tributaria		1	1

14	Sub Gerencia de Infraestructura, Urbano y Rural	2	1	3
15	Unidad de Obras Publicas	2	0	2
16	Unidad de Liquidación y Supervisión	2	3	5
17	Unidad de Catastro Urbano y Rural	1	1	2
18	Unidad de Estudios y Proyectos	1	2	3
19	Sub Gerencia de Desarrollo Social y Servicio Institucional	3	1	4
20	Secretaria de GDSSI	3	0	3
21	ULE SISFOH	3	1	4
22	PVL	1	2	3
23	Unidad Promoción Social	3	4	7
24	Sub Gerencia de Desarrollo Económico, Productivo y Medio Ambiente	4	1	5
25	Unidad de Gestión Ambiental y Residuos Sólidos	2	0	2
	TOTAL			**91**

Fuente: Elaboración propia.

Direccionamiento IP

Dependiendo de los aplicativos que hacen uso las oficinas y o áreas y la información que comparten, se han agrupado tal como se muestra en la siguiente tabla áreas u oficinas, llegándose a tener 5 grupos las que harán las respectivas redes virtuales que serán identificadas con un nombre de grupo y un identificador.

Tabla 4

Distribución de las Áreas u Oficinas en las diferentes redes virtuales.

Áreas/Oficinas	N° de Host	Ubicación	Nombre de Vlan	N° de host por Vlan
Alcaldía	3	Piso 3	Alcaldia	16
Oficina de secretaria general	7	Piso 3		
Oficina de Imagen Institucional	2	Piso 1		
Sub Gerencia de Asesoría Legal	4	Piso 2		
Gerencia Municipal	5	Piso 3	G_Municipal	32
Sub Gerencia de Planeamiento y Presupuesto	6	Piso 2		

Sub Gerencia de Administración y Finanzas	3	Piso 3		
Unidad de Logística	5	Piso 2		
Oficina de Patrimonio	3	Piso 2		
Unidad de Tesorería	4	Piso 2		
Unidad de Contabilidad	3	Piso 2		
Unidad de Recursos Humanos	2	Piso 1		
Unidad de Administración Tributaria	1	Piso 1		
Sub Gerencia de Infraestructura, Urbano y Rural	3	Piso 3		
Unidad de Obras Publicas	2	Piso 3		
Unidad de Liquidación y Supervisión	5	Piso 3	SG_y_Unidades	15
Unidad de Catastro Urbano y Rural	2	Piso 3		
Unidad de Estudios y Proyectos	3	Piso 3		
Sub Gerencia de Desarrollo Social y Servicio Institucional	4	Piso 2		
Secretaria de GDSSI	3	Piso 2		
ULE SISFOH	4	Piso 1	SGD_Social	21
PVL	3	Piso 1		
Unidad Promoción Social	7	Piso 2		
Sub Gerencia de Desarrollo Económico, Productivo y Medio Ambiente	5	Piso 2	SGD_Economico	7
Unidad de Gestión Ambiental y Residuos Sólidos	2	PISO 2		

Fuente: Elaboración propia.

Para el direccionamiento IP se está utilizando la dirección privada 192.168.20.0 con máscara de subred 255.255.255.0, con lo que disponemos de 254 direcciones IP para los dispositivos finales, pero como se tiene 25 áreas u oficinas contenidos en 5 grupos, eso quiere decir que de esta dirección IP se ha tenido que segmentar como mínimo en 5 subredes, para ello se ha utilizado VLSM (Máscara de subred de longitud variable), esto para tener una mejor administración de las direcciones IP. Como podemos visualizar en la tabla, todas las subredes no son redes con mascará de longitud fija.

Tabla 5

Generación de subredes de la red 192.168.20.0/24.

Red	Rango de Host	Broadcast
192.168.20.0/26	192.168.20.1 - 192.168.20.62	192.168.20.63
192.168.20.64/27	192.168.20.65 - 192.168.20.94	192.168.20.95
192.168.20.96/27	192.168.20.97 - 192.168.20.126	192.168.20.127
192.168.20.128/27	192.168.20.129 - 192.168.20.158	192.168.20.159
92.168.20.160/28	192.168.20.161 - 192.168.20.174	192.168.20.175
192.168.20.176/28	192.168.20.177 - 192.168.20.190	192.168.20.191
192.168.20.192/28	192.168.20.193 - 192.168.20.206	192.168.20.207
192.168.20.208/28	192.168.20.209 - 192.168.20.222	192.168.20.223
192.168.20.224/28	192.168.20.225 - 192.168.20.238	192.168.20.239
192.168.20.240/28	192.168.20.241 - 192.168.20.254	192.168.20.255

Fuente: Elaboración propia.

Para el diseño lógico, y dar solución a los problemas encontrados en la infraestructura del Gobierno Local de Paucará, se ha implementado redes locales virtuales más conocidos como Vlan, donde cada subred pertenece una Vlan en específico, para la asignación del identificador, se ha ordenado de forma descendente en función a la cantidad de Host por sub red.

Tabla 6

Asignación de nombres a las Redes virtuales

Áreas/Oficinas	N° de Host	Ubicación	Nombre de Vlan	Nombre de Vlan	N° de host por Vlan
Gerencia Municipal	5	Piso 3	Vlan 2	G_Municipal	32
Sub Gerencia de Planeamiento y Presupuesto	6	Piso 2			
Sub Gerencia de Administración y Finanzas	3	Piso 3			
Unidad de Logística	5	Piso 2			
Oficina de Patrimonio	3	Piso 2			
Unidad de Tesorería	4	Piso 2			
Unidad de Contabilidad	3	Piso 2			
Unidad de Recursos Humanos	2	Piso 1			

Unidad de Administración Tributaria	1	Piso 1			
Sub Gerencia de Desarrollo Social y Servicio Institucional	4	Piso 2	Vlan 3	SGD_Social	21
Secretaria de GDSSI	3	Piso 2			
ULE SISFOH	4	Piso 1			
PVL	3	Piso 1			
Unidad Promoción Social	7	Piso 2			
Alcaldía	3	Piso 3	Vlan 4	Alcaldia	16
Oficina de Secretaria General	7	Piso 3			
Oficina de Imagen Institucional	2	Piso 1			
Sub Gerencia de Asesoría Legal	4	Piso 2			
Sub Gerencia de Infraestructura, Urbano y Rural	3	Piso 3	Vlan 5	SG_y_Unidades	15
Unidad de Obras Publicas	2	Piso 3			
Unidad de Liquidación y Supervisión	5	Piso 3			
Unidad de Catastro Urbano y Rural	2	Piso 3			
Unidad de Estudios y Proyectos	3	Piso 3			
Sub Gerencia de Desarrollo Económico, Productivo y Medio Ambiente	5	Piso 2	Vlan 6	SGD_Economico	7
Unidad de Gestión Ambiental y Residuos Sólidos	2	Piso 2			

Fuente: Elaboración propia.

Asignando los números IPs a las respectivas Redes virtuales locales

Para asignar los números IPs a las redes virtuales locales, se ha utilizado una red privada de clase C la 192.168.20.0/24, teniendo esta red, se ha generado sub red utilizando máscaras de longitud variable, esto con el fin de sacar el máximo provecho de los números IPs, y observando que la cantidad de host con que cuenta cada área u oficina no es el mismo para todos, para asignar el identificador de Vlan para cada grupo se ha ordenado de forma descendente en función a la cantidad de Host por cada red virtual.

Tabla 7

Asignación de dirección de red a las Vlans.

N° de Vlan	Nombre de Vlan	N° de Host	Máximo de Host	Red	Rango de Host	Broadcast
Vlan 2	G_Municipal	32	62	192.168.20.0/26	192.168.20.1 - 192.168.20.62	192.168.20.63
Vlan 3	SGD_Social	21	30	192.168.20.64/27	192.168.20.65- 192.168.20.94	192.168.20.95
Vlan 4	Alcaldia	16	30	192.168.20.96/27	192.168.20.97- 192.168.20.126	192.168.20.127
Vlan 5	SG_y_Unidades	15	30	192.168.20.128/27	192.168.20.129- 192.168.20.158	192.168.20.159
Vlan 6	C_Computo	10	14	92.168.20.160/28	192.168.20.161- 192.168.20.174	192.168.20.175
Vlan 7	Camaras	10	14	192.168.20.176/28	192.168.20.177- 192.168.20.190	192.168.20.191
Vlan 8	SGD_Economico	7	14	192.168.20.192/28	192.168.20.193- 192.168.20.206	192.168.20.207
Vlan 9	Servidores	7	14	192.168.20.208/28	192.168.20.209- 192.168.20.222	192.168.20.223
Vlan 10	Libre		14	192.168.20.224/28	192.168.20.22- 192.168.20.238	192.168.20.239
Vlan 11	Libre		14	192.168.20.240/28	192.168.20.241- 192.168.20.254	192.168.20.255

Fuente: Elaboración propia.

Distribución de Número IPs a cada Área u Oficina

En forma secuencial se está asignando el identificador de la red virtual iniciando en 2, el primero no se está utilizando, esto debido que es una red virtual definida, se han agregado 3 subredes más, Centro de Cómputo que será el que administra la infraestructura de red, la sub red Servidores y la Sub red para las Cámaras Web, y se tiene 2 sub redes libres.

Tabla 8

Distribución de números IPs a las diferentes Áreas u Oficinas.

Áreas/Oficinas	N° de Host	N° max. De Host	Rango de Ips	Ubicación	Nombre de Vlan	Nombre de Vlan	Host por Vlan	Max. Host por Vlan	Puerta de Enlace	Rango de Ips para terminales Vlan	Máscara de subred
Gerencia Municipal	5	10	192.168.20.2 - 192.168.20.11	Piso 3	Vlan 2	G_Municipal					
Sub Gerencia de Planeamiento y Presupuesto	6	10	192.168.20.12 - 192.168.20.21	Piso 2	Vlan 2	G_Municipal					
Sub Gerencia de Administración y Finanzas	3	6	192.168.20.22 - 192.168.20.27	Piso 3	Vlan 2	G_Municipal	32	61	192.168.20.1	192.168.20.2 - 192.168.20.62	255.255.255.192
Unidad de Logística	5	10	192.168.20.28 - 192.168.20.37	Piso 2	Vlan 2	G_Municipal					
Oficina de Patrimonio	3	5	192.168.20.38 - 192.168.20.42	Piso 2	Vlan 2	G_Municipal					
Unidad de Tesorería	4	7	192.168.20.43 - 192.168.20.49	Piso 2	Vlan 2	G_Municipal					
Unidad de Contabilidad	3	6	192.168.20.50 - 192.168.20.55	PISO 2	Vlan 2	G_Municipal					

Unidad de Recursos Humanos	2	4	192.168.20.56 - 192.168.20.59	PISO 1	Vlan 2	G_Municipal					
Unidad de Administración Tributaria	1	3	192.168.20.60 - 192.168.20.62	PISO 1	Vlan 2	G_Municipal					
Sub Gerencia de Desarrollo Social y Servicio Institucional	4	6	192.168.20.66 - 192.168.20.71	PISO 2	Vlan 3	SGD_Social					
Secretaria de GDSSI	3	4	192.168.20.72 - 192.168.20.75	Piso 2	Vlan 3	SGD_Social	21	29	192.168.20.65	192.168.20.66 - 192.168.20.94	255.255.255.224
ULE SISFOH	4	6	192.168.20.76 - 192.168.20.81	Piso 1	Vlan 3	SGD_Social					
PVL	3	4	192.168.20.82 - 192.168.20.85	Piso 1	Vlan 3	SGD_Social					
Unidad Promoción Social	7	9	192.168.20.86 - 192.168.20.94	Piso 2	Vlan 3	SGD_Social					
Alcaldía	3	6	192.168.20.98 - 192.168.20.103	Piso 3	Vlan 4	Alcaldia					
Oficina de Secretaria General	7	11	192.168.20.104 - 192.168.20.114	Piso 3	Vlan 4	Alcaldia					
Oficina de Imagen Institucional	2	4	192.168.20.115 - 192.168.20.118	Piso 1	Vlan 4	Alcaldia	19	29	192.168.20.97	192.168.20.98 - 192.168.20.126	255.255.255.224
Sub Gerencia de Asesoría Legal	4	8	192.168.20.119 - 192.168.20.126	Piso 2	Vlan 4	Alcaldia					
Sub Gerencia de Infraest., Urbano y Rural	3	6	192.168.20.130 - 192.168.20.135	Piso 3	Vlan 5	SG_y_Unidades	15	29	192.168.20.129	192.168.20.130 - 192.168.20.158	255.255.255.224

Unidad de Obras Publicas	2	4	192.168.20.136 - 192.168.20.139	Piso 3	Vlan 5	SG_y_Unidades					
Unidad de Liquidación y Supervisión	5	9	192.168.20.140 - 192.168.20.148	Piso 3	Vlan 5	SG_y_Unidades					
Unidad de Catastro Urbano y Rural	2	4	192.168.20.149 - 192.168.20.152	Piso 3	Vlan 5	SG_y_Unidades					
Unidad de Estudios y Proyectos	3	6	192.168.20.153 - 192.168.20.158	Piso 3	Vlan 5	SG_y_Unidades					
Centro de Cómputo	10	13	192.168.20.162 - 192.168.20.174	Piso 2	Vlan 6	C_Computo	10	13	192.168.20.161	192.168.20.162 - 192.168.20.174	255.255.255.240
Cámaras Web	9	13	192.168.20.1778 - 192.168.20.190		Vlan 7	Cámaras	9	13	192.168.20.177	192.168.20.178 - 192.168.20.190	255.255.255.240
Sub Gerencia de Desarrollo Económico, Productivo y Medio Ambiente.	5	9	192.168.20.194 - 192.168.20.202	Piso 2	Vlan 8	SGD_Economico	7	13	192.168.20.193	192.168.20.194 - 192.168.20.206	255.255.255.240
Unidad de Gestión Ambiental y Residuos Sólidos	2	4	192.168.20.203 - 192.168.20.206	Piso 2	Vlan 8	SGD_Economico					
Servidores	4	13	192.168.20.210 - 192.168.20.222	Piso 2	Vlan 9	Servidores	4	13	192.168.20.209	192.168.20.210 - 192.168.20.222	255.255.255.240

Fuente: Elaboración propia.

Áreas y Oficinas por Pisos

Esta distribución de Áreas agrupados por pisos y teniendo sus respectivos rangos de números IPs nos servirá para dar inicio a la implementación en el Simulador Packet Tracert.

Tabla 9

Distribución de las diferentes Áreas u Oficinas en el Gobierno Local de Paucará.

Áreas/Oficinas	N° de Host Máximo	Rango de Ips	Puerta de enlace	Máscara de subred	Ubicación	Nombre de Vlan	Nombre de Vlan
Unidad de Recursos Humanos	4	192.168.20.56 - 192.168.20.59	192.168.20.1	255.255.255.192	Piso 1	Vlan 2	G_Municipal
Unidad de Administración Tributaria	3	192.168.20.60 - 192.168.20.62	192.168.20.1	255.255.255.192	Piso 1	Vlan 2	G_Municipal
ULE SISFOH	6	192.168.20.76 - 192.168.20.81	192.168.20.65	255.255.255.224	Piso 1	Vlan 3	SGD_Social
PVL	4	192.168.20.82 - 192.168.20.85	192.168.20.65	255.255.255.224	Piso 1	Vlan 3	SGD_Social
Oficina de Imagen Institucional	4	192.168.20.115 - 192.168.20.118	192.168.20.97	255.255.255.224	Piso 1	Vlan 4	Alcaldia

Sub Gerencia de Planeamiento y Presupuesto	10	192.168.20.12 - 192.168.20.21	192.168.20.1	255.255.255.192	Piso 2	Vlan 2	G_Municipal
Unidad de Logística	10	192.168.20.28 - 192.168.20.37	192.168.20.1	255.255.255.192	Piso 2	Vlan 2	G_Municipal
Oficina de Patrimonio	5	192.168.20.38 - 192.168.20.42	192.168.20.1	255.255.255.192	PISO 2	Vlan 2	G_Municipal
Unidad de Tesorería	7	192.168.20.43 - 192.168.20.49	192.168.20.1	255.255.255.192	Piso 2	Vlan 2	G_Municipal
Unidad de Contabilidad	6	192.168.20.50 - 192.168.20.55	192.168.20.1	255.255.255.192	Piso 2	Vlan 2	G_Municipal
Sub Gerencia de Desarrollo Social y Servicio Institucional	6	192.168.20.66 - 192.168.20.71	192.168.20.65	255.255.255.224	Piso 2	Vlan 3	SGD_Social
Secretaria de GDSSI	4	192.168.20.72 - 192.168.20.75	192.168.20.65	255.255.255.224	Piso 2	Vlan 3	SGD_Social
Unidad Promoción Social	9	192.168.20.86 - 192.168.20.94	192.168.20.65	255.255.255.224	Piso 2	Vlan 3	SGD_Social

Sub Gerencia de Asesoría Legal	8	192.168.20.119 - 192.168.20.126	192.168.20.97	255.255.255.224	Piso 2	Vlan 4	Alcaldia
Centro de Cómputo	13	192.168.20.162 - 192.168.20.174	192.168.20.161	255.255.255.240	Piso 2	Vlan 6	C_Computo
Sub Gerencia de Desarrollo Económico, Productivo y Medio Ambiente	9	192.168.20.194 - 192.168.20.202	192.168.20.193	255.255.255.240	Piso 2	Vlan 8	SGD_Economico
Unidad de Gestión Ambiental y Residuos Sólidos	4	192.168.20.203 - 192.168.20.206	192.168.20.193	255.255.255.240	Piso 2	Vlan 8	SGD_Economico
Servidores	13	192.168.20.210 - 192.168.20.222	192.168.20.209	255.255.255.240	Piso 2	Vlan 9	Servidores
Gerencia Municipal	10	192.168.20.2 - 192.168.20.11	192.168.20.1	255.255.255.192	Piso 3	Vlan 2	G_Municipal
Sub Gerencia de Administración y Finanzas	6	192.168.20.22 - 192.168.20.27	192.168.20.1	255.255.255.192	Piso 3	Vlan 2	G_Municipal

Alcaldía	6	192.168.20.98 - 192.168.20.103	192.168.20.97	255.255.255.224	Piso 3	Vlan 4	Alcaldia
Oficina de Secretaria General	11	192.168.20.104 - 192.168.20.114	192.168.20.97	255.255.255.224	Piso 3	Vlan 4	Alcaldia
Sub Gerencia de Infraestructura, Urbano y Rural	6	192.168.20.130 - 192.168.20.135	192.168.20.129	255.255.255.224	Piso 3	Vlan 5	SG_y_Unidades
Unidad de Obras Publicas	4	192.168.20.136 - 192.168.20.139	192.168.20.129	255.255.255.224	Piso 3	Vlan 5	SG_y_Unidades
Unidad de Liquidación y Supervisión	9	192.168.20.140 - 192.168.20.148	192.168.20.129	255.255.255.224	Piso 3	Vlan 5	SG_y_Unidades
Unidad de Catastro Urbano y Rural	4	192.168.20.149 - 192.168.20.152	192.168.20.129	255.255.255.224	Piso 3	Vlan 5	SG_y_Unidades
Unidad de Estudios y Proyectos	6	192.168.20.153 - 192.168.20.158	192.168.20.129	255.255.255.224	Piso 3	Vlan 5	SG_y_Unidades
Cámaras Web	13	192.168.20.177 - 192.168.20.190	192.168.20.177	255.255.255.240	Piso 3	Vlan 7	Cámaras

Fuente: Elaboración propia.

4.1.1.3. Desarrollo Diseño Físico

Seleccionando los dispositivos adecuados

Cisco 2811 Router

El Router Cisco 2811 es recomendable para implementar comunicaciones corporativas donde es necesario implementar muchas tareas, este dispositivo es interesante porque permite incrementar la productividad y menorar costos, a continuación, mostramos las características:

- Memoria RAM: 256 MB (instalados) / 768 MB (máx.) – DDR SDRAM, 256 MB (instalados) /760 MB (máx.) – DDR SDRAM
- Memoria Flash: 64 MB (instalados) / 256 MB (máx.)
- Protocolos de interconexión de datos: Ethernet, Fast Ethernet
- Red / Protocolo de transporte: IPSec
- Protocolo de gestión remota: SNMP 3
- Protección Firewall.

Figura 44

Router Cisco 2811.

Switches de la serie Catalyst 2860 de Cisco

Equipo de comunicación que soporta voz, video, datos, también brinda un acceso seguro y una mejor administración en la infraestructura de red, también permite gestionar la prioridad al tráfico de voz, mantiene a usuarios no autorizados alejados de la red, ya que permite implementar redes virtuales. Mostramos las características:

- Conmutador – 24 puertos – L3 – Gestionado
- Puertos 24 x10/100 + 2 x SPF

- Alimentación por Ethernet (PoE)

Figura 45

Switch Cisco Catalyst de la serie 2960.

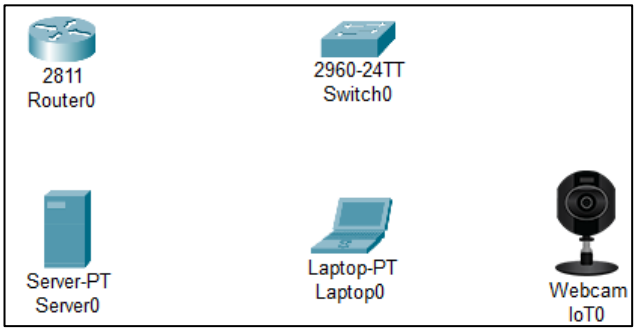
4.1.1.4. Pruebas del diseño

Diseñando la Simulación

Para el diseño de la simulación se está utilizando un router cisco 2811, nueve switch ciscos 2960 de 24 puertos Fast Ethernet, una computadora para cada área u oficina, un servidor para implementar un sistema de videovigilancia con cámaras Web.

Figura 46

Dispositivos finales e intermediarios utilizados en la simulación.



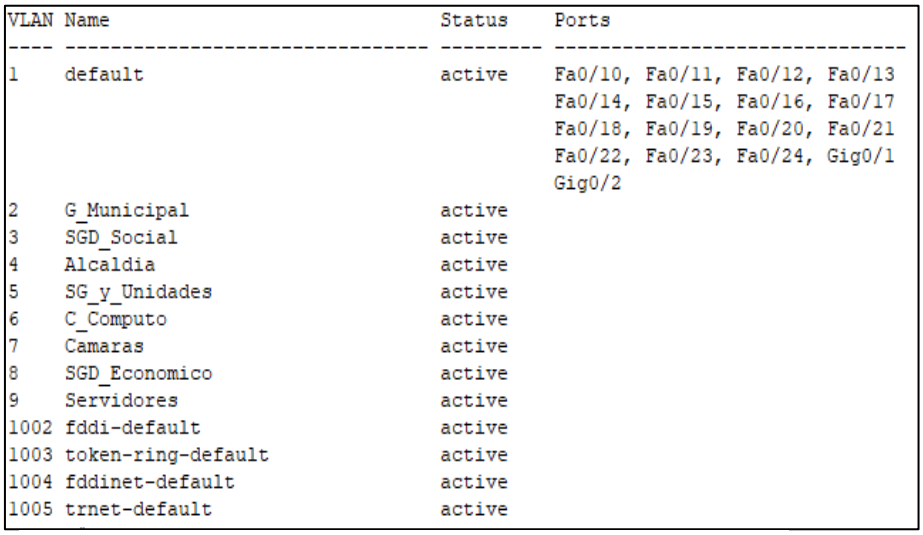
Los equipos de comunicación se han identificado con un nombre y en el piso del edificio del Gobierno Local de Paucará donde se encuentra. Para el Router tiene el nombre de Router_Principal, al Switch que se encuentre en el primer piso tiene el nombre de Switch1_Piso1, de esa forma para los siguientes switchs.

Nuestra infraestructura consta de redes virtuales, las cuales han sido configurados en los nueve switchs, como podemos visualizar en la

gráfica como identificativos están enumerados desde la Vlan 2 hasta la Vlan 9, con sus respectivos nombres.

Figura 47

Configuración de redes virtuales en el Swtich.



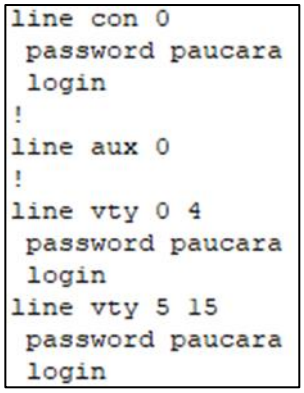
VLAN	Name	Status	Ports
1	default	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
2	G_Municipal	active	
3	SGD_Social	active	
4	Alcaldia	active	
5	SG_y_Unidades	active	
6	C_Computo	active	
7	Camaras	active	
8	SGD_Economico	active	
9	Servidores	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Fuente: Elaboración propia.

Los dispositivos de comunicación como Router y Switch, están protegidos con contraseña, esto para evitar el ingreso de terceras personas. Estas contraseñas también servirán para que el administrador de la infraestructura del Gobierno Local de Paucara pueda administrar remotamente.

Figura 48

Configurando seguridad en los dispositivos de comunicación.



```
line con 0
 password paucara
 login
!
line aux 0
!
line vty 0 4
 password paucara
 login
line vty 5 15
 password paucara
 login
```

Fuente: Elaboración propia.

También se ha configurado seguridad en todos los switches de acceso a los usuarios, de manera si terceras personas ajenas a la entidad quisieran ingresar los puertos de los switchs en el nivel de acceso serán bloqueados. En la configuración visualizamos la configuración que el puerto FastEthernet0/4 pertenece a la red virtual 3, es de modo acceso, y ese puerto solo reconoce la PC con dirección MAC 00E0.F927.D4AB.

Figura 49

Configurando seguridad en los switchs de acceso.

```
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.F927.D4AB
```

Fuente: Elaboración propia.

En el nivel de acceso los puertos han sido distribuidos a las diferentes redes virtuales, tal como visualizamos en la siguiente figura, los puertos FastEthernet0/4 y FastEthenrnet0/11 pertenecen a la red virtual 2, de igual forma el pueto FastEthernet0/17 y FastEthernet0/23 pertenece a la red virtual 3.

Figura 50

Asignación de puertos a las redes virtuales.

```
2    G_Municipal                       active    Fa0/4, Fa0/11
3    SGD_Social                        active    Fa0/17, Fa0/23
```

Fuente: Elaboración propia.

En el swtich de nombre Swtich_Principal los primeros 9 puertos FastEthernet están configurados como troncales, y pertenecen a la Red virtual con identificador 6 como podemos visualizar en la siguiente gráfica.

Figura 51

Asignación de puertos del switch como troncales.

```
Switch_Principal#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      6
Fa0/2       on           802.1q         trunking      6
Fa0/3       on           802.1q         trunking      6
Fa0/4       on           802.1q         trunking      6
Fa0/5       on           802.1q         trunking      6
Fa0/6       on           802.1q         trunking      6
Fa0/7       on           802.1q         trunking      6
Fa0/8       on           802.1q         trunking      6
Fa0/9       on           802.1q         trunking      6
```

Fuente: Elaboración propia.

En los ocho switchs que están en el nivel de acceso se ha configurado el FastEthernet0/1 como troncal pertenece a la red virtual con identificador 6. En la gráfica podemos visualizar que el puerto FastEthernet0/1 está configurado como troncal, y es por allí que va a pasar la información de las otras subredes.

Figura 52

Asignación de puertos del Switch de acceso para usuarios como troncales.

```
Switch1_Pisol#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      6

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,2,3,4,5,6,7,8,9

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,2,3,4,5,6,7,8,9
```

En el router también se ha implementado dhcp para otorgar números IPs a las cámaras Web.

Figura 53

Configuración de DHCP en el router.

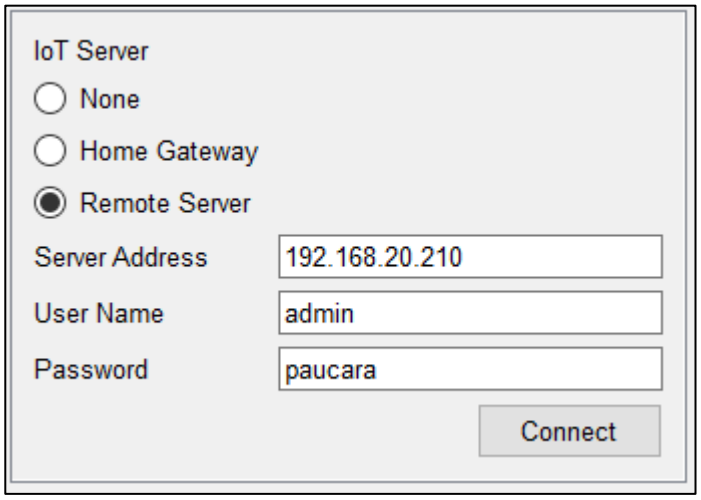
```
ip dhcp pool vlan7_Camaras
 network 192.168.20.176 255.255.255.240
 default-router 192.168.20.177
```

Fuente: Elaboración propia – Cisco Packet Tracer.

El sistema de videovigilancia se está utilizando un servidor, donde se puede visualizar lo que está mostrando las cámaras web. Para ello en las cámaras web se ha configurado como servidor remoto la dirección IP del servidor, la 192.168.20.210, con su respectivo nombre de usuario y contraseña.

Figura 54

Configuración del servicio de cámaras web en el servidor.



Para las computadoras se asignado números IP de forma estática.

Figura 55

Verificación de dirección IP en las computadoras.

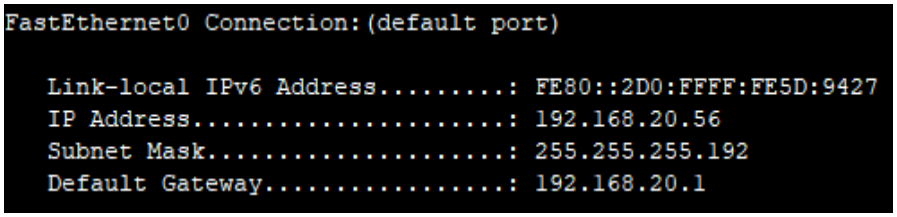
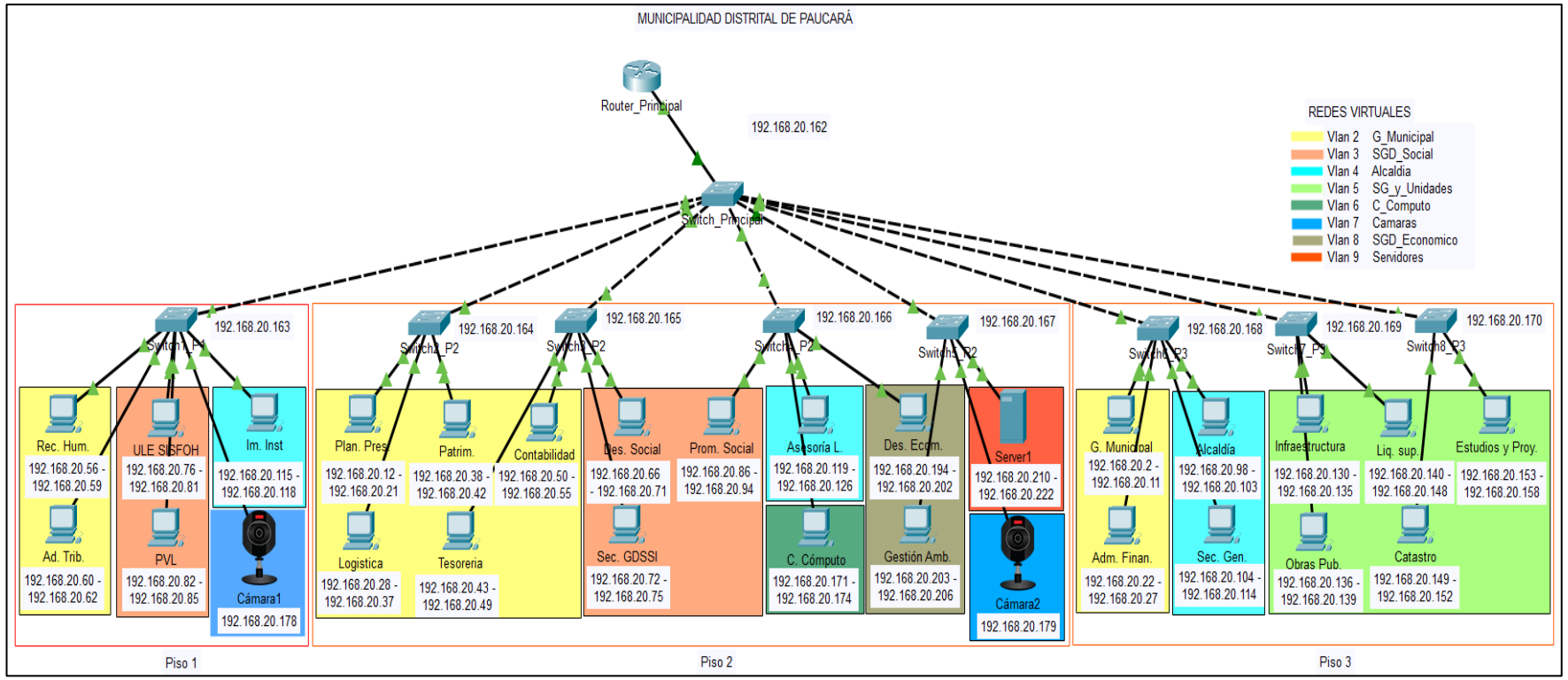


Figura 56

Diseño de Infraestructura de red de datos del Gobierno Local de Paucará.



Fuente: Elaboración propia.

Pruebas de la Infraestructura de red de datos

Estas pruebas han permitido demostrar las hipótesis planteadas en la investigación.

- ✓ Pruebas de conectividad en una misma red virtual, para ello hacemos ping del host de la **Unidad Recursos Humanos** con dirección IP **192.168.20.56** que se encuentra en el primer piso de la Municipalidad de Paucará al host de la **Unidad Contabilidad** con dirección IP **192.168.20.50**. Como podemos observar la figura la comunicación fue éxitos y se tuvo un resultado positivo.

  Figura 57

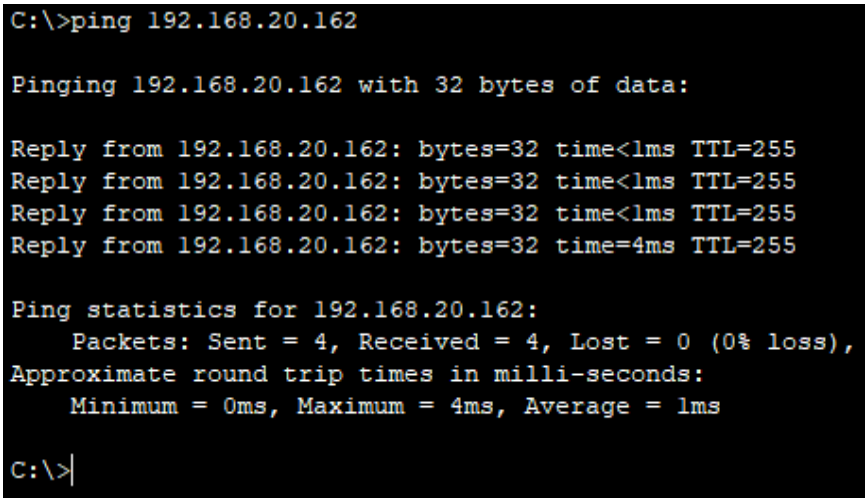
  Prueba de conectividad en una misma red virtual.

```
C:\>ping 192.168.20.50

Pinging 192.168.20.50 with 32 bytes of data:

Reply from 192.168.20.50: bytes=32 time<1ms TTL=128
Reply from 192.168.20.50: bytes=32 time=11ms TTL=128
Reply from 192.168.20.50: bytes=32 time=10ms TTL=128
Reply from 192.168.20.50: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>
```

- ✓ Prueba de conectividad del Centro de Cómputo cuyo host esta con dirección IP 192.168.20.171 al Swtich_Principal con dirección IP 192.168.20.162. como podemos observar el resultado fue positivo, todos los switch y los host del Centro de Cómputo pertenecen a una red virtual independiente, esto con la finalidad de tener una buena administración por parte de los responsables, como podrá visualizar se tuvo un resultado positivo.

Figura 58

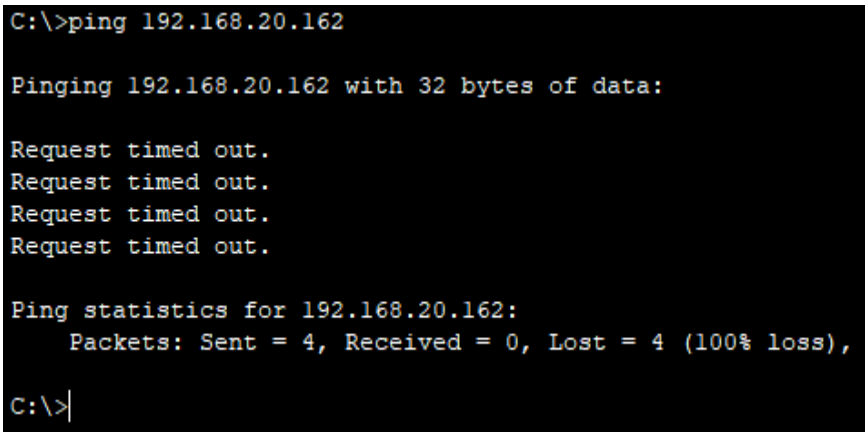
Conectividad de una PC a un Switch.



- ✓ Prueba de conectividad entre host que pertenecen a redes diferentes: ping del host de la Unidad Recursos Humanos con dirección IP 192.168.20.56 al Switch_Principal. Como puede visualizar en la gráfica el resultado fue exitoso, como son dos host que pertenecen a redes diferentes, no puede haber comunicación, es una forma de seguridad que también se está implementando.

Figura 59

Prueba de conectividad de host en redes virtuales diferentes.

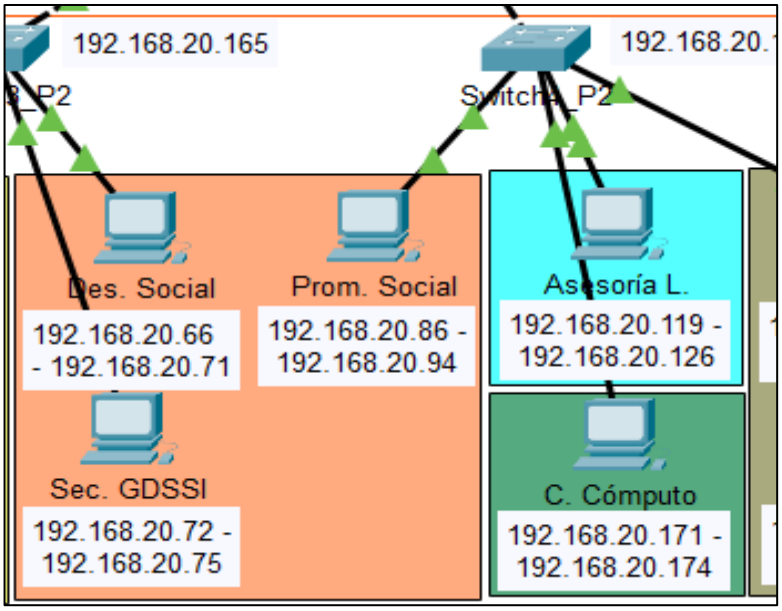


- ✓ Prueba de seguridad para usuarios no autorizados, lo haremos en la Vlan 3 SGD_Social, hacemos ping del host de la Unidad de Promoción Social con dirección IP 192.168.20.86 al host de ULE

SISFOH con dirección IP 192.168.20.76. La comunicación es éxitos porque son host que pertenecen a una misma red virtual.

Figura 60

Puerto del Switch de Asesoría Legal activado.

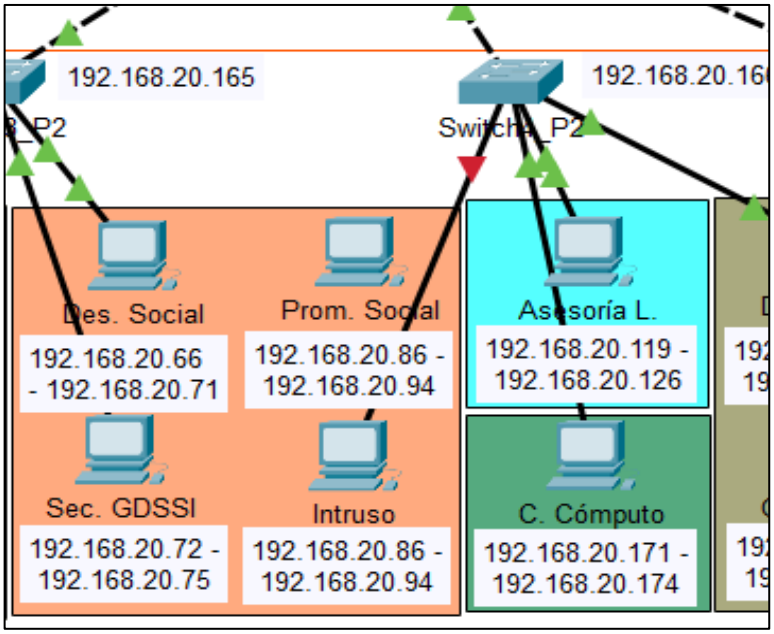


Fuente: Elaboración propia.

Ahora una tercera persona (intruso) intenta ingresar a la red, se conecta en el mismo puerto donde está conectado el host de la Unidad de Promoción social, el resultado es positivo, el puerto del switch se ha bloqueado, esto porque es una computadora no reconocible por la infraestructura de red de datos del Gobierno Local de Paucará.

Figura 61

Puerto del Switch de Asesoría Legal desactivado.

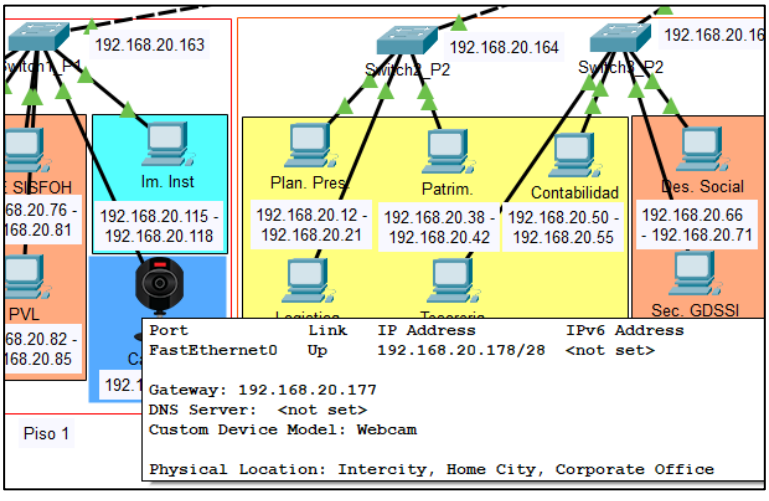


Fuente: Elaboración propia.

✓ Prueba del servicio de DHCP, este servicio solo se ha implementado para las cámaras web, se ha implementado en el Router, que es el encargado de asignar direcciones IP a todas las cámaras web. El resultado es positivo porque podemos visualizar las direcciones IPs en las cámaras Web.

Figura 62

Servicio DHCP para cámaras web.

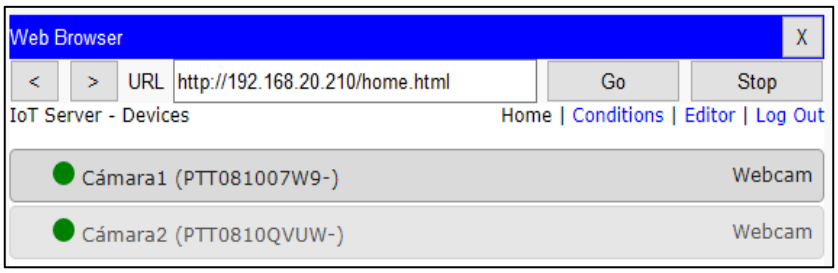


Fuente: Elaboración propia.

- ✓ Verificando las cámaras web en el servidor. El resultado es positivo porque el servidor está registrando las cámaras web implementados en el Gobierno Local de Paucara.

  Figura 63

  Reconocimiento de cámaras web en el servidor.



- ✓ Prueba de seguridad en los dispositivos intermediarios, solo haremos al Router_Principal. El resultado es positivo, los dispositivos intermediarios están protegidos con contraseñas, esto debido a que solo ingresan personas autorizadas.

  Figura 64

  Prueba de acceso al Router.

```
User Access Verification

Password:

Router_Principal>enable
Password:
Router_Principal#
```

- ✓ Mostrando las redes virtuales en el Switch_Principal. Utilizando el respectivo comando podemos visualizar las diferentes redes virtuales que se ha implementado en la infraestructura de red de datos del Gobierno Local de Paucará.

Figura 65

Verificando las redes virtuales locales en el Switch.

```
Switch_Principal>enable
Switch_Principal#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
2    G_Municipal                       active
3    SGD_Social                        active
4    Alcaldia                          active
5    SG_y_Unidades                     active
6    C_Computo                         active
7    Camaras                           active
8    SGD_Economico                     active
9    Servidores                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

4.1.2. Presentación de resultados

Ahora se están visualizando los resultados que se han obtenido teniendo los indicadores en cuanto a Seguridad de la información en la Infraestructura de Red de datos del Gobierno Local de Paucara.

4.1.2.1. Indicador: Tiempos de respuesta de las aplicaciones informáticas.

El tiempo de respuesta de las aplicaciones informáticas dentro de la red local del Gobierno Local de Paucara hace referencia que las aplicaciones se carguen en el menor tiempo posible, en la infraestructura actual existe un tiempo de demora en visualizarse, esto es un motivo que se tuvo énfasis cuando se diseñó la simulación.

Red de datos en la actualidad

La tabla nos muestra datos que han sido obtenidos como tiempos de respuesta de los 26 hosts al servidor de aplicación, el tiempo de respuesta esta medido en milisegundos.

Tabla 10

Resultado de los tiempos de respuesta en la red de datos en la actualidad (PRE TEST).

Host		Servidor de aplicación
	Host 1	77,30

Gerencia Municipal	Host 2	72,50
	Host 3	75,30
	Host 4	79,80
	Host 5	75,60
Sub Gerencia de Planeamiento y Presupuesto	Host 6	70,50
	Host 7	72,60
	Host 8	79,50
	Host 9	72,70
	Host 10	76,20
	Host 11	75,60
Sub Gerencia de Administración y Finanzas	Host 12	71,80
	Host 13	74,60
	Host 14	78,60
Unidad de Logística	Host 15	75,70
	Host 16	73,80
	Host 17	73,40
	Host 18	78,30
	Host 19	75,80
Oficina de Patrimonio	Host 20	70,50
	Host 21	78,90
	Host 22	70,30
Unidad de Tesorería	Host 23	76,40
	Host 24	72,70
	Host 25	79,90
	Host 26	73,50
Promedio		**75,07**

Fuente: Elaboración propia.

Infraestructura de la red de datos

La tabla nos muestra datos que han sido obtenidos como tiempos de respuesta de los 26 hosts al servidor de aplicación, esta prueba a sido

realizado en el diseño simulado, el tiempo de respuesta esta medido en milisegundos.

Tabla 11

Resultado de los tiempos de respuesta en la infraestructura de la red de datos (POST TEST).

Host		Servidor de aplicación
Gerencia Municipal	Host 1	38,80
	Host 2	39,00
	Host 3	37,20
	Host 4	34,30
	Host 5	39,80
Sub Gerencia de Planeamiento y Presupuesto	Host 6	34,10
	Host 7	36,40
	Host 8	39,20
	Host 9	36,70
	Host 10	34,50
	Host 11	36,10
Sub Gerencia de Administración y Finanzas	Host 12	39,10
	Host 13	32,90
	Host 14	35,40
Unidad de Logística	Host 15	32,30
	Host 16	30,10
	Host 17	31,00
	Host 18	36,60
	Host 19	37,60
Oficina de Patrimonio	Host 20	30,20
	Host 21	33,20
	Host 22	34,70
Unidad de Tesorería	Host 23	31,70
	Host 24	30,10
	Host 25	32,30

	Host 26	39,80
Promedio		**35,12**

Fuente: Elaboración propia.

4.1.2.2. Indicador: Velocidad de transferencia de información

La velocidad de carga y descarga de información está determinado por todo el personal que hace uso de la red de datos, esta acción lo pueden hacer ya sea desde email o de la nube, en la red de datos actual se tiene una velocidad no considerable, esto debido a la cantidad de usuarios que trabajan en la red, hay casos donde la red deja de funcionar.

Red de datos en la actualidad

Tabla 12

Resultado de la velocidad de transferencia de datos (Mbps) – Red actual (PRE TEST).

		Servidor de aplicación	
Host		**Carga**	**Descarga**
Gerencia Municipal	Host 1	3,90	1,80
	Host 2	3,20	2,20
	Host 3	4,90	2,40
	Host 4	2,70	2,60
	Host 5	4,80	2,80
Sub Gerencia de Planeamiento y Presupuesto	Host 6	4,80	2,20
	Host 7	2,10	2,50
	Host 8	4,20	2,80
	Host 9	4,90	2,80
	Host 10	3,40	2,70
	Host 11	2,40	2,40
Sub Gerencia de Administración y Finanzas	Host 12	4,80	2,20
	Host 13	3,70	2,10
	Host 14	4,10	2,50

Unidad de Logística	Host 15	4,30	1,70
	Host 16	3,10	1,80
	Host 17	4,50	2,60
	Host 18	3,10	2,30
	Host 19	2,80	2,50
Oficina de Patrimonio	Host 20	4,50	2,20
	Host 21	2,20	2,80
	Host 22	4,30	1,70
Unidad de Tesorería	Host 23	2,70	2,30
	Host 24	2,00	1,50
	Host 25	4,60	2,40
	Host 26	4,70	2,60
Promedio		**3,72**	**2,32**

Fuente: Elaboración propia.

Diseño simulado de la Infraestructura de la red de datos.

Tabla 13

Resultado de la velocidad de transferencia de datos (Mbps) – Infraestructura de red de datos (POST TEST).

Host		Carga	Descarga
Gerencia Municipal	Host 1	5,30	3,30
	Host 2	4,10	3,40
	Host 3	4,60	4,10
	Host 4	4,60	3,60
	Host 5	5,00	2,90
Sub Gerencia de Planeamiento y Presupuesto	Host 6	5,40	4,20
	Host 7	5,90	4,40
	Host 8	5,90	3,10
	Host 9	5,90	4,00
	Host 10	5,70	3,20
	Host 11	4,10	3,80

Sub Gerencia de Administración y Finanzas	Host 12	4,50	4,00
	Host 13	4,70	4,50
	Host 14	5,80	4,00
Unidad de Logística	Host 15	4,60	2,60
	Host 16	4,60	3,00
	Host 17	5,10	4,00
	Host 18	4,90	3,50
	Host 19	5,20	2,50
Oficina de Patrimonio	Host 20	5,50	3,40
	Host 21	4,50	3,10
	Host 22	4,10	4,10
Unidad de Tesorería	Host 23	5,50	2,80
	Host 24	5,10	4,00
	Host 25	4,80	2,50
	Host 26	5,80	3,30
Promedio		**5,05**	**3,51**

Fuente: Elaboración propia.

4.1.2.3. Indicador: Acceso de usuarios no autorizados.

Red de datos en la actualidad

Tabla 14

Resultado de accesos no autorizados – Red de datos en la actualidad (PRE TEST).

Puerto de Switch para Host		**Acceso al puerto**
Gerencia Municipal	Puerto de Switch para Host 1	1,00
	Puerto de Switch para Host 2	1,00
	Puerto de Switch para Host 3	1,00
	Puerto de Switch para Host 4	1,00
	Puerto de Switch para Host 5	1,00
	Puerto de Switch para Host 6	1,00

Sub Gerencia de Planeamiento y Presupuesto	Puerto de Switch para Host 7	1,00
	Puerto de Switch para Host 8	1,00
	Puerto de Switch para Host 9	1,00
	Puerto de Switch para Host 10	1,00
	Puerto de Switch para Host 11	1,00
Sub Gerencia de Administración y Finanzas	Puerto de Switch para Host 12	1,00
	Puerto de Switch para Host 13	1,00
	Puerto de Switch para Host 14	1,00
Unidad de Logística	Puerto de Switch para Host 15	1,00
	Puerto de Switch para Host 16	1,00
	Puerto de Switch para Host 17	1,00
	Puerto de Switch para Host 18	1,00
	Puerto de Switch para Host 19	1,00
Oficina de Patrimonio	Puerto de Switch para Host 20	1,00
	Puerto de Switch para Host 21	1,00
	Puerto de Switch para Host 22	1,00
Unidad de Tesorería	Puerto de Switch para Host 23	1,00
	Puerto de Switch para Host 24	1,00
	Puerto de Switch para Host 25	1,00
	Puerto de Switch para Host 26	1,00
Promedio		**1,00**

Fuente: Elaboración propia.

Diseño simulado de la Infraestructura de la red de datos.

Tabla 15

Resultado de accesos no autorizados – Infraestructura de red de datos (POST TEST).

Puerto de Switch para Host		**Acceso al puerto**
Gerencia Municipal	Puerto de Switch para Host 1	0,00

	Puerto de Switch para Host 2	0,00
	Puerto de Switch para Host 3	0,00
	Puerto de Switch para Host 4	0,00
	Puerto de Switch para Host 5	0,00
Sub Gerencia de Planeamiento y Presupuesto	Puerto de Switch para Host 6	0,00
	Puerto de Switch para Host 7	0,00
	Puerto de Switch para Host 8	0,00
	Puerto de Switch para Host 9	0,00
	Puerto de Switch para Host 10	0,00
	Puerto de Switch para Host 11	0,00
Sub Gerencia de Administración y Finanzas	Puerto de Switch para Host 12	0,00
	Puerto de Switch para Host 13	0,00
	Puerto de Switch para Host 14	0,00
Unidad de Logística	Puerto de Switch para Host 15	0,00
	Puerto de Switch para Host 16	0,00
	Puerto de Switch para Host 17	0,00
	Puerto de Switch para Host 18	0,00
	Puerto de Switch para Host 19	0,00
Oficina de Patrimonio	Puerto de Switch para Host 20	0,00
	Puerto de Switch para Host 21	0,00
	Puerto de Switch para Host 22	0,00
Unidad de Tesorería	Puerto de Switch para Host 23	0,00
	Puerto de Switch para Host 24	0,00
	Puerto de Switch para Host 25	0,00
	Puerto de Switch para Host 26	0,00
	Promedio	**0,00**

Fuente: Elaboración propia.

4.1.3. Síntesis de resultados

4.1.3.1. Tiempos de respuesta de las aplicaciones informáticas a nivel LAN

Tabla 16

Resumen de tiempos de respuesta de las aplicaciones informáticas a nivel LAN.

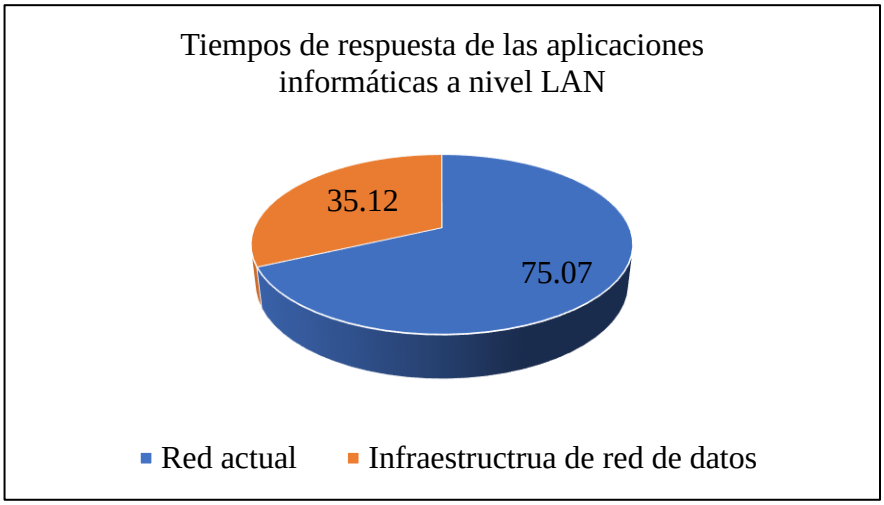
Indicador	Red actual (PRE TEST)	Diseño de la Red de datos (POST TEST)
Tiempos de respuesta de las aplicaciones informáticas a nivel LAN	75,07	35,12

Fuente: Elaboración propia.

La tabla muestra el tiempo de respuesta de las aplicaciones a nivel LAN en promedio, se tiene en la red actual 75.07 milisegundos en promedio, comparando con el Diseño de la Red de datos se tiene en promedio 35.12 milisegundos y podemos visualizar hay una reducción de 39.95 milisegundos.

Figura 66

Resumen de tiempos de respuesta de las aplicaciones informáticas a nivel LAN.



Fuente: Elaboración propia.

La figura muestra el tiempo de respuesta de las aplicaciones a nivel LAN en promedio, se tiene en la red actual 75.07 milisegundos en promedio, comparando con el Diseño de la Red de datos se tiene en promedio 35.12 milisegundos y podemos visualizar hay una reducción de 39.95 milisegundos.

4.1.3.2. Velocidad de transferencia de información

Velocidad de carga de información

Tabla 17

Velocidad de carga de información.

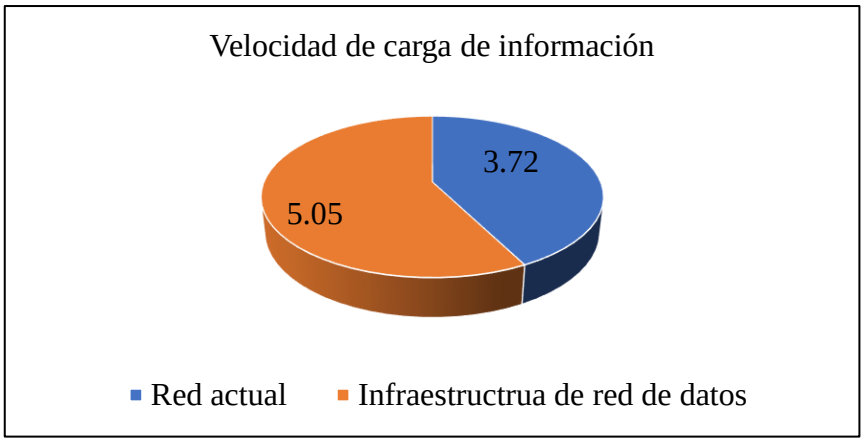
Indicador	Red actual (PRE TEST)	Infraestructura de red de datos (POST TEST)
Velocidad de carga de información	3,72	5,05

Fuente: Elaboración propia.

La tabla muestra la velocidad de carga de información de la red actual que en promedio tiene 3.72 Mps y la Infraestructura de red de datos que tiene en promedio de 5.05 Mbps y podemos ver que hay un aumento de 1.33 Mbps.

Figura 67

Velocidad de carga de información.



Fuente: Elaboración propia.

La figura muestra la velocidad de carga de información de la red actual que en promedio tiene 3.72 Mps y la Infraestructura de red de datos que tiene en promedio de 5.05 Mbps y podemos ver que hay un aumento de 1.33 Mbps.

Velocidad de descarga de información

Tabla 18

Velocidad de descarga de información.

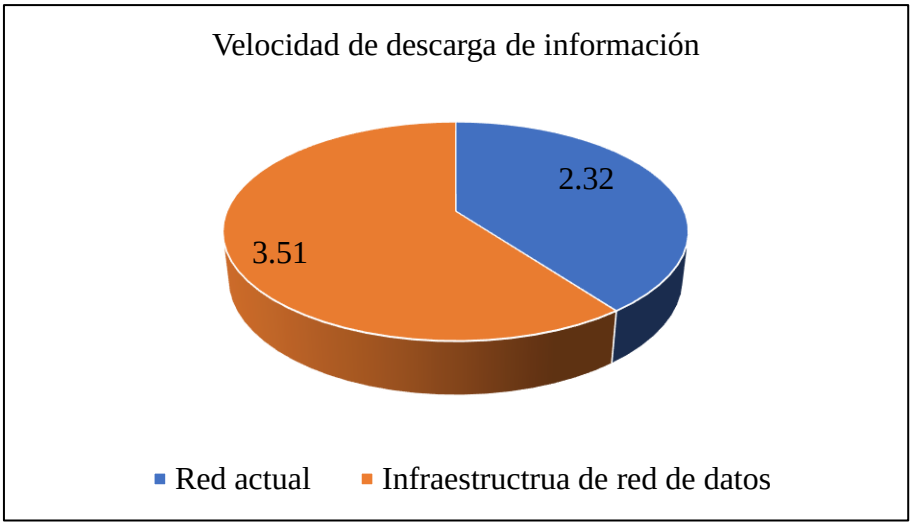
Indicador	Red actual (PRE TEST)	Infraestructura de red de datos (POST TEST)
Velocidad de descarga de información	2,32	3,51

Fuente: Elaboración propia.

La tabla muestra la velocidad de descarga de información de la red actual que en promedio tiene 2.32 Mps y la Infraestructura de red de datos que tiene en promedio de 3.51 Mbps y podemos ver que hay un aumento de 1.19 Mbps.

Figura 68

Velocidad de descarga de información.



Fuente: Elaboración propia.

La figura muestra la velocidad de descarga de información de la red actual que en promedio tiene 2.32 Mps y la Infraestructura de red de datos que tiene en promedio de 3.51 Mbps y podemos ver que hay un aumento de 1.19 Mbps.

4.1.3.3. Acceso de usuarios no autorizados.

Tabla 19

Acceso de usuarios no autorizados.

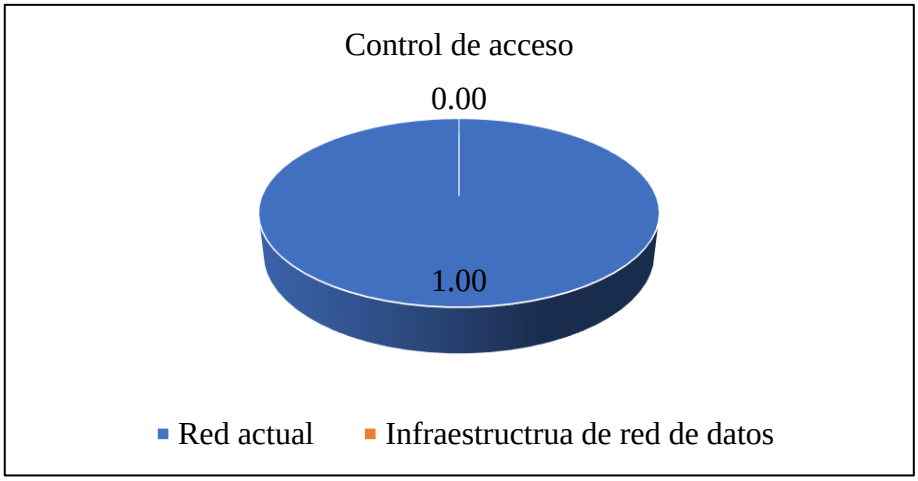
Indicador	Red actual (PRE TEST)	Infraestructura de red de datos (POST TEST)
Control de Acceso	1,00	0,00

Fuente: Elaboración propia.

La tabla muestra el acceso de personas no autorizadas a la red de datos teniendo en la red actual un 100% del ingreso de personas que no pertenecen a la municipalidad, mientras que en la Infraestructura de red de datos tenemos un 0% de ingresos de personas no autorizadas.

Figura 69

Control de acceso.



Fuente: Elaboración propia.

La figura muestra el acceso de personas no autorizadas a la red de datos teniendo en la red actual un 100% del ingreso de personas que no

pertenecen a la municipalidad, mientras que en la Infraestructura de red de datos tenemos un 0% de ingresos de personas no autorizadas.

4.1.4. Prueba de hipótesis

Estadísticas de grupo

Tabla 20

Estadísticas de grupo.

Estadísticas de grupo

	Infraestructura	N	Media	Desv. Desviación	Desv. Error promedio
Tiempos de respuesta de las aplicaciones informáticas a nivel LAN	Red de datos en la actualidad	26	75,0692	2,95767	,58005
	Infraestructura de la red de datos	26	35,1192	3,17994	,62364
Velocidad de carga de información	Red de datos en la actualidad	26	3,7192	,98021	,19224
	Infraestructura de la red de datos	26	5,0462	,58871	,11546
Velocidad de descarga de información	Red de datos en la actualidad	26	2,3231	,37449	,07344
	Infraestructura de la red de datos	26	3,5115	,59284	,11627
Acceso de usuarios no Autorizados	Red de datos en la actualidad	26	1,000	,0000[a]	,0000
	Infraestructura de la red de datos	26	,000	,0000[a]	,0000

a. t no se puede calcular porque las desviaciones estándar de ambos grupos son 0.

Prueba de muestras independientes

Tabla 21

Prueba de muestras independientes.

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Tiempos de respuesta de las aplicaciones informáticas a nivel LAN	Se asumen varianzas iguales	,320	,574	46,907	50	,000	39,95000	,85169	38,23933	41,66067
	No se asumen varianzas iguales			46,907	49,740	,000	39,95000	,85169	38,23911	41,66089
Velocidad de carga de información	Se asumen varianzas iguales	12,695	,001	-5,917	50	,000	-1,32692	,22424	-1,77733	-,87652
	No se asumen varianzas iguales			-5,917	40,959	,000	-1,32692	,22424	-1,77980	-,87404
Velocidad de descarga de información	Se asumen varianzas iguales	8,258	,006	-8,642	50	,000	-1,18846	,13752	-1,46468	-,91224
	No se asumen varianzas iguales			-8,642	42,211	,000	-1,18846	,13752	-1,46595	-,91098

- El tiempo promedio de respuesta de las aplicaciones informáticas a nivel LAN en la Infraestructura de red de datos es mayor que el tiempo promedio de respuesta de las aplicaciones informáticas a nivel LAN en la red de datos actual.

  H0: No existe una diferencia significativa entre el tiempo promedio de respuesta de las aplicaciones informática a nivel LAN en la Infraestructura de red de datos y la red de datos actual.

  H1: Existe una diferencia significativa entre el tiempo promedio de respuesta de las aplicaciones informática a nivel LAN en la Infraestructura de red de datos y la red de datos actual.

  Tabla 22

  Resultados del tiempo promedio de respuesta de las aplicaciones informáticas a nivel LAN.

Nivel de significancia = 0.00	**<**	**α=0.05**
Conclusión		
Existe una diferencia significativa entre el tiempo promedio de respuesta de las aplicaciones informática a nivel LAN en la Infraestructura de red de datos y la red de datos actual.		

  Fuente: Elaboración propia.

- La velocidad de carga de información en la Infraestructura de red de datos es mayor que la velocidad de carga de información en la red de datos actual.

  H0: No existe una diferencia significativa entre la velocidad de carga de información en la Infraestructura de red de datos y la red de datos actual.

  H1: Existe una diferencia significativa entre la velocidad de carga de información en la Infraestructura de red de datos y la red de datos actual.

Tabla 23

Resultados de la velocidad de carga de información.

Nivel de significancia = 0.00	**<**	**α=0.05**
Conclusión		
Existe una diferencia significativa entre la velocidad de carga de información en la Infraestructura de red de datos y la red de datos actual.		

Fuente: Elaboración propia.

- La velocidad de descarga de información en la Infraestructura de red de datos es mayor que la velocidad de descarga de información en la red de datos actual.

H0: No existe una diferencia significativa entre la velocidad de descarga de información en la Infraestructura de red de datos y la red de datos actual.

H1: Existe una diferencia significativa entre la velocidad de descarga de información en la Infraestructura de red de datos y la red de datos actual.

Tabla 24

Resultado de la velocidad de descarga de información.

Nivel de significancia = 0.00	**<**	**α=0.05**
Conclusión		
Existe una diferencia significativa entre la velocidad de descarga de información en la Infraestructura de red de datos y la red de datos actual.		

Fuente: Elaboración propia.

CONCLUSIONES

1. En esta investigación la Infraestructura de red de datos, determina la seguridad de la información de la red de datos en el Gobierno Local de Paucará, lo más importante de la Infraestructura es que lógicamente se ha dividido en redes locales virtuales de forma independiente.

2. En esta tesis se demostró que la infraestructura de red de datos tiene una influencia positiva en la disponibilidad de la información del Gobierno Local de Paucará, lo interesante de esta infraestructura, es que se está utilizando dispositivos de comunicación que sean configurables y permita implementar redes locales virtuales.

3. En esta investigación se demostró que la infraestructura de red de datos tiene una influencia positiva en la confidencialidad de la información en el Gobierno Local de Paucará, la importancia se da en que solo accedan a la información las personas autorizadas, esto se logró configurando los dispositivos de acceso.

RECOMENDACIONES

1. Implementar una infraestructura de red de datos en el Gobierno Local de Paucará, que soporte diferentes servicios involucra seleccionar dispositivos de comunicación con estas características.

2. Implementar redes virtuales locales en la infraestructura de red de datos, es una forma de asegurar la seguridad de la información y se podría considerar otras formas que nos permita llegar a este objetivo.

3. La infraestructura de red de datos que físicamente es una y lógicamente ocho sub redes, también se cuenta con dos subredes más para que se puedan implementar otros servicios según necesidad de la entidad.

REFERENCIAS BIBLIOGRÁFICAS

Areitio Bertolin, J. (2008). Seguridad de la Información Redes, Informatica y sistemas de Informacion. Madrid: Editorial Paraninfo S.A. Universidad de Deusto

Bastar, S. G. (2012). Metodología de la investigación. *Red Tercer Milenio*, *1*(1), 89.

Behrouz A, F. (2007). Transmision de Datos y Redes de Comunicacion (Segunda ed.). España: Mc Grw Hill.

Burgos, J. (2008). Modelo para el Control de Riesgos de Seguridad de la Información en Áreas de Tecnologías de la Información y Comunicaciones (TIC). Universidad del Bío-Bío - Concepción.

Camacho, R. (2008). Diseño e implantación de un Sistema de Gestión de Seguridad de la Información para la protección de los activos informáticos de la Universidad Central de Venezuela. Caracas, Venezuela: Universidad Central.

Castrizano Giménes, Y. (2019). *Configuración de la Red de Datos para los servicios de Acceso a la red por Suscripción de ETECSA*.

Coras Bendezú, J. J. (2013). *Rediseño de la red de comunicaciones basado en tecnologías de alta disponibilidad de gestión de tráfico para mejorar la comunicación de la municipalidad provincial de Churcampa - Huancavelica*.

Cisco Networking Academy, CCNA Exploration 4.0. (2009). Acceso a Wan. Obtenido de http://cisco.netacad.net

Espinosa Reyes, O. L. (2015). *Implementación de Arquitectura de Redes Seguras*. 1-7. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2915/Trabajo de grado.pdf?sequence=1

Fernández, C. (2012). La Norma ISO 27001 del Sistema de Gestión de eguridad de Información, garantía de confidencialidad, Integridad y disponibilidad. España: Asociación Española de Normalizacion y Certificación.

Fontalvo, & Vergara. (2010). La Gestión de la Calidad en los Servicios ISO

9001:2008. Colombia:. Colombia: Editorial Vertice S.L.

Galarza-Macancela, C. V. (2018). *Diseño e implementación de una red de datos segura para la Pontificia Universidad Católica del Ecuador, Santo Domingo*. *4*, 123-137.

Godoy, R. (2014). Seguridad de Información. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estrategica.

Guzman, F. G. (2015). *Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega*. 139. http://repositorio.uncp.edu.pe/handle/UNCP/1478

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2006). Metodologia de la Investigacion (Vol. VI). Mexico, Mexico: McGramHil Education.

Idalberto, C. (2006). Introducción a la Teoría General de la Administración. En *Mc Graw Hill Interamericana*.

Maldonado Chumbe, H. H. (2018). *Tecnología IP para la mejora de la gestión administrativa de la Municipalidad Distrital de Perene*. 139. http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/5119/Maldonado Chumbe.pdf?sequence=1&isAllowed=y

McCabe, J. (2005). Practical. Computer Network Analysis and Design.

Molina Robles, F. (2006). Planificcion y Admistracion de Redes. Madrid, España: Ra-Ma.

Murillo, W. (2008). La investigación científica. Venezuela.

Norma ISO 27001 (Organización Internacional de Estándares). (2013). Sistema de Gestión de Seguridad de Información (SGSI). Obtenido de www.iso27000.es

Oppenheimer, P. (2011). *Top-Down Network Design Third Edition.* Indianapolis: Cisco Press.

Oseda, D. (2018). Fundamentos de Investigacion Cientifica. Huancayo: Soluciones

Graficas.

Pacheco Moscoso, L. E. (2013). Diseño de un modelo de sistema integrado de infraestructura de red de datos para mejorar la gestión de la información en la municipalidad distrital de Mariscal Cáceres. *Universidad Nacional del Centro del Perú*. http://repositorio.uncp.edu.pe/handle/UNCP/1475

Pino, G. G. (2019). El método científico: En *Construcción de problemas de investigación*. https://doi.org/10.2307/j.ctvfc5506.4

Soriano, M. (2014). Seguridad en redes y seguridad de la información (Primera ed.). Improvet.

Stallings, W. (2004). Comunicacion y Redes de Computadoras. Madrid, España: Pearson/Prentice Hall.

Systems: Academia de Networking de Cisco Systems:, A. d. (2004). Guía del Primer año CCNA 1 y 2.

Tanenbaum, A. (2003). Redes de Computadoras (Quinta ed.). Mexico, Mexico: Pearson/Prentice Hall

Vergara Quiroz, G. (2017). Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016. *Universidad César Vallejo*.

Vidal loor, J. A. (2016). *Diseño una propuesta de mejoramiento en la infraestructura de red de datos en la ESPAM MFL con calidad de servicio*.

APÉNDICE

Matriz de consistencia

"DISEÑO DE INFRAESTRUCTURA DE RED DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UN GOBIERNO LOCAL, 2021"

Problemas	Objetivos	Hipótesis	Variable y dimensiones:	Metodología
Problema general: ¿De qué manera el diseño de infraestructura de red de datos influye en la seguridad de la información en el Gobierno Local de Paucará? **Problemas específicos:** 1. ¿Cómo el diseño de infraestructura de red de datos influye en la Integridad de la Información del Gobierno Local de Paucará?	**Objetivo general:** Determinar de qué manera el diseño de infraestructura de red de datos influye en la seguridad de la información en el Gobierno Local de Paucará. **Objetivos específicos:** 1. Determinar la influencia del diseño de infraestructura de red de datos en la Integridad de la Información en el	**Hipótesis general:** El diseño de infraestructura de red de datos influye significativamente en la seguridad de la información en el Gobierno Local de Paucará. **Hipótesis específicas:** 1. El diseño de infraestructura de red de datos influye significativamente en la Integridad de la Información en el Gobierno Local de Paucará.	**Variable Independiente:** Diseño de Infraestructura de red de datos **Cisco S. (2004)** **Dimensiones:** - Tolerancia a fallas - Escalabilidad - Calidad de Servicio (QoS) **Variable Dependiente:** Seguridad de la Información **Godoy R.** (2014) **Dimensiones:** – Integridad,	**Enfoque**: Cuantitativo. **Tipo**: Aplicada **Nivel**: Explicativo. **Diseño**: Pre experimental: 01 x 02 Donde: 01: pre test 02: post test X: Manipulación de la VI. **Población**: Total de Host conectados en el edificio del Gobierno Local de Paucará. **Muestra: No probabilístico por conveniencia** Seleccionando una muestra de 26 host.

2. ¿Cómo el diseño de infraestructura de red de datos influye en la Disponibilidad de la Información del Gobierno Local de Paucará? 3. ¿Cómo el diseño de infraestructura de red de datos influye en la Confidencialidad de la Información del Gobierno Local de Paucará?	Gobierno Local de Paucará. 2. Determinar la influencia del diseño de infraestructura de red de datos en la Disponibilidad de la Información en el Gobierno Local de Paucará. 3. Determinar la influencia del diseño de infraestructura de red de datos en la Confidencialidad de la Información en el Gobierno Local de Paucará.	2. El diseño de infraestructura de red de datos influye significativamente en la Disponibilidad de la Información en el Gobierno Local de Paucará. 3. El diseño de infraestructura de red de datos influye significativamente en la Confidencialidad de la Información en el Gobierno Local de Paucará.	– Disponibilidad – Confidencialidad	**Técnicas de recojo de información:** Observación **Instrumentos de recojo de información**: Ficha de Observación Lista de cotejo **Técnicas de procesamiento y análisis de datos**: Tablas de distribución de frecuencia. Prueba estadística t de Student. Utilización del Software SPSS. **Aspectos éticos.** Consentimiento informado. Uso del software anti plagio. El simulador Cisco Packet Tracer 7.3