Implementación de Redes Virtuales Locales

Fortaleciendo la Seguridad de la Información

Carlos Alcides Almidón Ortiz
Amanda Duran Carhuamaca
Miriam Angoma Astucuri
Leonidas Asto Huamán

Sello Editorial CITSA

Carlos Alcides Almidón Ortiz

Amanda Duran Carhuamaca

Miriam Angoma Astucuri

Leonidas Asto Huamán

Implementación de Redes Virtuales Locales:

Fortaleciendo la seguridad de la Información

https://doi.org/10.61286/edcitsa.vi.97

Sello Editorial CITSA

Maracay, estado Aragua, Venezuela 2024

Catalogación en Fuente

Carlos Alcides Almidón Ortiz

Implementación de Redes Virtuales Locales: Fortaleciendo la seguridad de la Información. 1ª ed. – Maracay: Sello Editorial CITSA, 2024.

Recursos en línea (85 páginas); 42 il. ; 21 x 29,7 cm.

ISBN: 978-980-8050-09-7

Teoría de la comunicación y el control Cibernética I. Almidón Ortiz, Carlos Alcides. II. Duran Carhuamaca, Amanda. III.Angoma Astucuri, Miriam. IV. Asto Huamán, Leonidas.

CDD 003.5

Centro de Investigación en Tecnologías de Salud y Ambiente. Dirección: Calle el Stadium N° 3-A, Las Brisas, La Pedrera, Parroquia Las Delicias, Maracay estado Aragua, Venezuela.

Sello Editorial CITSA

Email: citsa@investigaciondetecnologias.com
Web: www.investigaciondetecnologias.com

Coordinación Editorial: Dr. José Romero
Revisión y corrección de estilo: Dra. Mirta Camacho
Diseño de cubierta: CITSA
Composición y puesta en línea: MSc. Vita María Calzolaio Cristofano
Depósito Legal en la Biblioteca Nacional de Venezuela según el Número AR2024000493

Índice

Presentación

En la actualidad, la digitalización ha transformado la forma en que las organizaciones operan, pero también ha dado lugar a un aumento significativo en la frecuencia y sofisticación de los ataques a los sistemas informáticos. Este fenómeno es consecuencia directa de los avances en los servicios y modelos de comunicación, así como del auge de las nuevas tecnologías de la información y la comunicación (TIC).

Ante este panorama, las organizaciones se ven obligadas a implementar estrategias proactivas que les permitan llevar a cabo análisis exhaustivos para prevenir, controlar y mitigar los riesgos asociados con la violación o vulnerabilidad de su información. La necesidad de proteger los datos y mantener la integridad de los sistemas se ha vuelto imperativa no solo para salvaguardar la información sensible, sino también para preservar la confianza de los clientes y la reputación empresarial.

Además, es crucial que estas estrategias no solo se centren en la detección de amenazas, sino que también incluyan planes de respuesta ante incidentes y formación continua del personal. De esta manera, las organizaciones podrán adaptarse a un entorno digital en constante evolución y enfrentar los desafíos que presentan los ciberataques de manera efectiva.

Este libro, ***Implementación de Redes Virtuales Locales (VLAN): Fortaleciendo la Seguridad de la Información***, surge como una respuesta a esta necesidad imperiosa de blindar la información virtual en la Universidad Nacional de Huancavelica, de esta manera optimizar los procesos informáticos.

La implementación de VLAN (Redes de Área Local Virtual) en el contexto de la norma ISO 27001 se presenta como una estrategia eficaz para mejorar la seguridad y la gestión de la información en entornos educativos. En particular, el apartado A.13 de la norma, que se centra en la seguridad en las comunicaciones, establece directrices claras para proteger la información durante su transmisión. Las VLAN permiten segmentar la red en dominios lógicos independientes, lo que ayuda a controlar el acceso a datos sensibles y a reducir el riesgo de violaciones de seguridad.

Las VLAN ofrecen múltiples beneficios en términos de seguridad. Al separar grupos de usuarios, como docentes y estudiantes, se minimiza el riesgo de accesos no autorizados a información confidencial. Esto es esencial para cumplir con normativas como la ISO 27001 y el GDPR, ya que asegura que solo los usuarios autorizados puedan acceder a datos críticos. Además, la segmentación del tráfico mejora el rendimiento de la red al contenerlo en dominios más pequeños, lo que también dificulta ataques por difusión.

Por último, la implementación de VLAN no solo fortalece la seguridad, sino que también enriquece la comunicación entre docentes y alumnos. Al crear redes específicas para cada grupo, se optimiza el acceso a recursos educativos y plataformas virtuales, facilitando una interacción más fluida. Esto permite a los docentes responder de manera más ágil a las necesidades del alumnado, garantizando un entorno educativo virtual más seguro y eficiente. Así, las VLAN se convierten en una herramienta poderosa para mejorar tanto la seguridad como la efectividad en el proceso educativo.

La metodología propuesta implica la recopilación de datos sobre el estado actual de las redes informáticas en la Universidad, el diseño e implementación de las VLAN. Se seleccionaron indicadores para evaluar la eficacia y eficiencia de la nueva metodología comparada con datos previos a la instalación. Como meta, aportar soluciones para mejorar el funcionamiento de las herramientas web de la UNH.

Los Autores

Carlos Alcides Almidón Ortiz
https://orcid.org/0000-0003-1055-9724
Universidad Nacional de Cañete: Cañete - Lima, Lima, PE
calmidon@undc.edu.pe

Amanda Duran Carhuamaca
https://orcid.org/0000-0001-8183-5891
Universidad Nacional de Cañete: Cañete - Lima, Lima, PE
aduran@undc.edu.pe

Míriam Angoma Astucuri
https://orcid.org/0000-0002-4436-1276
Universidad Nacional de Cañete: Cañete - Lima, Lima, PE
miriamangoma@gmail.com / mangoma@undc.edu.pe

Leonidas Asto Huamán
https://orcid.org/0000-0003-2003-1798
Universidad Nacional de Cañete: Cañete - Lima, Lima, PE
astoleonidas@gmail.com

Introducción

En el dinámico panorama de las redes informáticas, la seguridad de la información se ha convertido en una preocupación primordial. Las instituciones a nivel mundial y de cualquier tamaño buscan proteger sus valiosos datos de accesos no autorizados y amenazas cibernéticas. En este contexto, las Redes Virtuales Locales (VLAN) han surgido como una tecnología fundamental para fortalecer la seguridad de la red y segmentar el tráfico de manera eficiente.

El propósito principal de este libro ***Implementación de Redes Virtuales Locales (VLAN): Fortaleciendo la Seguridad de la Información***, es determinar la influencia de redes virtuales locales (VLAN) en la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica, de esta manera optimizar los procesos virtuales dentro de la institución. Las VLAN mejoran la seguridad de la información en las redes informáticas. Al segmentar la red, controlar el acceso y aislar el tráfico, las VLAN contribuyen a reducir el riesgo de incidentes de seguridad y a proteger los activos más valiosos de una organización.

Con ese basamento, se planteó la hipótesis general: "*Las redes virtuales locales (VLAN) influyen positivamente en la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica, es significativa.*" La investigación se sustentó en el estado de arte relacionado con las VLAN, seguridad de información, riesgo, la norma ISO 27001 y recomendaciones establecidas por CISCO.

Para la realización de este estudio se contó con las herramientas metodológicas necesarias para examinar y valorar la pertinencia de instalar VLAN en la situación problemática abordada y la veracidad de los resultados.

Asimismo, se cumplió con la rigurosidad del método científico con coherencia a los principios éticos y políticas administrativas correspondientes. Lo que permitió detectar e interpretar los hallazgos de manera objetiva e interpretar el requerimiento de transformación e innovación.

La presente investigación está organizada en capítulos; el primer capítulo, ***"Redes Virtuales Locales"***, se encausa en presentar cómo las VLAN pueden ser una herramienta favorable para establecer nuevas políticas para el fortalecimiento de la seguridad de la información. Además, esboza la situación problemática. En el segundo capítulo, ***"Fundamentos científicos y teóricos de las Redes Virtuales Locales"*** se describen los componentes de la investigación, antecedentes y el marco teórico usado. El tercer capítulo, ***"Enfoque metodológico VLAN y seguridad de la Información"***, describe la metodología implementada en la investigación, siendo de enfoque mixto, tipo tecnológico y nivel descriptivo explicativo. En el cuarto capítulo, ***"Diseño de Redes Virtuales Locales"***, detalla las metodologías referentes y las fases que se siguieron para el diseño y la implementación de las VLAN. En el quinto capítulo, ***"Fortalecimiento de la Seguridad de Información"***, haciendo uso de la estadística, se estimó el grado de significancia, con respecto de los indicadores planteados para estimar la influencia de las VLAN en la seguridad de la información. Finalmente, en el sexto capítulo ***"Aplicación de las Redes Virtuales Locales"***, se mencionan alcances de la investigación y los nuevos retos para lograr la optimización de la seguridad de información virtual, según los hallazgos demostrados en este estudio.

Los Autores.

Capítulo 1
Redes Virtuales Locales

En el dinámico panorama de internet, la seguridad de la información se ha convertido en una preocupación primordial. Las organizaciones de todos los tamaños buscan proteger sus valiosos datos de accesos no autorizados, amenazas cibernéticas y posibles brechas de seguridad. En este contexto, las Redes Virtuales Locales (VLAN) han surgido como una tecnología fundamental para fortalecer la seguridad de la red y segmentar el tráfico de manera eficiente.

Las VLAN son clave para mejorar la seguridad, la gestión y la asignación de recursos en las redes informáticas. Además, son un concepto fundamental en redes que permite la segmentación de una red física en múltiples redes lógicas, cada una de las cuales opera como una entidad separada. Esta división en segmentos aporta varios beneficios que contribuyen significativamente a la eficiencia, seguridad y capacidad de administración generales de una infraestructura de red.

Una de las principales ventajas de las VLAN es la mejora de la seguridad de la red. Al dividir lógicamente una red en VLAN separadas, las organizaciones pueden aislar datos confidenciales y recursos críticos de otras partes de la red. Este aislamiento ayuda a contener las violaciones de seguridad y limitar el impacto de posibles amenazas cibernéticas. Por ejemplo, en la red de una empresa, separar la VLAN del departamento de finanzas de la VLAN del departamento de marketing garantiza que los datos financieros permanezcan inaccesibles para usuarios no autorizados, lo que reduce el riesgo de violaciones de datos o acceso no autorizado.

Además, las VLAN facilitan una gestión mejorada de la red al permitir a los administradores de red agrupar usuarios según funciones lógicas en lugar de ubicaciones físicas. Esta agrupación permite a los administradores implementar políticas de red, como listas de control de acceso (ACL) y configuraciones de calidad de servicio (QoS), de manera más eficiente en diferentes VLAN. Por ejemplo, la red de un campus universitario puede crear VLAN independientes para estudiantes, profesores y personal administrativo, cada uno con políticas de red específicas adaptadas a sus necesidades. Esta segmentación simplifica las tareas de administración de la red y agiliza los procesos de resolución de problemas al proporcionar una delimitación clara de los segmentos de la red.

En términos de asignación de recursos, las VLAN ofrecen mayor flexibilidad y control sobre los recursos de la red. Al segmentar la red en VLAN, las organizaciones pueden priorizar la asignación de ancho de banda, optimizar el flujo de tráfico de la red y asignar recursos en función de requisitos específicos dentro de cada VLAN. Por ejemplo, una VLAN VoIP se puede configurar para priorizar el tráfico de voz sobre el tráfico de datos para garantizar una comunicación de alta calidad, mientras que una VLAN invitada puede restringir el acceso a ciertos recursos para mantener el rendimiento y la seguridad de la red.

Además, las VLAN admiten la escalabilidad y la expansión de la red al permitir la adición de nuevos dispositivos y usuarios sin la necesidad de una reconfiguración extensa de toda la red. Se pueden crear fácilmente nuevas VLAN para adaptarse al crecimiento o los cambios en los requisitos de la red, proporcionando una solución rentable y eficiente para la expansión de la red.

Las VLAN ofrecen una variedad de beneficios que mejoran la seguridad de la red, la administración de la red y la asignación de recursos en entornos de redes informáticas. Al segmentar las redes en dominios lógicos, las VLAN proporcionan un marco sólido para mejorar la postura de seguridad, simplificar

las tareas de administración de la red, optimizar la utilización de recursos y respaldar la escalabilidad de la red.

En el dinámico panorama de las redes informáticas, la seguridad de la información se ha convertido en una preocupación primordial. Las organizaciones de todos los tamaños buscan proteger sus valiosos datos de accesos no autorizados, amenazas cibernéticas y posibles brechas de seguridad. En este contexto, las Redes Virtuales Locales (VLAN) han surgido como una tecnología fundamental para fortalecer la seguridad de la red y segmentar el tráfico de manera eficiente.

Las VLAN desempeñan un papel importante en la mejora de la seguridad de la red, la gestión de la red y la asignación de recursos en el ámbito de las redes informáticas. Además, son un concepto fundamental en redes que permite la segmentación de una red física en múltiples redes lógicas, cada una de las cuales opera como una entidad separada. Esta segmentación genera varios beneficios que contribuyen significativamente a la eficiencia, seguridad y capacidad de administración generales de una infraestructura de red.

Una de las principales ventajas de las VLAN es la mejora de la seguridad de la red. Al dividir lógicamente una red en VLAN separadas, las organizaciones pueden aislar datos confidenciales y recursos críticos de otras partes de la red. Este aislamiento ayuda a contener las violaciones de seguridad y limitar el impacto de posibles amenazas cibernéticas. Por ejemplo, en la red de una empresa, separar la VLAN del departamento de finanzas de la VLAN del departamento de marketing garantiza que los datos financieros permanezcan inaccesibles para usuarios no autorizados, lo que reduce el riesgo de violaciones de datos o acceso no autorizado.

Además, las VLAN facilitan una gestión mejorada de la red al permitir a los administradores de red agrupar usuarios según funciones lógicas en lugar de

ubicaciones físicas. Esta agrupación permite a los administradores implementar políticas de red, como listas de control de acceso (ACL) y configuraciones de calidad de servicio (QoS), de manera más eficiente en diferentes VLAN. Por ejemplo, la red de un campus universitario puede crear VLAN independientes para estudiantes, profesores y personal administrativo, cada uno con políticas de red específicas adaptadas a sus necesidades. Esta segmentación simplifica las tareas de administración de la red y agiliza los procesos de resolución de problemas al proporcionar una delimitación clara de los segmentos de la red.

En términos de asignación de recursos, las VLAN ofrecen mayor flexibilidad y control sobre los recursos de la red. Al segmentar la red en VLAN, las organizaciones pueden priorizar la asignación de ancho de banda, optimizar el flujo de tráfico de la red y asignar recursos en función de requisitos específicos dentro de cada VLAN. Por ejemplo, una VLAN VoIP se puede configurar para priorizar el tráfico de voz sobre el tráfico de datos para garantizar una comunicación de alta calidad, mientras que una VLAN invitada puede restringir el acceso a ciertos recursos para mantener el rendimiento y la seguridad de la red.

Además, las VLAN admiten la escalabilidad y la expansión de la red al permitir la adición de nuevos dispositivos y usuarios sin la necesidad de una reconfiguración extensa de toda la red. Se pueden crear fácilmente nuevas VLAN para adaptarse al crecimiento o los cambios en los requisitos de la red, proporcionando una solución rentable y eficiente para la expansión de la red.

Las VLAN ofrecen una variedad de beneficios que mejoran la seguridad de la red, la administración de la red y la asignación de recursos en entornos de redes informáticas. Al segmentar las redes en dominios lógicos, las VLAN proporcionan un marco sólido para mejorar la postura de seguridad, simplificar las tareas de administración de la red, optimizar la utilización de recursos y respaldar la escalabilidad de la red.

1.1 Situación problemática

Por todo lo anteriormente mencionado, se visualiza cómo con el uso de la tecnología se está cambiando la forma de hacer las cosas, eliminando las fronteras de tiempo y sobre todo espacio en cada una de las actividades del quehacer diario de las personas, pero se suman nuevas amenazas tecnológicos: ataques masivos a estas infraestructuras de las organizaciones, apoderándose sobre todo de los servidores que contienen las bases de datos de los sistemas implementados. Uno de los ciberataques mundiales fue el registrado el 12 de mayo de 2017, donde un programa malicioso afectó de manera masiva e indiscriminada a empresas de servicios, bancos e instituciones públicas de alrededor de 150 países, desatando una alerta de seguridad sin precedentes.

En este contexto, se plantea establecer redes virtuales locales para fortalecer la seguridad de la información de la Universidad Nacional de Huancavelica. La cual es un organismo público autónomo constituido por profesores, estudiantes y graduados, dedicado al estudio, la formación profesional, promueve investigación científica, la proyección social, comprometida con el desarrollo integral, preferentemente de la Región Huancavelica y de la comunidad nacional; está organizada en nueve facultades y en 21 escuelas profesionales, que funcionan en forma descentralizada; desarrollan actividades académicas de pregrado y posgrado en la provincia de Huancavelica y en sus tres sedes de Pampas, Lircay y Acobamba.

En el Complejo Educativo de Servicios Académicos funcionan la mayor parte de las oficinas administrativas. Para lograr sus fines, tiene implementadas diferentes áreas y oficinas donde los docentes, estudiantes y trabajadores utilizan diversos sistemas de información. Se han clasificado en dos, sistemas de información a nivel WAN y sistemas de información a nivel LAN, a estos sistemas se accede a través de los diferentes aparatos electrónicos que tienen tarjetas de red, y están conectados a la red a los cuales denominamos host. Los

hosts están interconectados a través de una red de comunicaciones, que por ser una red de área amplia (WAN) presenta varios problemas como:

a) Las fichas de observación muestran que el tiempo promedio de acceso a las aplicaciones WAN es 246 milisegundos, evidenciando lentitud en el acceso.

b) El reporte del administrador de redes de la universidad muestra que un 60% de los hosts pierden la conectividad con la red de datos en las sedes de Lircay, Acobamba y Tayacaja entre las 10:00 am y las 2:00 pm, evidenciando los constantes problemas de pérdida de conectividad. Una de las causas es que los usuarios realizan uso indebido del servicio de internet, haciendo descargas, viendo videos, incluso muchos jugando en línea.

c) El reporte de accesos del software académico durante el proceso de matrícula de los últimos dos semestres (2017-II, 2018-I) muestra que, de los 4000 estudiantes de pregrado en el período de matrícula, el 40 % en la sede central y el 80 % en las sedes de Lircay, Acobamba y Tayacaja, realizaron su proceso de matrícula durante la madrugada y/o en la ampliación del período del tiempo programado. Puede atribuirse a varios factores. la congestión del sistema durante las horas pico, que provoca que muchos estudiantes opten por acceder en horarios menos concurridos para evitar problemas de conectividad y lentitud en el acceso a las aplicaciones. Además, la falta de una infraestructura de red robusta y eficiente puede desincentivar a los estudiantes a realizar el proceso de matrícula en horarios regulares, llevando a una mayor concentración de accesos en momentos donde el sistema presenta menor carga. Por último, el comportamiento habitual de los estudiantes que tienden a procrastinar hasta el último momento para completar su matrícula también contribuye a esta tendencia observada.

d) El reporte de casos de pérdida y alteraciones de datos de la Dirección de Tecnologías de la Información y Comunicación en el semestre 2018-I,

muestra la pérdida de datos de 10 días ingresados en los sistemas de gestión documentaria, SIAF, SIGA, debido a la desconfiguración de los servidores.

e) El reporte del personal de soporte informático en el semestre 2018-I, muestra un 60% de equipos infectados de virus, troyanos, spyware, etc., en toda la universidad, afectando la confidencialidad de la información.

La creciente dependencia de la tecnología en la educación ha transformado la manera en que se llevan a cabo las actividades diarias, pero también ha introducido nuevas amenazas cibernéticas que pueden comprometer la seguridad de las infraestructuras organizativas. Un ejemplo notable es el ciberataque del 12 de mayo de 2017, que afectó a empresas y organizaciones en 150 países, subrayando la vulnerabilidad de los sistemas ante ataques masivos. En este contexto, la Universidad Nacional de Huancavelica busca fortalecer la seguridad de su información mediante la implementación de redes virtuales locales (VLAN), lo que permitiría una gestión más efectiva y segura de los datos en sus diversas sedes.

La Universidad Nacional de Huancavelica, compuesta por múltiples facultades y escuelas profesionales, enfrenta desafíos significativos relacionados con su infraestructura de red. Los sistemas de información se clasifican en WAN y LAN, y se han identificado problemas como lentitud en el acceso a aplicaciones WAN (246 milisegundos) y una alta tasa de pérdida de conectividad (60%) en las sedes durante horas pico. Además, el uso indebido del servicio de internet por parte de los usuarios agrava estos problemas, lo que resulta en un impacto negativo en el rendimiento general de la red. La implementación de VLAN podría segmentar el tráfico, priorizando el acceso a aplicaciones críticas y limitando el uso no autorizado.

Para evaluar la efectividad de las VLAN en mejorar la seguridad y el rendimiento de la red, es fundamental establecer métricas claras antes y después de su implementación. Se podrían considerar indicadores como:

Tiempo promedio de acceso a aplicaciones: Medir el tiempo promedio antes y después para determinar mejoras en la velocidad.

Tasa de pérdida de conectividad: Comparar porcentajes antes y después para evaluar si hay una reducción significativa.

Porcentaje de equipos infectados: Evaluar si hay una disminución en la cantidad de dispositivos comprometidos tras la segmentación.

Incidencias reportadas: Analizar cambios en los reportes sobre alteraciones y pérdidas de datos.

Estas métricas proporcionarían un diagnóstico más claro sobre el impacto positivo que las VLAN pueden tener en la seguridad y eficiencia operativa dentro del entorno educativo.

Con base en lo anteriormente expuesto, surge la problemática siguiente: **¿Cuál es la influencia de redes virtuales locales (VLAN) en la seguridad de la información?** De ahí, se deriva:

¿Desarrolla la medición del pre y post del diseño e implementación del modelo de red con redes virtuales locales?

¿Realiza el análisis y determina la influencia en cada una de sus dimensiones, que son disponibilidad, integridad y confidencialidad de la información, aplicado en la red de datos de la Universidad Nacional de Huancavelica?

1.2 Objetivos de la investigación

Objetivo general

Determinar la influencia de redes virtuales locales (VLAN) en la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Objetivos específicos

- Determinar la influencia de las redes virtuales locales (VLAN) en la integridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

- Determinar la influencia de las redes virtuales locales (VLAN) en la disponibilidad de la información en la red de la Universidad Nacional de Huancavelica.

- Determinar la influencia de las redes virtuales locales (VLAN) en la confidencialidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Capítulo 2

Fundamentos científicos y teóricos de las Redes Virtuales Locales

Para comprender plenamente el desarrollo y el propósito de este estudio, es esencial abordar primero los antecedentes investigativos y teóricos que lo sustentan. Estos antecedentes proporcionan un marco de referencia perentorio, que permite situar la publicación en un contexto más amplio y entender las bases sobre las cuales se erige. A través del análisis de investigaciones previas y teorías fundamentales, se pueden apreciar las raíces de las problemáticas abordadas y la evolución de las soluciones propuestas a lo largo del tiempo. De esta manera se subrayan la relevancia y contribución de esta propuesta investigativa al conocimiento existente.

2.1 Antecedentes de la investigación

En el 2015, Martelo en su investigación menciona que un software contribuye en el control de documentos generados a partir del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este software permite recepcionar, administrar y organizar la documentación generada en el proceso de implantación del SGSI. Con esta software se diseña e implementa un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI, produciendo como resultado un módulo para gestión documental que permite el control de documentos durante el proceso de implantación de un SGSI, trabajando bajo procedimientos del estándar ISO 27001, concluyendo que el modelo y la herramienta que lo soporta: permite identificar el estado de los documentos,

previene la utilización de documentos obsoletos, permite la gestión de roles y asignación de actividades, garantiza la disponibilidad, accesibilidad y seguimiento a documentos asignados. Además, permite trabajar bajo procedimientos estrictamente del estándar ISO 27001.

Por su parte, Melchor et al. (2011) analizan el grado de influencia que tiene la seguridad en la administración y calidad de los datos de un sistema de información contable (SIC) en el desempeño organizacional de las pequeñas y medianas empresas (Pyme). Este estudio se llevó a cabo en la región centro del estado de Tamaulipas (México) por medio del análisis correlacional con el software SPSS. Como resultados se muestran el gran impacto que tiene la seguridad en la administración y calidad de la información para obtener una mayor productividad en las empresas.

Asimismo, Tejena-Macías (2018) menciona que la metodología de análisis de riesgos proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información. Luego del estudio realizado en la empresa ECO – VOLTIO que evaluó las diferentes metodologías de riesgo donde el objetivo es el mismo, pero cada una con sus características propias, determina que la metodología MAGERIT resulta ser más efectiva y completa, debido a que protege la información en cuanto a la integridad, confidencialidad y disponibilidad de la información.

Mientras que Luján Vergara y Medina Osorio (2015) en su tesis titulada *"implementación de una red informática hospitalaria, usando metodología top-down network design; para el hospital Chancay y servicios básicos de salud"*. Para ello, modela una red informática hospitalaria moderna, automatizada, con la finalidad de agilizar la transferencia de información (voz, datos, texto, imágenes) entre sus unidades y áreas de trabajo, en beneficio de los usuarios finales, los pacientes. Este modelado lo realiza usando la metodología top-down network design. Para ello, determinaron el estado actual de la red de informática del Hospital

Chancay y Servicios Básicos de Salud; posteriormente, analizaron e identificaron la problemática respecto a la transmisión de información entre sus diversas unidades y áreas, definieron los componentes tecnológicos, determinaron la plataforma de administración de la red que será Windows Server 2012. Como resultado, muestraron que el acceso a la información en promedio es 274.01 segundos y la red propuesta es 63 segundos, disminuyendo 211.01 segundos.

En el mismo orden de ideas, Socualaya (2018), en su tesis "*Diseño de una de red de area local para comunicación de datos del municipio de Iscos"*, tuvo como determinación dar respuesta al problema general de ¿Cómo influye la red de área local para la comunicación de datos en la municipalidad de Iscos?, se planteó el objetivo de determinar la influencia del diseño de red de área local para la comunicación de datos en el municipio de ISCOS, el tipo de investigación es aplicada, con un nivel de estudio explicativo, el diseño de la investigación es pre experimental, el modelo de red se realizó utilizando la metodología de diseño de red "TOP DOWN", de la ingeniera Priscilla Oppenheimer, siendo el universo del estudio y la muestra están conformados por 40 host constituidos en la municipalidad de Iscos – Chupaca, sus resultados muestran que disminuye el tiempo de respuesta del servidor de 52.53 a 30.58 milisegundos en promedio, concluyendo de esta manera la investigación que el diseño de una red de área local influye positivamente en los problemas de comunicación de datos en la municipalidad de Iscos, mejorando significativamente en la eficacia laboral de la Municipalidad.

2.2 Fundamentos teóricos

2.2.1 Información

ISO 27001 define *información* el conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la

forma en que se guarde o transmita (escrita, imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (Normas ISO 27001, 2013, pág. 1).

2.2.2 Seguridad

Proviene de la palabra securitas del latín. La seguridad se define como la ausencia de peligro, daño o riesgo. También puede referirse a la confianza en algo o en alguien. Por tanto, puede tener diversos significados dependiendo del contexto. Por ejemplo, en el ámbito jurídico, la seguridad es la cualidad de ser seguro, libre y exento de todo peligro, daño o riesgo. En el ámbito de la protección, la seguridad es el conjunto de medidas organizativas y de control, personal y medios de seguridad destinados a garantizar la integridad y custodia de recursos humanos y materiales. En el ámbito personal, la seguridad es la confianza en uno mismo y en el propio talento. Se trata de saber, internamente y con serenidad, que eres una persona capaz.

2.2.3 Seguridad de la información

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización (ISO 27001).

Durante los primeros días de las computadoras y su uso, solo había unas pocas amenazas a la protección de la información. Esto se debió principalmente al hecho de que estos dispositivos eran costosos, raros y estaban muy bien protegidos. Los sistemas informáticos que contenían la información solo fueron expuestos a un número limitado de personas con habilidades de programación informática que tenían acceso a la información y podían, esto potencialmente puede ser una amenaza válida. Por lo tanto, el

enfoque inicial para proteger la información consistía en garantizar la fiabilidad del propio sistema, con el fin de garantizar que siempre estaría operativa cuando fuera necesario. Como resultado, la información de la protección se logró principalmente mediante el control del acceso físico a ordenadores.

A medida que disminuyó el costo de la tecnología informática y aumentó su uso, hubo un cambio en el enfoque de la protección de computadoras a la protección de información. Mientras que anteriormente la confiabilidad de las computadoras era dominante, la noción de confidencialidad, integridad y disponibilidad comenzó a ganar importancia. Las raíces de la tríada de la CIA (confidentiality, integrity and availability) están profundamente arraigadas en la mentalidad de seguridad militar, que siempre se ha centrado en proteger la información de amenazas externas. Al principio, existía un vínculo estrecho entre la práctica de la seguridad de la información profesional y el investigador académico o de seguridad de la información, con respecto a lo que consideraban importante para la protección de los activos de información. Según el informe RAND R-609, Security Controls Systems (The Ware Report, 1970) y la planificación de la tecnología de seguridad informática Estudio (The Anderson Report, 1972).

Los Reportes Anderson, encargados por la USAF, identificaron tres categorías de riesgos de seguridad potenciales que eventualmente se convirtieron en la base de la tríada de la confidencialidad, integridad y disponibilidad.

a) Divulgación de información no autorizada: una persona no autorizada puede leer y aprovechar la información almacenada en la computadora. Esta categoría de la preocupación a veces se extiende al "análisis de tráfico", en el que el intruso solo observa los patrones de uso de la información. De esos patrones, el intruso puede inferir algún contenido de

información. Esta categoría también incluye el uso no autorizado de un programa propietario (Confidencialidad).

b) Modificación de información no autorizada: una persona no autorizada puede realizar cambios en la información almacenada, una forma de sabotaje. Se debería notar que, en el caso de este tipo de violación, el intruso no necesariamente ve la información que ha cambiado (Integridad).

c) Denegación de uso no autorizada: un intruso puede impedir que un usuario autorizado refiera o modifique información, aunque el intruso no pueda poder hacer referencia, ni modificar la información por sí mismo (Disponibilidad).

2.2.4 Confidencialidad

El término "confidencialidad" se deriva del verbo latino *confidere*, que significa tener plena confianza. Es un principio fundamental de la seguridad de la información que tiene sus raíces en la mentalidad militar de mantener una autoridad y control sobre aquellos que tienen acceso a la información, sobre la necesidad de conocer la base (Spagnoletti, 2007). En este contexto, Camp (1999) postula que la confidencialidad implica la noción de que los datos y la información representada por tales datos deben estar protegidas; de tal manera que su uso se limita a fines autorizados por personas autorizadas únicamente. Del mismo modo, Zwick y Dholakia (2004) definen la confidencialidad como la capacidad percibida para llevar a cabo una tarea externa que restringe el flujo de información con respecto a lo que se divulga en él, y a quién llega a verlo. Estos aspectos de la confidencialidad también se reflejan en documentos oficiales del gobierno y legislación. En la Sección 3542 del Título 44 del Código de los Estados Unidos, la confidencialidad se conoce como la "restricción autorizada de acceso y divulgación de información, incluidos los medios para proteger privacidad e información de propiedad".

2.2.5 Integridad

Spagnoletti (2007), define desde un punto de vista etimológico, la palabra "integridad" significa *solidez, integridad* y se deriva de la palabra latina tangere, que significa "tocar". El prefijo 'in' indica una fuerza negativa o privativa, y por lo tanto el significado de la palabra "integridad" se puede asociar con ciertas connotaciones de la palabra "intocable" que, a su vez, está relacionada con el concepto de integridad ética. A este respecto, las cuestiones de ética y responsabilidad, que se consideran principios clave de seguridad.

La investigación en seguridad de la información ha estudiado la ética desde muchos puntos de vista diferentes. Por ejemplo, Gattiker y Kelley (1999) estudiaron las diferencias en las actitudes y la moral de los usuarios y juicios con respecto al comportamiento ético relacionado con la informática. Por su parte, Cardinali (1995) sugiere que la legislación estatal y federal se utilice como salvaguardas contra la falta de ética en el comportamiento. En líneas similares, Harrington (1996) recomienda que, ante la aplicación de códigos y políticas y la comunicación de sanciones, se pueda dispensar rápidamente al personal moroso. Mientras que Sipior y colaboradores (2005) argumentan que la formación y la concienciación sobre la seguridad informática es una forma de defenderse de los comportamientos poco éticos.

Para Spagnoletti (2007), la palabra "disponibilidad" proviene del latín valere, que significa "valer". En seguridad de la información, el término disponibilidad significa "acceso y uso oportunos y confiables de información"; esto implica los aspectos que pertenecen a la usabilidad de los sistemas. Desde una perspectiva de ingeniería de usabilidad, un sistema es considerado utilizable cuando es eficaz y eficiente, y sus usuarios son generalmente satisfechos con su desempeño de tareas específicas dentro de un determinado entorno (Weir et al., 2009). En el caso del software de seguridad, Padayachee (2012) cita a Whitten y Tygar (1999) al señalar que la usabilidad también se

asocia con la capacidad de evitar errores peligrosos y hacer que los usuarios sean conscientes de forma fiable de las tareas que necesitan realizar.

2.2.6 ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO), que describe: "*Cómo gestionar la seguridad de la información en una empresa. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada con base en la norma británica BS 7799-2. Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.*"

Su eje central es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Para lograrlo, se investiga cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego se define qué es necesario hacer para evitar que estos problemas se produzcan (mitigación o tratamiento del riesgo). Podemos afirmar entonces que la filosofía principal de la norma ISO 27001 se desarrolla con base en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente (Figura 1).

Figura 1. *Estructura ISO 27001*

Cuando se realiza la implementación de ISO 27001, por lo general, se determina reglas organizacionales e implementación técnica de software y equipos que prevengan la violación de seguridad. Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc. ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI). Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc. Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa; hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información (ISO 27001, 2013).

2.2.7 Riesgos

La ISO 27001 define *riesgos* como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo. Mientras que el riesgo tecnológico es la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños (ISO 27001, 2013).

De acuerdo a la definición, se puede afirmar que cualquier evento que afecte al funcionamiento total de la empresa es considerado un riesgo o amenaza para la entidad (Figura 2). La ISO 27001 es fundamental para las organizaciones porque proporciona un marco integral para gestionar los riesgos relacionados con la seguridad de la información. Al seguir esta norma, las empresas pueden identificar y evaluar amenazas y vulnerabilidades, implementar controles adecuados y tomar decisiones informadas para mitigar los riesgos.

Figura 2. *Gestión del riesgo*

Tipos de amenazas a la seguridad. Aquellas que son vulnerables en las organizaciones se visualizan en la Figura 3.

Amenazas humanas, como su nombre lo indica, son aquellas acciones provocadas por el hombre y pueden ser de dos tipos: maliciosas y no maliciosas.

- **Maliciosas** son aquellas que se llevan a efecto con el propósito de causar daño a la organización. Estas pueden ser:

  a) **Externas:** pueden afectar al desarrollo de las actividades de las organizaciones, frecuentemente originadas por el acceso a internet, el cual trae una serie de peligros como son los virus, hackers, entre otros. Al ser infiltrados en la red interna de la organización, puede provocar daños como mal funcionamiento de los sistemas y pérdida de información.

  b) **Internas:** más frecuentes son las originadas por los propios empleados y ex empleados de la organización por diferentes motivos.

♦ **No maliciosas** este tipo de amenazas son producidas en la mayoría de los casos por errores ocasionados por empleados que no cuentan con el conocimiento o adecuada capacitación en el manejo de equipos y sistemas.

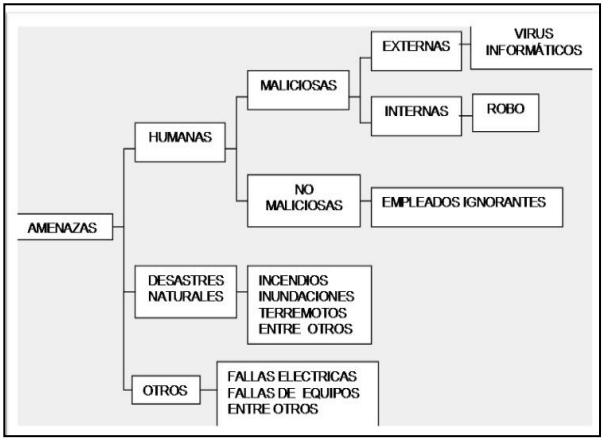


Figura 3. *Tipos de amenaza a la seguridad*

Amenazas por desastres naturales estas amenazas originadas por la naturaleza son las menos frecuentes en las organizaciones, pero aun así no podemos dejar de considerarlas.

Otras amenazas son aquellas referentes a las que están fuera del alcance del hombre, como son las interrupciones eléctricas, fallas de equipos originadas por los cortes de energía o no mantenerlos en el ambiente adecuado, aunque esta es una responsabilidad más bien de carácter humano; entre otros (Dulaney, 2011).

2.2.8 Modelo de redes jerárquicas

De acuerdo a la academia de networking de Cisco Systems, para que la construcción de una red de área local satisfaga las necesidades de organizaciones pequeñas o medianas, el modelo de diseño de red jerárquico

tiene más probabilidades de ser exitoso. Luego de un análisis comparativo con otros diseños de redes, las redes jerárquicas se pueden administrar y expandir con más facilidad, permitiendo resolver los problemas con mayor rapidez.

La metodología de diseño de redes jerárquicas está basada en la división de la red en capas independientes, donde cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico (Figura 4) se separa en tres capas: capa de acceso, capa de distribución y capa núcleo (CISCO, 2007).

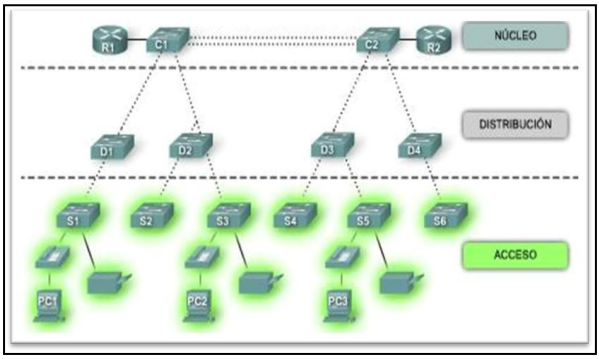


Figura 4. *Modelo de diseños de redes jerárquicas.*

Capa de acceso. En el modelo de red jerárquica, la capa de acceso está compuesta por los equipos de comunicación que interconectan a los hosts (dispositivos electrónicos finales como las computadoras de escritorio, laptops, celulares, impresoras, teléfonos IP, etc.) con el resto de la red (Figura 5). Su propósito es aportar un medio de conexión de los dispositivos a la red y controlar la comunicación de cada uno de estos en la red. En esta capa de acceso se pueden utilizar routers, switches, puentes, hubs y puntos de acceso inalámbricos (CISCO, 2007).

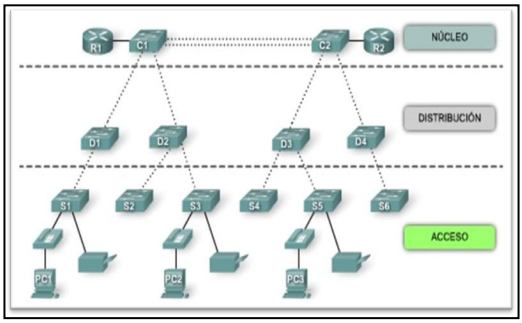


Figura 5*. Capa de acceso según el modelo de redes jerárquicas*

Capa de distribución. Esta de distribución está compuesta por los switches que interconectan los equipos de la capa de acceso con los equipos de comunicación de la capa núcleo; su propósito es controlar el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las VLAN definidas en la capa de acceso. Estas permiten al administrador segmentar el tráfico sobre un switch en subredes separadas; los switches de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad (CISCO, 2007). Se observa en la Figura 6 la separación del tráfico en la red asignada a profesores, estudiantes y visitantes.

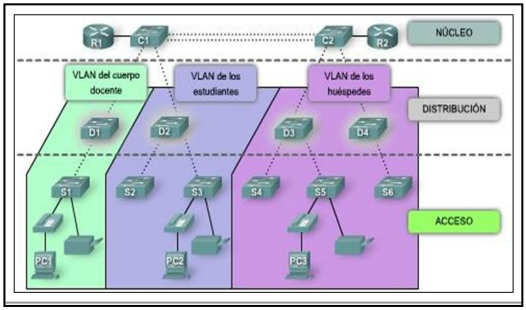


Figura 6. *Capa de distribución según el modelo de redes jerárquicas*

Capa núcleo. En el diseño jerárquico, la capa núcleo es la que administra todo el tráfico generado, también lo conocido como backbone de alta velocidad de la red. Esta capa es esencial para la interconectividad entre los dispositivos de la capa de distribución; es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto, debe poder reenviar grandes cantidades de datos rápidamente (Figura 7) (CISCO, 2007).

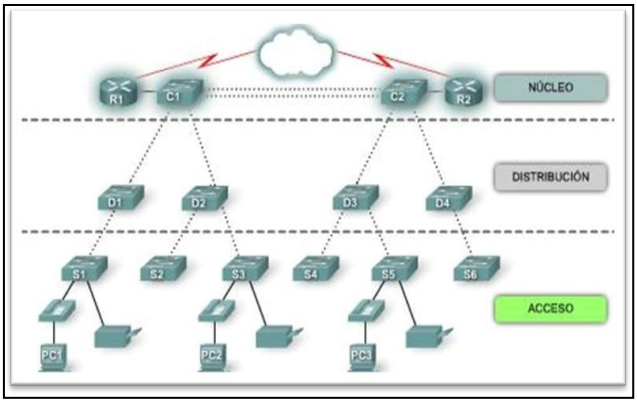


Figura 7. *Capa de núcleo según el modelo de redes jerárquicas*

2.2.9 Redes Virtuales Locales (VLAN)

La VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física; es una división lógica del dominio de broadcast a nivel de la capa dos del modelo OSI. Es una agrupación lógica de dispositivos que se pueden comunicar entre sí. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. También permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Asimismo, admite que un administrador de red

cree grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Mediante las VLAN, puede segmentar de manera lógica las redes conmutadas basadas en equipos de proyectos, funciones o departamentos. En la Figura 8, se crea una VLAN para los estudiantes y otra para el cuerpo docente. Estas VLAN permiten que el administrador de la red implemente políticas de acceso y seguridad para grupos particulares de usuarios. Una política puede ser permitir que el cuerpo docente, pero no los estudiantes, obtenga acceso a los servidores de administración de e-learning para desarrollar. materiales de cursos en línea (CISCO PRESS, 2017).

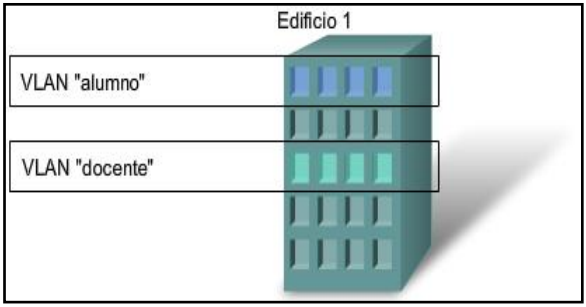


Figura 8. *Redes virtuales locales independientes*

A continuación, se definen algunos beneficios que brinda una VLAN, los cuales son mostrados en la Figura 9 (CISCO (2017):

- **Seguridad:** se independiza a todos los hosts que transmiten datos sensibles de la organización al ubicarlos en una red virtual independiente, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

- **Reducción de costos:** los costos se reducen porque no es necesario implementar más hardware para mejorar el ancho de banda y administrar el tráfico, debido a que las redes virtuales locales (VLAN), por ser independiente,s

solo transmiten datos entre los miembros de la red virtual, disminuyendo considerablemente el tráfico y ruido generado cuando todos los hosts están en la misma red; sobre todo mejora el uso eficiente del ancho de banda existente.

♦ **Mejor rendimiento:** la división en múltiples grupos lógicos de trabajo a través de los dominios de broadcast en la capa 2 reduce el tráfico innecesario en la red y potencia el rendimiento.

♦ **Mitigación de la tormenta de broadcast:** el dividir una red en redes virtuales locales (VLAN) impide que una tormenta de broadcast se propague a toda la red, reduciendo el número de dispositivos que puedan participar en una tormenta de broadcast.

♦ **Mayor eficiencia del personal de TI:** las redes virtuales locales permiten agrupar a los usuarios con requerimientos similares de red, facilitando su administración a través de políticas y procedimientos por VLAN y no por host.

♦ **Administración de aplicación o de proyectos más simples:** las redes virtuales locales permiten agregar hosts y usuarios de manera sencilla, considerando los requerimientos geográficos o comerciales.

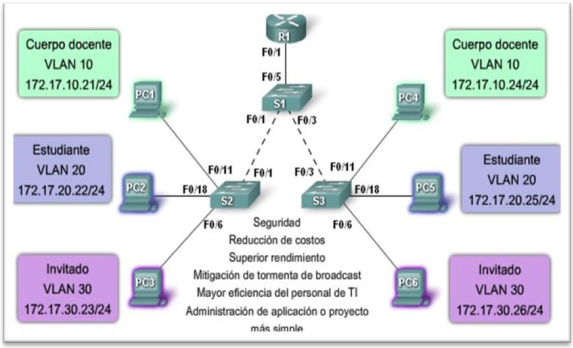


Figura 9. Beneficios de las VLAN

2.2.10 Clasificación de VLAN

Según CISCO Press 2017, las redes virtuales locales se clasifican de acuerdo al tipo de datos que transmiten, a continuación, se describe algunas de ellas:

- **VLAN de datos.** VLAN configurada solo para enviar tráfico de datos generado por el usuario.
- **VLAN predeterminada.** Es la VLAN 1; todos los puertos pertenecen a esta VLAN, cuando un switch se inicia por primera vez.
- **VLAN de administración.** VLAN que se configura para acceder a las capacidades administrativas de un switch.
- **VLAN de voz.** Configurada para admitir la voz sobre IP (VoIP).
- **LAN VTP.** Protocolo de trunking VLAN (VTP) creado para resolver los problemas operativos en una red conmutada con VLAN (Figura 10).

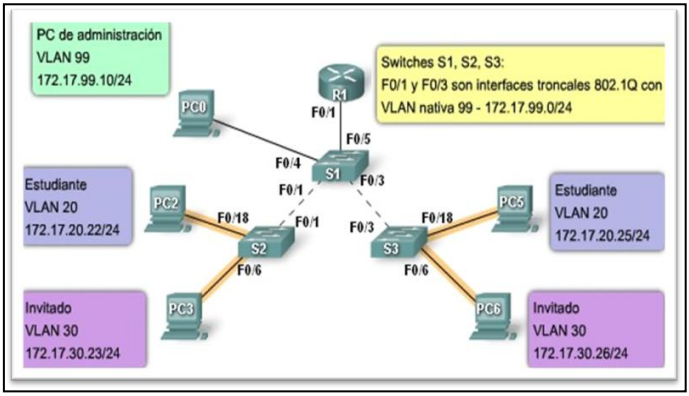


Figura 10. Protocolo de trunking VLAN (VTP)

2.2.11 Metodología James McCabe - CISCO de diseño de redes

El estudio en el diseño de red tiene como base la metodología propuesta por James McCabe en su libro "*Practical Computer Network Analysis and Design"* y lo combina con la metodología top – down utilizada por CISCO. Seguidamente se describe:

- **Fase 1: Diagnóstico.** Se realiza la descripción detallada de la infraestructura de red de comunicaciones actual, también la verificación de la documentación sobre la infraestructura física (planos) y documentación lógica de la red (descripción del funcionamiento); luego se evalúa si la infraestructura de comunicaciones cumple con los estándares internacionales.

- **Fase 2: Análisis.** Se lista todas las áreas que funcionan en la infraestructura (campus, edificio u otro), determinando la cantidad de host que funcionan en cada área. Además, se determina la ubicación de cada host en planos, describiendo las actividades de interacción de cada usuario según su función con la red. Asimismo, se describen las aplicaciones informáticas a nivel LAN y WAN utilizadas por cada host; listar los sistemas de comunicación a implementar, describiendo cada uno de los sistemas de comunicaciones a implementar, definiendo los requerimientos de red y la realización del análisis de requerimiento de ancho de banda LAN y WAN.

- **Fase 3: Diseño.** Se realiza el diseño físico y el diseño lógico de la infraestructura de comunicaciones.

  a) **Diseño físico.** Diseñar la infraestructura de comunicaciones a nivel físico, considerando lo siguiente:

  - Determinar la cantidad de hosts por área, oficina, o ambiente.
  - Realizar el plano de ubicación de host.

- Evaluar y determinar los medios de transmisión.
- Diseñar los planos de cada sistema a implementar.
- Realizar el diseño de cableado estructurado.
- Evaluar y determinar los equipos de comunicación.

b) **Diseño lógico.** Evaluar y diseñar la infraestructura lógica de la infraestructura de comunicaciones. Considerando:

- Realizar la identificación de los equipos (host) a comunicar por cada sistema a implementarse.
- Realizar el mapa de aplicaciones a nivel LAN y a nivel WAN.
- Identificar y determinar los servicios de comunicaciones que se desean implementar.
- Diseñar las redes virtuales de área local (VLAN).
- Evaluar y realizar la asignación de direcciones IP V4 para cada host.
- Evaluar y elegir los protocolos de administración a nivel LAN.
- Determinar tabla y protocolos de enrutamiento
- Determinar los protocolos para soportar los servicios a implementarse.
- Determinar las políticas de seguridad de la red de datos.
- Generar las listas de acceso.
- Evaluar y diseñar la infraestructura lógica de la red de datos.

♦ **Fase 4: Implementación.** Construir la infraestructura de comunicaciones de acuerdo al diseño.

♦ **Fase 5: Operación.** La infraestructura de comunicaciones es puesta en marcha, monitoreada. Esta fase es la prueba máxima del diseño.

♦ **Fase 6: Optimización.** En esta fase, se detectan y corrigen errores, además de que se realizan nuevas actualizaciones de acuerdo a las necesidades.

El diseño de VLAN (Redes de Área Local Virtual) es fundamental para la segmentación y gestión eficiente de redes, y existen diversas metodologías que se pueden aplicar. Entre ellas, destaca el modelo top-down de Cisco, que se contrapone a enfoques más tradicionales. A continuación, se presenta un análisis comparativo de estas metodologías.

Modelo Top-Down de Cisco

El modelo top-down de Cisco se basa en una planificación y diseño que comienza desde la capa superior de la red hacia abajo. Este enfoque implica:

Análisis de Requerimientos: Se inicia con un estudio exhaustivo de los requerimientos del negocio y las necesidades de los usuarios, lo que permite identificar claramente las aplicaciones y servicios críticos.

Diseño Lógico: A partir del análisis, se desarrolla un diseño lógico que incluye la creación de VLANs basadas en funciones o grupos de usuarios, asegurando que la segmentación responda a las necesidades operativas.

Implementación Gradual: La implementación se realiza en fases, permitiendo ajustes y optimizaciones en cada etapa, lo que facilita la adaptación a cambios en el entorno o en los requisitos.

Este enfoque permite una mayor alineación entre la infraestructura de red y los objetivos del negocio, además de facilitar la escalabilidad y el mantenimiento.

Enfoques Tradicionales

Por otro lado, los enfoques tradicionales suelen seguir un modelo bottom-up, donde el diseño comienza desde la infraestructura existente. Este método implica:

Configuración Directa: Se asignan VLANs a puertos específicos sin un análisis profundo de las necesidades organizativas. Esto puede llevar a una segmentación ineficaz.

Limitada Flexibilidad: Dado que las configuraciones son estáticas, cualquier cambio en la estructura organizativa o en las necesidades del usuario requiere reconfiguraciones significativas.

Dificultad para Escalar: A medida que la red crece, puede volverse complicada y difícil de gestionar debido a la falta de un diseño lógico claro.

Este enfoque puede resultar en una red subóptima donde las VLANs no reflejan adecuadamente la estructura organizativa ni las necesidades operativas.

Finalmente, el modelo top-down de Cisco ofrece una metodología más estructurada y alineada con las necesidades modernas, mientras que los enfoques tradicionales pueden ser menos efectivos para gestionar redes complejas y cambiantes (Tabla 1). La elección del enfoque adecuado dependerá de las características específicas de cada organización y sus objetivos estratégicos.

Tabla 1. *Comparación de metodologías de diseño de VLAN: Modelo Top-Down de Cisco vs. Enfoques tradicionales*

Aspecto	Modelo Top-Down (Cisco)	Enfoques Tradicionales
Inicio del Diseño	Desde los requerimientos del negocio	Desde la infraestructura existente
Flexibilidad	Alta; permite ajustes según necesidades cambiantes	Baja; requiere reconfiguración para cambios
Escalabilidad	Alta; diseñado para crecer con el negocio	Limitada; puede volverse complicada
Eficiencia	Optimiza el uso de recursos y segmentación	Puede resultar en una segmentación ineficaz
Implementación	Gradual y adaptativa	Directa y rígida

Capítulo 3

Enfoque metodológico VLAN y seguridad de la Información

3.1 Método específico de investigación

3.1.1 Tipo de investigación

Por el desarrollo de la naturaleza de las variables de estudio, la investigación se ubicó dentro del tipo de investigación aplicada, llamado también utilitaria o tecnológica, cuyo objetivo fue determinar la influencia del modelo de red con redes virtuales locales en la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica, 2018. En concordancia con lo referido por Sánchez, 2017: "*la investigación aplicada tiene por objetivo la generación de conocimiento con aplicación directa y a mediano plazo en la sociedad o en el sector productivo; este tipo de estudios presenta un gran valor agregado por la utilización del conocimiento que proviene de la investigación básica*" (Sanchez Carlesi, 2017, pág. 41).

3.1.2 Nivel de la investigación

Según los objetivos de la investigación y el tipo de problemas planteados, tiene nivel de investigación descriptivo-explicativo. Al respecto, Sánchez y Reyes (2017) afirman: "*las investigaciones descriptivas consisten fundamentalmente en describir un fenómeno o una situación mediante el estudio del mismo en una circunstancia témpora – espacial determinada*"; además, es explicativo, basado en que "*nos permitirá explicar tentativamente la ocurrencia de un fenómeno*" (Sanchez Carlesi, 2017, pág. 45). Por tanto, en la realización de esta investigación se consideraron los datos provenientes de los distintos campus universitarios, facultades y oficinas que

transmiten información; asimismo, se realizó el análisis de disponibilidad, integridad y confidencialidad de la información en un pre y postanálisis.

3.1.3 Métodos

- **Método general**, basado en el método científico, debido a que, a través de sus procedimientos, permitió el análisis de los datos, comprobación de hipótesis, discusión de los resultados que permitió establecer conclusiones y recomendaciones, de acuerdo a lo que plantea Tamayo (1999) "*El método científico es un procedimiento para descubrir las condiciones en que se presentan sucesos específicos, caracterizado generalmente por ser tentativo, verificable, de razonamiento riguroso y observación empírica*" (p. 28), exigencias que se han seguido en la presente investigación.

- **Métodos particulares**, como cimientos metodológicos específicos, fueron los siguientes:

  - **Método experimental**, debido a que se organiza deliberadamente las condiciones, "*con el fin de investigar las posibles relaciones causa-efecto del problema en estudio*", exponiendo al grupo total a la acción de una variable experimental que son redes virtuales locales y "*contrastando sus resultados del pre y post*" (Sanchez Carlesi, 2017, pág. 67).

  - **Método de observación**, este método fue útil para percibir las características de la red respecto a disponibilidad, integridad y confidencialidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

  - **Método descriptivo**, en el estudio, este método permitió detallar las características técnicas de la transmisión de información en la red de datos de la Universidad Nacional de Huancavelica.

3.1.4 Diseño de investigación

Para la contratación de hipótesis, el diseño experimental se realizó con un solo grupo con Pretest y Postest, cuyo esquema es el siguiente:

$$M: \quad O_1 \rightarrow X \rightarrow 0_2$$

Donde:

M: Muestra

O_1: Seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica (sin VLAN)

O_2: Seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica (con VLAN)

X: Redes Virtuales Locales (VLAN)

3.2 Población y muestra

3.2.1 Población

En el caso particular, se cuantificaron los hots que componen la red de datos de la Universidad Nacional de Huancavelica, los cuales son 1320, lo que representaría el número total o población a intervenir.

3.2.2 Muestra

Para validar la situación problemática planteada, se trabajó con 140 hosts de la red de datos de la universidad. El muestreo fue probabilístico estratificado, diseñado para abarcar los seis campus universitarios, donde se definen claramente las áreas de trabajo y oficinas. Se seleccionó un host de cada oficina y de cada tipo de usuario, incluyendo administrativos, docentes y estudiantes. La distribución quedó así: campus universitario de Acobamba 20, Lircay 20, Daniel

Hernández 20, Pampas 20, edificio administrativo 30 y campus universitario de Paturpampa 30.

Para el análisis del tráfico y la validación de datos en esta red, se utilizaron herramientas como Wireshark y NetFlow. Wireshark es un analizador de protocolos que permite capturar y visualizar en tiempo real todos los paquetes que circulan por la red, facilitando la identificación de problemas y el comportamiento del tráfico13. Esta herramienta ofrece filtros personalizados que permiten enfocarse en paquetes específicos, lo que es crucial para un análisis detallado45. Por otro lado, NetFlow proporciona información sobre el flujo de datos en la red, permitiendo un análisis más profundo del rendimiento y la utilización del ancho de banda37. Ambas herramientas fueron fundamentales para obtener una visión clara del estado actual de la red y para identificar áreas que requieren atención o mejora.

3.3 Variables: definición operacional

Variable dependiente: Seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Variable independiente: Redes Virtuales Locales LAN.

Operacionalización de variables (Tabla 2):

Y= F(X)

Variable dependiente

Y= Seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Variable independiente

X = Redes Virtuales Locales LAN.

Tabla 2. *Matriz de operacionalización de variables*

VARIABLES	OPERACIONALIZACION			
	DIMENSIONES	INDICADORES	TÉCNICA DE RECOLECCIÓN DE DATOS	INSTRUMENTO
REDES VIRTUALES LOCALES VLAN redes lógicas independientes dentro de una misma red física.	✓ 0 = sin presencia de las redes virtuales locales VLAN. ✓ 1 = con presencia de redes virtuales locales VLAN		Observación	• Fichas de observación. • Lista de cotejo • Entrevistas • Encuestas
SEGURIDAD DE LA INFORMACION La seguridad de la información, según (Normas ISO 27001, 2013), "consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización".	1. Disponibilidad de la información en la red de datos.	1.1 Tiempo de respuesta a nivel LAN de la Red. 1.2 Tiempos de respuesta nivel WAN de la Red 1.3 Tasa de Transferencia a nivel LAN 1.4 Tasa de Transferencia a nivel WAN 1.5 N° de servicios ofrecidos por la red.	Observación	• Fichas de observación. • Lista de cotejo • Entrevistas • Encuestas
	2. Integridad de la información en la red de datos.	2.1 N° de casos de alteraciones - perdida de datos.		
	3. Confidencialidad de la información en la red de datos	3.1 % de accesos a servicios no autorizados a nivel LAN. 3.2 % de accesos a servicios no autorizados a nivel WAN.		

3.4 Hipótesis

Hipótesis general.

Las redes virtuales locales (VLAN) influyen positivamente en la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Hipótesis específicas

H_1: Las redes virtuales locales (VLAN) influyen positivamente en la integridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

H_2: Las redes virtuales locales (VLAN) influyen positivamente en la disponibilidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

H_3: Las redes virtuales locales (VLAN) influyen positivamente en la confidencialidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

3.5 Técnicas e instrumentos de recopilación de datos

Tomando en cuenta lo señalado por Ñaupas Paitan (2018), quien refiere que las "*técnicas e instrumentos de investigación se refieren a los procedimientos y herramientas mediante los cuales vamos a recoger los datos e informaciones necesarias para probar o contrastar nuestras hipótesis de investigación*" (p. 201). En el estudio se utilizó como técnica la entrevista, con el objeto de recabar los datos necesarios de los trabajadores de la dirección de tecnologías de información y comunicación, así como de los responsables del sistema académico. Asimismo, se empleó la observación directa, técnica que sirvió para la recopilación de datos de los indicadores de las tres dimensiones de la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica en el pre y post implementación de redes virtuales locales.

3.6 Instrumentos de recopilación de datos

Se emplearon dos instrumentos, los cuales fueron validados a juicio de expertos, denominados técnica de recolección de datos y herramientas informáticas de medición. Con la **ficha técnica de recolección de datos** se recopilaron las mediciones de cada indicado por herramienta informática respectiva, fue validado por juicios de expertos en la materia de seguridad de la información, de manera que los indicadores correspondan a las variables y dimensiones del estudio. El coeficiente de validez promedio es de 0.91; de acuerdo al criterio de los jueces, los cuatro recomiendan su aplicabilidad (Tabla 3).

Tabla 3. *Validación de ficha técnica de recolección de datos*

Juez	Universidad	Coeficiente de validez
Dr. Juan Jesus Arenas Iparraguirre	Pontificie Universidad Javeriana de Bogota	1
Dr. Jose Luis Risco Becerra	Universidad de Sao Paulo	0.72
Dr. Jose Manuel Armada Pacheco	Universidad Nacional de Huancavelica	0.96
Dr. Alex Sandro Landeo Quispe	Universidad Peruana los Andes	0.96
Promedio		**0.91**

Para el instrumento denominado **herramientas informáticas de medición**, se emplearon la ventana de comandos del sistema operativo y el software Wireshark, en concordancia con las recomendaciones de la Unión Internacional de Telecomunicaciones, en las categorías de calidad de servicio para los usuarios de extremo de servicios multimedia (G.1010, aprobada en el año 2001), la cual se encuentra vigente UIT-T G.1010 y la IEEE. Por tanto, la ventana de comandos de sistema operativo se utilizó para medir la dimensión disponibilidad de la información:

- **Indicador 1.1:** Tiempo de respuesta a nivel LAN, unidad de medida milisegundos.
- **Indicador 1.2:** Tiempo de respuesta a nivel WAN, unidad de medida milisegundos.

Mientras que el software Wireshark, se utilizó para medir la dimensión disponibilidad de la información, considerando los siguientes indicadores:

- **Indicador 1.3:** Tasa de transferencia LAN, unidad de medida megabits por segundo (Mbps).
- **Indicador 1.4:** Tasa de transferencia WAN, unidad de medida megabits por segundo (Mbps).

Asimismo, se consideraron para la medición dimensión integridad de la información:

- **Indicador 3.1:** Porcentaje de accesos a servicios no autorizados a nivel LAN unidad paquetes de datos.
- **Indicador 3.2:** Porcentaje de accesos a servicios no autorizados a nivel WAN unidad paquetes de datos.

El análisis de los datos se llevó a cabo de manera sistemática, organizando la información a través de la estadística descriptiva, que permitió presentar los resultados de las mediciones de cada indicador en tablas claras y comprensibles.

Se calcularon las medidas de tendencia central, como la media aritmética, mediana y moda, así como las medidas de dispersión, que incluyen la desviación estándar, rango y varianza. Estos cálculos son esenciales para entender la distribución de los datos y detectar patrones que puedan influir en el diseño de la red.

Además, se aplicó la estadística inferencial para determinar parámetros que respaldan decisiones más amplias sobre el diseño de la infraestructura. Para este propósito, se utilizaron herramientas estadísticas como SPSS y Excel, que facilitaron el procesamiento y análisis de grandes volúmenes de datos.

La interpretación de los resultados se realizó mediante un enfoque hermenéutico, utilizando un lenguaje accesible que permite a la comunidad científica comprender fácilmente los hallazgos del trabajo de investigación. Este enfoque no solo ayuda a comunicar los resultados, sino que también justifica las decisiones tomadas en el diseño, asegurando que estén fundamentadas en datos sólidos.

Finalmente, se utilizó una herramienta de simulación del modelo de red para representar visualmente la topología de la red de datos con redes virtuales locales antes de su implementación. Esta simulación es crucial, ya que permite evaluar diferentes escenarios y optimizar el diseño propuesto, garantizando que las decisiones tomadas no solo sean teóricas, sino también prácticas y efectivas en la mejora del rendimiento y la eficiencia de la red.

Capítulo 4

Diseño de Redes Virtuales Locales

4.1 Diseño de redes virtuales locales

Con la intención de resolver la situación problemática planteada, se diseñó las VLAN que permiten dividir una red física en múltiples redes lógicas, lo que mejora la gestión y la seguridad al separar diferentes grupos de usuarios o dispositivos. Al agrupar dispositivos según su función o ubicación, se pueden definir políticas de tráfico específicas para cada VLAN, reduciendo la congestión de la red y mejorando la velocidad de transferencia de datos. De esta manera, limitar el acceso a recursos de red específicos, reduciendo el riesgo de ataques y accesos no autorizados.

El diseño de la infraestructura de comunicaciones con VLAN se desarrolló utilizando la metodología propuesta por James McCabe, "*Practical Computer Network Analysis and Design*" y la metodología top –down de CISCO. Para ello, se siguieron las siguientes fases:

4.1.1 Fase de diagnóstico

La descripción de la ciudad de Huancavelica se refleja en la tabla 3, tiene un campus universitario donde funcionan las diferentes facultades con sus escuelas profesionales, algunas oficinas como biblioteca, archivo central, almacén, comedor, videoconferencia, auditorio general, residencia estudiantil, distribuidos en diferentes pabellones. En el centro de la ciudad se encuentra el edificio administrativo donde funciona la gran mayoría de sus oficinas administrativas.

Los edificios y pabellones fueron construidos sin considerar los ductos, canalizaciones de las redes de datos y comunicación. Las redes de datos se implementaron sobre la infraestructura, paredes, techos y a través de canaletas de forma artesanal, sin ningún tipo de planificación, mucho menos diseño (Figura 11).

Figura 11*. Fotografía diagnóstica de la situación previa en el área a intervenir*

Se solicitó la documentación correspondiente acerca de la infraestructura física de la red de datos, verificándose la inexistencia de la misma; no se tiene ningún documento de cómo está instalado físicamente y mucho menos la distribución física de la red de datos.

De igual manera se procedió a la solicitud de datos; documentando la infraestructura lógica de la red, evidenciándose situación similar a lo anteriormente señalado.

Finalmente, se realizó la evaluación de la instalación física y la distribución de la red de datos; se puede determinar que no se tuvo en cuenta ningún tipo de estándar internacional, como en este caso el de cableado estructurado. También se precisa que no existe ningún tipo de configuración

lógica, por ende, no existe ningún tipo de seguridad, entonces no cumple con ningún estándar de calidad de servicio y seguridad (Tabla 4).

Tabla 4. *Distribución por pabellón universitario del número de host por pabellón universitario*

Ciudad	Lugar	infraestructura	N° de host
Huancavelica	Centro ciudad	Edificio administrativo	340
	Campus universitario	Pabellón derecho	50
		Pabellón educación	50
		Pabellón de ingeniería	55
		Pabellón ingeniería civil	25
		Pabellón enfermería	60
		Pabellón obstetricia	60
		Pabellón ciencias administrativas	70
		Pabellón video conferencia	60
		Biblioteca	40
		Pabellón auditorio general	20
		pabellón comedor - bienestar	20
		pabellón almacén - mantenimiento obras	30
		Pabellón archivo central	10
		Residencia universitaria	30
Pampas	Campus universitario Pampas	Pabellón facultad FIES	20
		Pabellón de electrónica	60
	Campus universitario Daniel Hernández	Pabellón sistemas	110
		Residencia universitaria	20
Lircay	Campus universitario	pabellón facultad Minas-Civil	20
		Pabellón minas	30
		Pabellón civil	30
		Residencia universitaria	20
Acobamba	Campus universitario	Pabellón facultad Ciencias Agrarias	10
		Pabellón Agronomía	30
		Pabellón agroindustrias	30
		Residencia universitaria	20
total			**1320**

4.1.2 Fase de análisis

La Universidad Nacional de Huancavelica (UNH) es una entidad educativa de enseñanza superior que opera en el sistema universitario nacional, con un modelo de enseñanza referido al conocimiento científico y tecnológico acorde a nuestra realidad. Para tal propósito cuenta con 20 carreras profesionales en los campos de la educación (5 especialidades), las ingenierías (9

especialidades), Ciencias Administrativas (3 especialidades), Ciencias de la salud (2 especialidades) y Derecho (una especialidad); siendo débil aún, el desarrollo de competencias genéricas, que actualmente se ha puesto en práctica en las principales universidades acreditadas a nivel mundial.

La UNH desarrolla sus actividades académicas de pregrado, principalmente de manera concentrada en la provincia de Huancavelica y en sus tres sedes de Pampas, Lircay y Acobamba; en tanto que, a nivel de postgrado lo desarrolla en la provincia de Huancavelica en sedes descentralizadas (Lircay, Huancayo, Chincha, Coracora y Jauja). En este centro de estudios, su proceso de expansión tecnológico está en función del desarrollo nacional en TIC.

La UNH desarrolla sus actividades académicas de manera autónoma, siendo aún débil el desarrollo conjunto con otras universidades a través de alianzas estratégicas; así a nivel mundial, opera con otras universidades a través de la suscripción de convenios, mediante el desarrollo de la cooperación internacional. En esta modalidad se participa con becas para seguir los estudios de postgrado (maestría y doctorado) y en el intercambio recíproco de profesores en los campos académico y de investigación.

Como **Misión:** *"Universidad formadora de profesionales competitivos de acuerdo a la demanda laboral, generando y transfiriendo conocimiento; comprometida con el desarrollo del talento humano de la comunidad universitaria, para contribuir con el desarrollo sostenible de la región"*. Con la **Visión:** *"Ser una universidad innovadora, competitiva en la formación profesional de calidad, que promueve la investigación científica, con una organización flexible y con valores, comprometida con el desarrollo descentralizado de la región"*. Para el logro de sus objetivos, está organizado de acuerdo al organigrama mostrado en la Figura 12.

En la Tabla 5, se describen las áreas y oficinas de la UNH con respecto al número de host en la red de datos, las cuales han sido consideradas como objeto de estudio para la presente investigación.

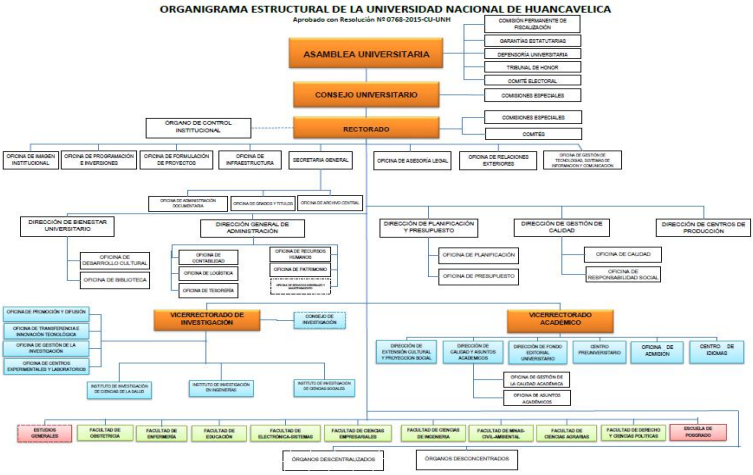


Figura 12. *Organigrama de la Universidad Nacional de Huancavelica*

Tabla 5. *Distribución del número de hosts por campus universitario*

AREAS - OFICINAS	N° HOST
Edificio administrativo	
Total c.u.- edificio administrativo	340
Campus universitario Huancavelica	
Total c.u.- Huancavelica	580
Campus universitario electrónica	
Total c.u.- electrónica	80
Campus universitario sistemas	
Total c.u.- sistemas	130
Campus universitario Lircay	
Total c.u.- Lircay	100
Campus universitario Acobamba	
Total c.u.- Acobamba	110

Descripción de aplicaciones de software usadas en la UNH

La UNH dispone de una variedad de software que es fundamental para optimizar tanto la experiencia educativa como la administrativa. Cada tipo de software desempeña una función específica, contribuyendo a la mejora de procesos. Por ejemplo, las herramientas de gestión de proyectos, como SisAcad y Seguimiento del Docente, facilitan una planificación y seguimiento precisos de las actividades académicas.

Además, este software interactúa con las VLAN (Redes de Área Local Virtual) para mejorar la segmentación, priorización del tráfico y seguridad. La segmentación permite que diferentes tipos de tráfico, como el académico y el administrativo, se mantengan separados, lo que reduce la congestión y mejora el rendimiento general de la red. La priorización del tráfico garantiza que las aplicaciones críticas para el aprendizaje y la administración reciban el ancho de banda necesario, minimizando así las interrupciones. Por último, la seguridad se ve reforzada al aislar diferentes segmentos de la red, lo que dificulta el acceso no autorizado y protege la información sensible de la universidad..

La implementación de estos programas no solo agiliza las operaciones cotidianas, sino que también potencia la capacidad de la institución para adaptarse a los desafíos y oportunidades del entorno digital actual (Figura 13). Las mencionadas herramientas de colaboración y comunicación permiten una interacción más eficiente entre estudiantes y docentes. En resumen, estos softwares (Tabla 6) no solo optimizan los procesos internos, sino que también enriquecen el entorno de aprendizaje, preparando a los estudiantes para los desafíos del mundo digital.

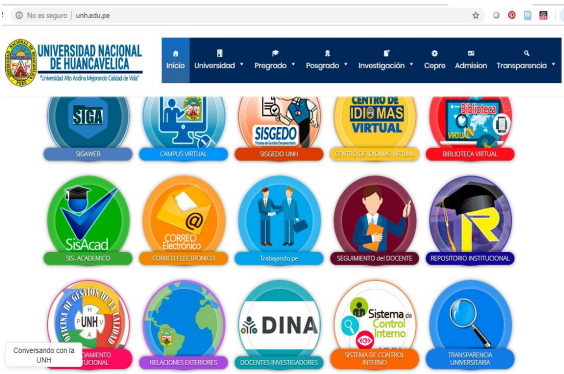


Figura 13. *Pantalla de inicio del portal web de la UNH (www.unh.edu.pe.)*

Tabla 6*. Software – servicios de red usados UNH*

Item	software - servicio de red usados UNH
1	Sistema Académico SISACAD
2	Sistema Virtual de Autoevaluación
3	Sistema de Revistas Científicas
4	Plataforma Virtual Moodle
5	Plataforma Virtual Chamilo
6	Plataforma Virtual Classroom
7	Sistema Integrado de Administración Financiera – SIAF
8	Sistema Integrado de Gestión Administrativa – SIGA
9	Sistema de Caja
10	Sistema de Tramite Documentario SIGEDO
11	Sistema biométrico control personal
12	Email corporativo
13	Redes sociales
14	Impresora en red
15	Teléfono ip.
16	Cámara ip.

Para realizar las descripciones de flujos de datos, simples y compuestos, se consideró el análisis de ancho de banda LAN y WAN en cada una de las oficinas y en todos los campus universitarios (tabla 5), determinando al final el ancho de banda necesario para un adecuado funcionamiento de la universidad (Tabla 7).

Tabla 7 *Ancho de banda LAN requerido por campus universitario*

Campus universitario	Ancho de banda requerido a nivel LAN total
Edificio administrativo	
Total c.u.- Huancavelica	8423
Campus universitario Huancavelica	
Total c.u.- Huancavelica	9900
Campus universitario electrónica	
Total c.u.- electrónica	3200
Campus universitario sistemas	
Total c.u.- sistemas	5200
Campus universitario Lircay	
Total c.u.- Lircay	4000
Campus universitario Acobamba	
Total c.u.- Acobamba	4400

Por tanto, en esta etapa se explicó la descripción del servicio de internet contratado. Para la interconexión de las sedes, la universidad implementó el servicio de internet a través de fibra óptica a través de un proveedor externo en cada uno de los campus universitarios. El servicio tiene las siguientes características:

- Provincia Huancavelica, Ciudad Huancavelica: Campus universitario de Paturrana 20 Mbps, edificio administrativo 20 Mbps.

- Provincia de Acobamba, Ciudad Acobamba: Campus universitario 5 Mbps. Provincia de Angaraes, Ciudad Lircay: Campus universitario 5 Mbps.

- Provincia de Tayacaja, Ciudad Pampas: Campus universitario de Pampas 5 Mbps, Campus universitario de Daniel Hernández 5 Mbps.

La universidad a nivel global cuenta con un servicio de internet de 60 Mbps de ancho de banda.

En cuanto al análisis de ancho de banda, primero se realizó el ancho de banda necesario para que podamos acceder a cada aplicación, para lo cual utilizó el software Wireshark (Figura 14).

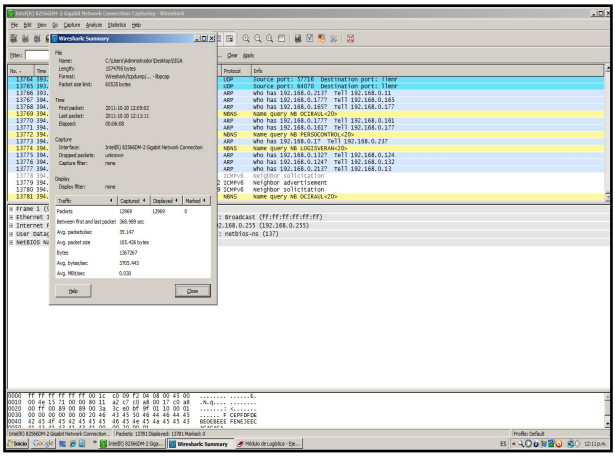


Figura 14. *Análisis de ancho de banda utilizado por el programa SIAF*

Para evaluar el requerimiento de ancho de banda LAN, se evaluó qué software o servicio de red LAN requiere cada host, luego se realizó una suma de los requerimientos LAN en cada host, para luego multiplicarlos por la cantidad de hosts y finalmente se obtiene el requerimiento de ancho de banda LAN necesario en la sala de servidores. Asimismo, para evaluar el requerimiento de ancho de banda WAN, se evaluó qué software o servicio de red WAN requiere cada host, luego se realizó una suma de los requerimientos WAN en cada host, para multiplicarlos por la cantidad de hosts y, finalmente, se obtiene el requerimiento de ancho de banda WAN por cada campus universitario.

De acuerdo a la Tabla 8, se resumen del requerimiento de ancho de banda LAN, se tiene que las necesidades según los software y servicios de red a nivel LAN, en el edificio administrativo y el campus universitario de la sede

Huancavelica es donde más necesidad de un ancho de banda apropiado a nivel LAN, esto debido a que la sala de servidores donde están instalados todos los software – servicios de red se encuentran en el edificio administrativo y a través de una conexión interna por fibra se enlaza con el campus universitario, por lo que, la red se ve como una red de área local LAN, pero a nivel de conexión de la sala de servidores con los demás host en el edificio administrativo se tiene un cableado en categoría 5E que transmite a 10/100mbps, que es soporta la transmisión a nivel LAN siempre en cuando solo se trabajase con equipos de comunicación capa 2, pero en la actualidad los concentradores que conectan los diferentes host son de capa 1 es decir, concentradores físicos capa 1 que lo único que hacen es repetir la señal, generando bloqueos de la red constantemente debido a que no controlan el broadcast de la red, en otras palabras, si uno trasmite todos escuchan y si todos transmiten la red se satura completamente hasta bloquearse.

Tabla 8. *Ancho de banda WAN requerido por campus universitario*

Campus universitario	Total, ancho de banda WAN requerido
Edificio administrativo	
Total c.u.- Huancavelica	8925
Campus universitario Huancavelica	
Total c.u.- Huancavelica	35494
Campus universitario electrónica	
Total c.u.- electrónica	5965
Campus universitario sistemas	
Total c.u.- sistemas	9615
Campus universitario Lircay	
Total c.u.- Lircay	7550
Campus universitario Acobamba	
Total c.u.- Acobamba	8280

Posterior al análisis las necesidades según los software y servicios de red a nivel WAN se tienen que duplicar porque uno es ancho de banda de descarga (download) y otro es ancho de banda de envío (upload). Calculándose un déficit,

en casi todos los campus, de 91658 Kbps (92 Mbps), esta es una de las razones por la que está sobresaturando continuamente la conexión a internet.

4.1.3 Fase de diseño

Se realizó la **definición de ubicación de host**; para ello se recolecta la información del funcionamiento actual de la universidad, plasmándolo en los planos de ubicación de cada uno de los hosts. Debe resaltarse que, en un inicio, la universidad instaló las computadoras según necesidad: se compraba, se instalaba en las oficinas y luego se tendía un cable para conectarlo a un switch para conectarse a internet, sin un análisis técnico previo, motivo por el cual no se tiene ningún tipo de documentación de la infraestructura de red. Tampoco existe una política del proceso de asignamiento IP, de cada uno de los hosts.

Posteriormente, se procedió a **identificar y determinar los servicios que se desea implementar**. En este caso, se evaluó y se determinó que los servicios a implementar en la infraestructura de red son:

- Servidor de archivos LAN donde se almacenarán las bases de datos de los aplicativos informáticos LAN como SISACAD, caja, trámite documentario, control de personal, y otros.
- Servidor de archivos WAN donde se almacenarán las bases de datos de los aplicativos informáticos WAN como software de autoevaluación, revistas científicas, Moodle, Chamilo, Classroom, SIAF, SIGA, otros.
- Servidor WEB para almacenar el portal web de la universidad.
- Servidor de correo.
- Servidor de nombre de dominio (DNS).
- Servidor proxy para el control de acceso a internet.
- Servidor caché para mejorar la velocidad de acceso a internet.

- Servidor de control de acceso inalámbrico (Radius).
- Servidor telefonía IP con Asterisk.
- Servidor de software de video conferencia.
- Servidor de sistema videovigilancia IP.
- Servidor de impresoras.

El análisis de impacto de los servicios propuestos para la infraestructura tecnológica de la Universidad Nacional de Huancavelica revela consideraciones clave en términos de tráfico y seguridad. Los servidores de archivos, tanto LAN como WAN, centralizan el almacenamiento de bases de datos para diversas aplicaciones. Esto puede generar un alto volumen de tráfico interno y externo, especialmente durante horarios pico. Para mitigar riesgos de seguridad, es fundamental implementar autenticación robusta y cifrado de datos, así como utilizar firewalls y sistemas de detección de intrusiones (IDS) para proteger el acceso a la información sensible.

El servidor web y el servidor de correo también requieren atención especial. El servidor web manejará picos de tráfico durante eventos académicos, lo que exige un dimensionamiento adecuado para evitar caídas del servicio. Además, es esencial protegerlo contra ataques DDoS e inyecciones SQL mediante el uso de un firewall para aplicaciones web (WAF). Por otro lado, el servidor de correo debe contar con filtros y protocolos de seguridad como SPF y DKIM para prevenir ataques de phishing y malware, asegurando así la integridad de las comunicaciones.

Finalmente, otros servicios como el servidor proxy, el servidor Radius y el sistema de videovigilancia IP ofrecen oportunidades para mejorar tanto el rendimiento como la seguridad. El servidor proxy optimiza el tráfico saliente y añade una capa adicional de protección al ocultar direcciones IP internas. El servidor Radius refuerza la seguridad del acceso inalámbrico mediante

autenticaciones controladas. Por su parte, el sistema de videovigilancia IP debe estar protegido contra accesos no autorizados mediante redes privadas virtuales (VPN) y configuraciones seguras. En conjunto, estas consideraciones permitirán una infraestructura tecnológica más robusta y eficiente que satisfaga las necesidades académicas y operativas de la universidad.

Seguidamente, se realizó la **asignación de direcciones IP, distribución de subredes y hosts**. La cantidad de hosts conectados a la red de datos fue 1320. Por lo tanto, se administró como dicen las redes de clase B, de acuerdo a la teoría las redes privadas de organizaciones que no están directamente conectadas a Internet; esto es, las redes que se conectan por medio de un router a una única línea con una sola dirección IP dada por un proveedor de servicios, tienen asignados unos rangos de direcciones IP para su funcionamiento interno (Tabla 9).

Tabla 9. *Asignación de direcciones IPv4 en los campus universitarios*

Áreas – oficinas	Nº HOST.	Rango de direcciones ip.
Edificio administrativo		
Total c.u.- edificio administrativo	340	172.17.0.0 - 172.17.7.255
Campus universitario Huancavelica		
Total c.u.- Huancavelica	580	172.17.8.0 - 172.17.15.255
Campus universitario electrónica		
Total c.u.- electrónica	80	172.17.16.0 - 172.17.23.255
Campus universitario sistemas		
Total c.u.- sistemas	130	172.17.24.0 - 172.17.31.255
Campus universitario Lircay		
Total c.u.- Lircay	100	172.17.32.0 - 172.17.39.255
Campus universitario Acobamba		
Total c.u.- Acobamba	110	172.17.40.0 - 172.17.47.255

Creación de VLANs. En esta etapa se desarrolla el diseño de las redes virtuales de área local VLANs. Esto permitió eliminar la saturación broadcast de la red, también permitió agrupar a los hosts con ciertas características en grupos de una misma familia para que puedan ser una red independiente a nivel lógico, logrando de esta manera, tener una mejor seguridad en la red, permitiendo una mejor segmentación en grupos y reducir el congestionamiento de la red. En la

Tabla 10 se muestra el resultado de crear las VLAN dentro de la red de datos del edificio administrativo de la Universidad Nacional de Huancavelica, mientras que en la Tabla 11, las VLAN con su respectivo nombre y su rango de IP V4.

Tabla 10. *Redes de área local VLAN: su nombre y áreas que alberga en los campus universitarios*

VLAN	NOMBRE VLAN	Nº HOST
CAMPUS UNIVERSITARIO		
Pabellon derecho		
VLAN 110	laboratorios	30
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellon educación		
VLAN 110	laboratorios	30
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellón de ingeniería		
VLAN 110	laboratorios	40
VLAN 120	docentes	10
VLAN 130	administrativos	5
Pabellón ingeniería civil		
VLAN 110	laboratorios	20
VLAN 120	docentes	4
VLAN 130	administrativos	1
Pabellón enfermería		
VLAN 110	laboratorios	40
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellón obstetricia		
VLAN 110	laboratorios	40
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellón ciencias administrativas		
VLAN 110	laboratorios	50
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellón video conferencia		
VLAN 110	salas de video conferencias - Laboratorios	55
VLAN 130	administrativos	5
Biblioteca		
VLAN 110	equipos para consulta estudiantes	35
VLAN 130	administrativos	5
Pabellón auditorio general		
VLAN 110	auditorio general	5
VLAN 130	administrativos	15
Pabellón comedor - bienestar		
VLAN 130	administrativos	20
Pabellón almacen - mantenimiento obras		
VLAN 130	administrativos	30
Pabellón archivo central		
VLAN 130	archivo central	10
Residencia universitaria		
VLAN 110	laboratorio	30
VLAN 130	administrativos	
CAMPUS UNIVERSITARIO		
VLAN 110	laboratorios	60
VLAN 120	docentes	15
VLAN 130	administrativos	5
CAMPUS UNIVERSITARIO SISTEMAS		
VLAN 110	laboratorios	90
VLAN 120	docentes	15
VLAN 130	administrativos	5
VLAN 110	Residencia	20
CAMPUS UNIVERSITARIO LIRCAY		
Pabellon minas		
VLAN 110	laboratorios	20
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellón civil		
VLAN 110	laboratorios	20
VLAN 120	docentes	15
VLAN 130	administrativos	5
VLAN 110	residencia	20
CAMPUS UNIVERSITARIO ACOBAMBA		
Pabellón agronomía		
VLAN 110	laboratorios	25
VLAN 120	docentes	15
VLAN 130	administrativos	5
Pabellón agroindustrias		
VLAN 110	laboratorios	25
VLAN 120	docentes	15
VLAN 130	administrativos	5
VLAN 110	residencia	20

Tabla 11. *VLAN con su respectivo nombre y su rango de IPv4*

VLAN	NOMBRE VLAN	RANGO DE IP POR VLAN
VLAN 10	TICS	172.17.0.0 - 172.17.0.63
VLAN 20	ADMINISTRACION	172.17.0.0 - 172.17.0.63
VLAN 30	VIGILANCIA	172.17.0.0 - 172.17.0.63
VLAN 40	SEGUNDA ESPECIALIZACION	172.17.0.0 - 172.17.0.63
VLAN 50	ALTA DIRECCION	172.17.0.0 - 172.17.0.63
VLAN 60	CONTROL INTERNO	172.17.0.0 - 172.17.0.63
VLAN 70	SECRETARIA GENERAL	172.17.0.0 - 172.17.0.63
VLAN 80	ACADEMICO	172.17.0.0 - 172.17.0.63
VLAN 90	INFRAESTRUCTURA	172.17.0.0 - 172.17.0.63
VLAN 25	VOZ	172.17.0.0 - 172.17.0.63
VLAN 35	VIDEOCONFERENCIA	172.17.0.0 - 172.17.0.63
VLAN 55	INALAMBRICO	172.17.0.0 - 172.17.0.63

La elección del medio de transmisión para la infraestructura física del modelo de comunicaciones unificadas se basa en el uso de cable de par trenzado no apantallado (UTP) categoría 6A, que permite la transmisión de datos a velocidades de 10, 100 y 1000 Mbps. Esta selección es ideal debido a su alta capacidad de ancho de banda, costo-efectividad y facilidad de instalación. Además, todos los componentes del cableado estructurado, como jacks, tomas de datos, conectores RJ45 y patch panels, serán de categoría 6A, asegurando así una infraestructura robusta y eficiente que optimiza la conectividad y la integración con tecnologías modernas.

Por su parte, la **elección de los equipos de comunicación** para la infraestructura física del modelo de comunicaciones unificadas según los requerimientos, fue:

a) **Router Cisco 4351**. Características: servicios de software concurrentes a velocidades de hasta 2 gbps. arquitectura backplane soporta gran ancho de banda de comunicación de módulo a módulo a

velocidades de hasta 10 gbps. arquitectura multinúcleo con primer plano de los servicios internos de la industria, instalación remota de servicios de aplicaciones-conscientes, que funcionan de forma idéntica a sus contrapartes en dispositivos dedicados, menores gastos WAN, solución embebida IWAN para la creación, conexiones de internet de clase empresarial de más costos crecimiento modular: la capacidad del router se puede aumentar con una actualización remota rendimiento bajo demanda, licencia (sin necesidad de actualización del hardware) para los ahorros excepcionales.

b) **Switch núcleo Cisco Catalyst 3850;** 12 Port 10G Fiber Switch IP Base. Especificaciones técnicas: capacidad para operar con al menos 32,000 direcciones MAC. Accesorios para montaje en rack de 19. Modo de operación full y half duplex. Capacidad de switching: superior a 65 gbps. Velocidad de reenvío mínimo: 225 mpps. Presentar indicadores led de operación por puerto. Capacidad mínima de VLAN IDS soportados: 4000. Memoria dram mínima: 4 GB. Memoria flash mínima: 2 GB. Número total de rutas IPv4: 24000. Mecanismos de operación y gestión. Protocolo Spanning Tree y mejoras tales como convergencia rápida (rst 802.1w). Tráfico multicast IGMP debe permitir múltiples sesiones.

c) **Switch Cisco Catalyst** 3560: es una línea de switches de clase empresarial que incluye soporte para PoE, QoS y características de seguridad avanzada como ACL. Son los switches de capa de acceso ideales para acceso a la LAN de pequeñas empresas. Características: Velocidades de envío entre 32 Gbps y 128 Gbps. Administración basada en la web y CLI de Cisco. Funciones de LAN avanzadas: (QoS). Conectividad Fast Ethernet y Gigabit Ethernet. 24 puertos 10/100/1000 más 4 puertos SFP. Puertos PoE con 15.4 Watt.

d) **Router Cisco Inalámbrico Broanland 150 N 802.11b/g**. Wireless-N broadband router wireless Cisco Systems Linksys Wrt160n,

estándar IEEE 802.11b/g/n, estándar IEEE 802.3/802.3u, antena dual, 4 puertos 10/100.

e) **Teléfono VoIP CISCO Unified IP Phone 521SG POE**. Características: Soporte de múltiples líneas, soporte de múltiples protocolos VoIP, conmutador Ethernet integrado. Protocolos VoIP: SIP, SIP v2, SPCP, soporte para alimentación mediante Ethernet (PoE), líneas soportadas: 8 líneas, teléfono con altavoz: sí (teléfono digital de dos vías), capacidad de correo de voz y remarcación automática.

En este punto se procedió al **diseño del cableado estructurado**; en la Figura 15 se muestra el plano del cableado estructurado de cada campus universitario y sus pabellones.

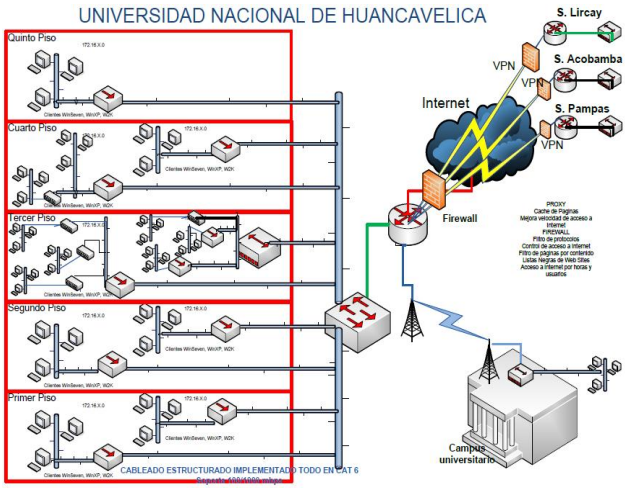


Figura 15. *Modelo de red con redes virtuales locales (VLAN)*

De igual modo, se realizó el **diseño lógico de la red de datos** del modelo de red con redes virtuales locales de la Universidad Nacional de Huancavelica (Figura 16).

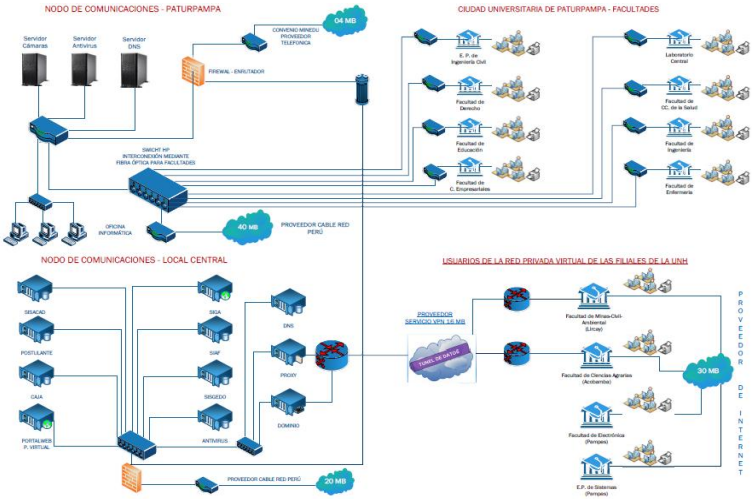


Figura 16. *Diseño lógico del modelo de red con redes virtuales locales (VLAN)*

La Figura 16, representa una infraestructura de red compleja, dividida en tres secciones principales. La sección superior izquierda, etiquetada como "NODO DE COMUNICACIONES - PLENUM/PARAPETO," muestra varios componentes de red interconectados, incluyendo servidores y bases de datos. La sección superior derecha, "CIUDAD UNIVERSITARIA DE PUNTARENAS - FACULTADES," también contiene múltiples elementos de red, sugiriendo una conexión entre diferentes facultades universitarias. La sección inferior, "NODO DE COMUNICACIONES - LOCAL CENTRAL," abarca todo el ancho de la imagen y parece ser el nodo central de la red, conectando los otros dos nodos.

La sección de USUARIOS PRIVADOS, incluye varios nodos etiquetados y conectados por flechas, indicando la secuencia o flujo de las operaciones. Los nodos representan diferentes etapas como "Inicio del

Proceso," "Recepción de Requerimientos," "Análisis," "Desarrollo," y "Pruebas." Además, hay símbolos como edificios bancarios, documentos y lupas que representan visualmente cada etapa.

Cada sección está detalladamente conectada con enlaces de comunicación, indicando una red robusta y redundante. Los iconos y etiquetas proporcionan información adicional sobre cada componente y su función dentro del sistema. Esta estructura sugiere un diseño pensado para asegurar la continuidad del servicio y la eficiencia en la transmisión de datos entre los diferentes nodos y componentes de la red.

Capítulo 5

Fortalecimiento de la Seguridad de Información

Con el fin de comprobar la eficacia de la instalación de las redes virtuales locales en concordancia con la situación problemática mencionada en la UNH, con el objetivo del fortalecimiento de la seguridad de la información, que en la actualidad se ha convertido en una prioridad esencial. Por tanto, se compara las mediciones de la seguridad de información previas a la instalación de VLAN y post, de acuerdo a sus dimensiones confidencialidad, integridad y disponibilidad, según ISO 27001, sus indicadores planteados en la matriz de operacionalización de variables. Además de mencionar las pruebas, se realizaron en cada uno de los hosts de cada oficina en todos los campus universitarios (UNH).

5.1 Seguridad de la información

5.1.1 Dimensión: Disponibilidad de la información en la red de datos

Indicador 1.1: Tiempo de respuesta de aplicaciones LAN. En la figura 17, se observan los resultados de la prueba de tiempos de respuesta de las aplicaciones LAN expresadas en milisegundos, mostrando que existe una disminución del tiempo de respuesta de las aplicaciones LAN de 77,35 milisegundos con la red de datos sin VLAN a un tiempo de respuesta de 15,79 milisegundos con la red de datos con VLAN; por lo tanto, se puede afirmar que el tiempo de respuesta disminuye en 61,56 milisegundos cuando se implementan redes virtuales locales VLAN en una red de datos.

Estos tiempos de respuesta se realizaron a través de la ventana de comandos con el comando ping, que envía un lote de 1400 bytes de extremo a extremo (Figura 17). Esta prueba se realizó desde cada host de cada oficina de la universidad hacia los servidores de las aplicaciones LAN. Estos servidores se encuentran en el local administrativo en Huancavelica; se interactuó con el campus universitario de Paturpampa y con los diferentes campus universitarios en las sedes respectivas de la UNH.

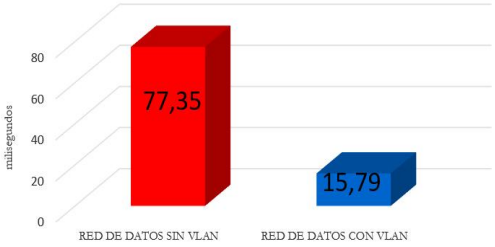


Figura 17. *Tiempo de respuesta de aplicaciones LAN en milisegundos*

Indicador 1.2: Tiempo de respuesta de aplicaciones WAN. En este caso se observó que el tiempo de respuesta de las aplicaciones WAN con la red de datos sin VLAN disminuye de 246,12 milisegundos a un tiempo de respuesta de 39,83 milisegundos con la red de datos con VLAN; por lo tanto, se puede afirmar que el tiempo de respuesta disminuye en 206, 29 milisegundos cuando se implementan redes virtuales locales VLAN en una red de datos (Figura 18). Es importante mencionar que para medir la respuesta de las aplicaciones WAN expresadas en milisegundos, el acceso a aplicaciones WAN a través de internet o líneas dedicadas en los diferentes campus universitarios, al igual que la evaluación anterior, los tiempos de respuesta se realizaron a través de la ventana de comandos con el comando ping, que envía un lote de 1400 bytes de extremo

a extremo. Esta prueba se realizó desde cada host de cada oficina de la universidad hacia los servidores de las aplicaciones WAN.

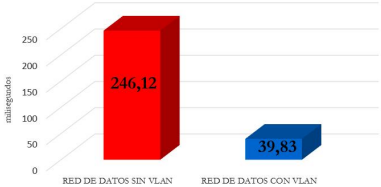


Figura 18. *Tiempo d respuesta de aplicaciones WAN en milisegundos*

Indicador 1.3: Tasa de transferencia a nivel LAN. Para visualizar las diferencias de transferencia a nivel de área local LAN entre la red de datos sin VLAN con la red de datos con VLAN, sus dos estados: carga y descarga de paquetes de datos. En la Figura 19 se observa que, en el estado de descarga, la red de datos sin VLAN tiene una tasa de transferencia de 18,78 megabits por segundo y la red de datos con VLAN tiene una tasa de transferencia de 30,1 megabits por segundo, teniendo un incremento de 11,32 megabits por segundo en la tasa de transferencia a nivel de red de área local LAN. Para el estado de carga, la red de datos sin VLAN tiene una tasa de transferencia de 15,2 megabits por segundo y la red de datos con VLAN tiene una tasa de transferencia de 20,29 megabits por segundo, con un incremento de 5,09 megabits por segundo en la tasa de transferencia.

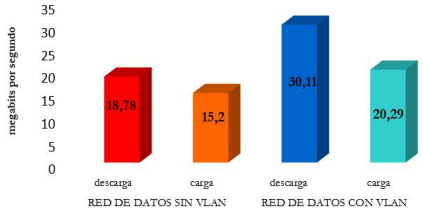


Figura 19*. Tasa de transferencia a nivel LAN en Mbps*

Indicador 1.4: Tasa de transferencia a nivel WAN. En la figura 20 se observa que existen diferencias en la tasa de transferencia a nivel de red de área amplia entre la red de datos sin VLAN con la red de datos con VLAN, en sus dos estados: carga y descarga de paquetes de datos. En el estado de descarga, la red de datos sin VLAN tiene una tasa de transferencia de 1,32 megabits por segundo y la red de datos con VLAN tiene una tasa de transferencia de 2,33 megabits por segundo. Se puede observar que se tiene un incremento de 1,01 megabits por segundo en la tasa de transferencia a nivel de red de área amplia en el estado de descarga de datos. En el estado de carga, la red de datos sin VLAN tiene una tasa de transferencia de 0,88 megabits por segundo y la red de datos con VLAN tiene una tasa de transferencia de 1,73 megabits por segundo. Se puede observar que se tiene un incremento de 0,85 megabits por segundo o su equivalente 850 kilobits por segundo en la tasa de transferencia a nivel de red de área amplia en el estado de carga de datos.

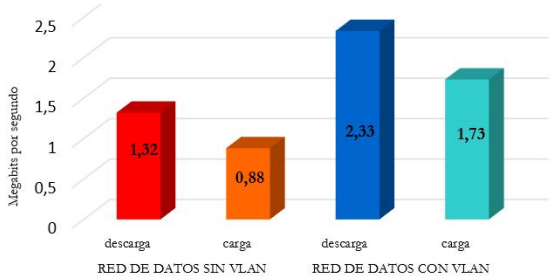


Figura 20. *Tasa de transferencia a nivel WAN en Mbps*

Indicador 1.5: Número de servicios ofrecidos por la red. Los resultados mostraron que existen diferencias en la cantidad de servicios ofrecidos por la red (Figura 21). La red de datos sin VLAN ofrece 5 servicios de red y la red de datos con VLAN ofrece 16 servicios de red, es decir, hubo un incremento de 11 servicios de red.

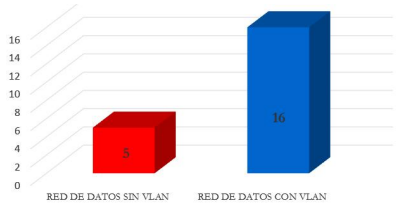


Figura 21. *Número de servicios ofrecidos por la red*

5.1.2. Dimensión: integridad de la información en la red de datos

Indicador 2.1: Número de casos de alteraciones - pérdida de datos. Según el ISO 27001, en la Figura 22 se muestra la cantidad de casos registrados de alteraciones de la información y/o pérdida de datos en la red de datos con VLAN y la red de datos sin VLAN. En la red de datos sin VLAN se registraron 1076 casos de alteraciones – pérdida de datos durante el semestre 2018 -I, mientras que en la red de datos con VLAN se registraron 201 casos durante el semestre 2018 -II. Se puede observar que se tiene una disminución de 875 casos.

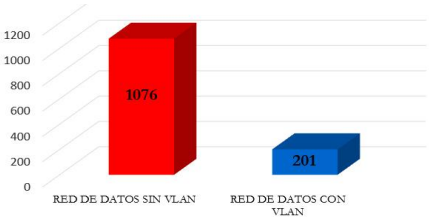


Figura 22. *Números de alteraciones - pérdida de datos*

5.1.3. Dimensión confidencialidad de la información en la red de datos

Indicador 3.1: Porcentaje de accesos a servicios no autorizados a nivel LAN. Uno de los indicadores considerados en este estudio es el

porcentaje de accesos a servicios no autorizados a nivel LAN, el cual evalúa el número de solicitudes de acceso de paquetes de la red de área local LAN a servicios no permitidos que tuvieron éxito respecto al total de solicitudes de acceso de paquetes de la red de área local LAN a servicios no autorizados, y los expresa en porcentajes cada día durante 20 días. En la Figura 23 se muestra el resumen de porcentajes de acceso a servicios no autorizados a nivel LAN en la red de datos sin VLAN y la red de datos con VLAN. La red de datos sin VLAN se registró un 88 % de éxito de las solicitudes de acceso a servicios no permitidos, mientras que la red de datos con VLAN registró un 9 %, se puede observar que se tiene una disminución del 79 %.

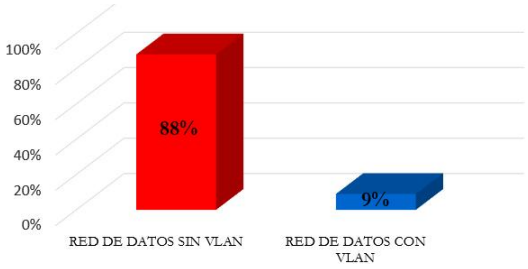


Figura 23. *Número de acceso a servicios no autorizados a nivel LAN*

Indicador porcentaje 3.2: Porcentaje de accesos a servicios no autorizados a nivel WAN. Evalúa el número de solicitudes de acceso de paquetes de la red de área amplia quiere decir provenientes de la línea dedicada o internet, a servicios no permitidos que tuvieron éxito respecto al total de solicitudes de acceso de paquetes de la red de área amplia a servicios no autorizados, y los expresa en porcentajes cada día durante 20 días. En la Figura 24 se observa que la red de datos sin VLAN registró un 88 % de éxito de las solicitudes de acceso a servicios no permitidos, mientras que la red de datos con VLAN registró un 9 %, con una disminución del 79 %.

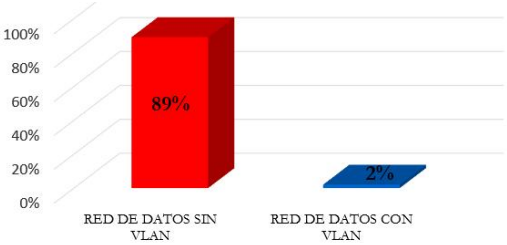


Figura 24. *Porcentaje de accesos a servicios no autorizados a nivel WAN*

5.2 Contrastación de hipótesis

Con base en los resultados, se realiza la evaluación de las hipótesis en relación a los ítems o indicadores de interés en esta investigación. Partiendo de la hipótesis general: *"Las redes virtuales locales (VLAN) influyen positivamente en la seguridad de la información en la red de datos de la Universidad Nacional de Huancavelica*". Se establecieron:

♦ **H_1:** Las redes virtuales locales (VLAN) influyen positivamente en la integridad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Indicador 1.1: Tiempo de respuesta a nivel LAN de la red.

- **Ho:** El promedio de los tiempos de respuesta a nivel LAN de la red de datos actual es menor o igual que el promedio de los tiempos de respuesta a nivel LAN con VLAN.
- **Ha:** El promedio de los tiempos de respuesta a nivel LAN de la red de datos actual es mayor que el promedio de los tiempos de respuesta a nivel LAN con VLAN.

Entonces:

Utrlrda = Promedio de los tiempos de respuesta a nivel LAN en la red de datos actual.

Utrlrdvlan = Promedio de los tiempos de respuesta a nivel LAN en la red de datos con VLAN.

Ho = Utrlrda $\leqslant$ Utrlrdvlan

H1 = Utrlrda > Utrlrdvlan

Como la hipótesis es una prueba de una cola a la derecha, entonces los valores críticos para $\propto$ =0,05 = 5% quedarán definidos como se muestra en la Figura 24.

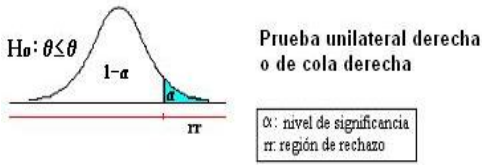


Figura 24. *Prueba unilateral derecha*

Tomando en cuenta la prueba no paramétrica de Wilcoxon, cuyos resultados se visualizan en la Tabla 10, donde se obtuvo *p*=0.000, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna H1. Es decir, el promedio de los tiempos de respuesta a nivel LAN de la red de datos actual es mayor que el promedio de los tiempos de respuesta a nivel LAN con VLAN.

Tabla 10. *Resultados estadísticos para la evaluación de las hipótesis*

Rangos				
		N	Rango promedio	Suma de rangos
tiempo de respuesta a nivel LAN red de datos VLAN - tiempo de respuesta a nivel LAN red de datos actual	Rangos negativos	85[a]	43,00	3655,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	85		
a. tiempo de respuesta a nivel LAN red de datos VLAN < tiempo de respuesta a nivel LAN red de datos actual				
b. tiempo de respuesta a nivel LAN red de datos VLAN > tiempo de respuesta a nivel LAN red de datos actual				
c. tiempo de respuesta a nivel LAN red de datos VLAN = tiempo de respuesta a nivel LAN red de datos actual				
Estadísticos de prueba[a]				
	Tiempo de respuesta a nivel LAN red de datos VLAN - tiempo de respuesta a nivel LAN red de datos actual			
Z	-8,008[b]			
Sig. asintótica (bilateral)	,000			
a. Prueba de rangos con signo de Wilcoxon				
b. Se basa en rangos positivos.				

♦ **H_2:** Las redes virtuales locales (VLAN) influyen positivamente en la disponibilidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Indicador 1.2: Tiempo de respuesta a nivel WAN de la red.

- **Ho:** El promedio de los tiempos de respuesta a nivel WAN de la red de datos actuales es menor o igual que el promedio de los tiempos de respuesta a nivel WAN con VLAN.
- **Ha:** El promedio de los tiempos de respuesta a nivel WAN de la red de datos actual es mayor que el promedio de los tiempos de respuesta a nivel WAN con VLAN.

Entonces:

Utrwrda = Promedio de los tiempos de respuesta a nivel WAN en la red de datos actual.

Utrwrdvlan = Promedio de los tiempos de respuesta a nivel WAN en la red de datos con VLAN.

Ho =Utrwrda $\leqslant$ Utrwrdvlan

H1 =Utrwrda > Utrwrdvlan

En este caso la hipótesis es una prueba de una cola a la izquierda, entonces los valores críticos para $\propto$ =0.05 = 5% quedarán definidos como se observa en la Figura 25.

Figura 25. *Prueba unilateral izquierda*

Basados en la prueba no paramétrica de Wilcoxon p=0.000 (Tabla 11), se rechaza la hipótesis nula Ho y se acepta la hipótesis alterna H_1. El promedio de los tiempos de respuesta a nivel WAN de la red de datos actual es mayor que el promedio de los tiempos de respuesta a nivel WAN con VLAN.

Tabla 11. *Resultados estadísticos para la evaluación de las hipótesis*

Rangos				
		N	Rango promedio	Suma de rangos
tiempo de respuesta a nivel WAN red de datos VLAN - tiempo de respuesta a nivel WAN red de datos Actual	Rangos negativos	85[a]	43,00	3655,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	85		
a. tiempo de respuesta a nivel WAN red de datos VLAN < tiempo de respuesta a nivel WAN red de datos Actual				
b. tiempo de respuesta a nivel WAN red de datos VLAN > tiempo de respuesta a nivel WAN red de datos Actual				
c. tiempo de respuesta a nivel WAN red de datos VLAN = tiempo de respuesta a nivel WAN red de datos Actual				
Estadísticos de prueba[a]				
	Tiempo de respuesta a nivel WAN red de datos VLAN - tiempo de respuesta a nivel WAN red de datos Actual			
Z	-8,008[b]			
Sig. asintótica (bilateral)	,000			
a. Prueba de rangos con signo de Wilcoxon				
b. Se basa en rangos positivos.				

Indicador 1.3: Tasa de transferencia a nivel LAN.

- **Ho:** El promedio de la tasa de transferencia a nivel LAN de la red de datos actuales es mayor o igual que el promedio de la tasa de transferencia a nivel LAN de la red de datos con VLAN.
- **Ha:** El promedio de la tasa de transferencia a nivel LAN de la red de datos actual es menor que el promedio de la tasa de transferencia a nivel LAN de la red de datos con VLAN.

Entonces:

Uttlrda = Promedio tasa de transferencia a nivel LAN en la red de datos actual

Uttlrdvlan = Promedio tasa de transferencia a nivel LAN en la red de datos con VLAN

Ho = Uttlrda $\geqslant$ Uttlrdvlan

H1 = Uttlrda < Uttlrdvlan

En este caso la hipótesis es una prueba de una cola a la izquierda. Se elige la prueba no paramétrica de Wilcoxon, para muestras relacionadas p=0.000. Por lo tanto, se rechaza la hipótesis nula Ho y se acepta la hipótesis alterna H_1 El promedio de la tasa de transferencia a nivel LAN de la red de datos actual es menor que el promedio de la tasa de transferencia a nivel LAN de la red de datos con VLAN (Tabla 12).

Tabla 12. *Resultados estadísticos para la evaluación de las hipótesis*

Rangos				
		N	Rango promedio	Suma de rangos
Tasa de transferencia LAN descarga red de datos VLAN - tasa de transferencia LAN descarga red de datos actual	Rangos negativos	2[a]	3,00	6,00
	Rangos positivos	81[b]	42,96	3480,00
	Empates	2[c]		
	Total	85		
a. tasa de transferencia LAN descarga red de datos VLAN < tasa de transferencia LAN descarga red de datos actual				
b. tasa de transferencia LAN descarga red de datos VLAN > tasa de transferencia LAN descarga red de datos actual				
c. tasa de transferencia LAN descarga red de datos VLAN = tasa de transferencia LAN descarga red de datos actual				
Estadísticos de prueba[a]				
	Tasa de transferencia LAN descarga red de datos VLAN - tasa de transferencia LAN descarga red de datos actual			
Z	-7,890[b]			
Sig. asintótica (bilateral)	,000			
a. Prueba de rangos con signo de Wilcoxon				
b. Se basa en rangos negativos.				

Indicador 1.4: Tasa de Transferencia a nivel WAN.

- **Ho:** El promedio de la tasa de transferencia a nivel WAN de la red de datos actuales es mayor o igual que el promedio de la tasa de transferencia a nivel WAN de la red de datos con VLAN.
- **Ha:** El promedio de la tasa de transferencia a nivel WAN de la red de datos actuales es menor que el promedio de la tasa de transferencia a nivel WAN de la red de datos con VLAN.

Entonces:

Uttwrda = Promedio tasa de transferencia a nivel WAN en la red de datos actual

Uttwrdvlan = Promedio tasa de transferencia a nivel WAN en la red de datos con VLAN

Ho = Uttwrda $\geqslant$ Uttwrdvlan

H1 =Uttwrda < Uttwrdvlan

La hipótesis es una prueba de una cola a la izquierda, luego de aplicar la prueba no paramétrica de Wilcoxon, para muestras relacionadas p=0.000. Por lo tanto, se rechaza la hipótesis nula Ho y acepta la hipótesis alterna H_1 El promedio de la tasa de transferencia a nivel WAN de la red de datos actual es menor que el promedio de la tasa de transferencia a nivel WAN de la red de datos con VLAN (Tabla 13).

Tabla 13. *Resultados estadísticos para la evaluación de las hipótesis*

Rangos				
		N	Rango promedio	Suma de rangos
Tasa de transferencia WAN descarga red de datos VLAN - tasa de transferencia WAN descarga red de datos actual	Rangos negativos	0[a]	,00	,00
	Rangos positivos	85[b]	43,00	3655,00
	Empates	0[c]		
	Total	85		
a. tasa de transferencia WAN descarga red de datos VLAN < tasa de transferencia WAN descarga red de datos actual				
b. tasa de transferencia WAN descarga red de datos VLAN > tasa de transferencia WAN descarga red de datos actual				
c. tasa de transferencia WAN descarga red de datos VLAN = tasa de transferencia WAN descarga red de datos actual				
Estadísticos de prueba[a]				
	Tasa de transferencia WAN descarga red de datos VLAN - tasa de transferencia WAN descarga red de datos actual			
Z	-8,031[b]			
Sig. asintótica (bilateral)	,000			
a. Prueba de rangos con signo de Wilcoxon				
b. Se basa en rangos negativos.				

Indicador 2.1: Número de casos de Alteraciones – Pérdida de datos.

Ho: El promedio de casos de alteraciones – pérdida de datos de la red de datos actual es menor o igual que el promedio de casos de alteraciones – pérdida de datos de la red de datos con VLAN.

• **Ha:** El promedio de casos de alteraciones – pérdida de datos de la red de datos actual es mayor que el promedio de casos de alteraciones – pérdida de datos de la red de datos con VLAN.

Entonces:

Ucapdrda = Promedio de casos de alteraciones -pérdida de datos en la red de datos actual

Ucapdrdvlan = Promedio de casos de alteraciones -pérdida de datos en la red de datos con VLAN

Ho = Ucapdrda $\leqslant$ Ucapdrdvlan

H1 = Uttlrda > Uttlrdvlan

Como la hipótesis es una prueba de una cola a la derecha, se observa en la Tabla 14 los resultados de la prueba no paramétrica de Wilcoxon, para muestras relacionadas p=0.000. Se rechaza la hipótesis nula Ho y se acepta la alterna.

Tabla 14. *Resultados estadísticos para la evaluación de las hipótesis*

Rangos				
		N	Rango promedio	Suma de rangos
Nro casos alteraciones red de datos VLAN - nro casos alteraciones red de datos actual	Rangos negativos	16[a]	10,50	168,00
	Rangos positivos	2[b]	1,50	3,00
	Empates	5[c]		
	Total	23		
a. nro casos alteraciones red de datos VLAN < nro casos alteraciones red de datos actual				
b. nro casos alteraciones red de datos VLAN > nro casos alteraciones red de datos actual				
c. nro casos alteraciones red de datos VLAN = nro casos alteraciones red de datos actual				
Estadísticos de prueba[a]				
	Nro casos alteraciones red de datos VLAN - nro casos alteraciones red de datos actual			
Z	-3,594[b]			
Sig. asintótica (bilateral)	,000			
a. Prueba de rangos con signo de Wilcoxon				
b. Se basa en rangos positivos.				

♦ H_3: Las redes virtuales locales (VLAN) influyen positivamente en la confidencialidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Indicador 3.1: Porcentaje de accesos a servicios no autorizados a nivel LAN.

- **Ho:** El promedio de porcentaje de accesos a servicios no autorizados a nivel LAN de la red de datos actual es menor o igual que el promedio de accesos a servicios no autorizados a nivel LAN de la red de datos con VLAN.

- **Ha:** El promedio de casos de alteraciones – pérdida de datos de la red de datos actual es mayor que el promedio de casos de alteraciones – pérdida de datos de la red de datos con VLAN.

Entonces:

U%asnalrda = Promedio porcentaje de accesos a servicios no autorizados a nivel LAN de la red de datos actual.

U%asnalvlan = Promedio porcentaje de accesos a servicios no autorizados a nivel LAN de la red de datos con VLAN.

Ho = U%asnalrda $\leqslant$ U%asnalvlan

H1 = U%asnalrda > U%asnalvlan

La hipótesis es una prueba de una cola a la derecha. Se eligió la prueba de T Student, para muestras relacionadas, por ser un estudio longitudinal con medidas del antes y después, y también por trabajar con variables numéricas. Se trabajó con el estadístico Shapiro Wilk (<30 host). Criterios para determinar la normalidad:

p valor => α Aceptar Ho = Los datos provienen de una distribución normal. p valor < α Aceptar H1 = Los datos NO provienen de una distribución normal.

Se puede observar en la Tabla 15, el valor de p=0,000. Por lo tanto, el promedio de porcentaje de accesos a servicios no autorizados a nivel LAN de la red de datos actual es mayor que el promedio de accesos a servicios no autorizados a nivel LAN de la red de datos con VLAN.

Tabla 15. *Resultados estadísticos para la evaluación de las hipótesis*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
% de accesos a servicios no autorizados a nivel LAN red datos actual	,125	20	,200*	,945	20	,301
% de accesos a servicios no autorizados a nivel LAN red datos VLAN	,153	20	,200*	,942	20	,259
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

NORMALIDAD		
P valor (%asnalrda)=0,301	>	α =0.05
P-valor (%asnalvlan)=0,259	>	α =0.05
Conclusión: Los datos del % de accesos servicios no autorizados a nivel LAN provienen de una distribución normal.		

Estadísticas de muestras emparejadas					
		Media	N	Desviación estándar	Media de error estándar
Par 1	% de accesos a servicios no autorizados a nivel LAN red datos actual	88,0000	20	4,40096	,98408
	% de accesos a servicios no autorizados a nivel LAN red datos VLAN	9,1000	20	1,65116	,36921

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	% de accesos a servicios no autorizados a nivel LAN red datos actual & % de accesos a servicios no autorizados a nivel LAN red datos VLAN	20	,007	,976

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl.	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	IC 95 % Inferior	IC 95 % Superior			
Par 1	% de accesos a servicios no autorizados a nivel LAN red datos actual - % de accesos a servicios no autorizados a nivel LAN red datos VLAN	78,90000	4,68929	1,04856	76,70534	81,09466	75,246	19	,000

Indicador 3.2: Porcentaje de accesos a servicios no autorizados a nivel WAN.

- **H_o:** El promedio de porcentaje de accesos a servicios no autorizados a nivel WAN de la red de datos actual es menor o igual que

el promedio de accesos a servicios no autorizados a nivel WAN de la red de datos con VLAN.

- **H_1:** El promedio de porcentaje de accesos a servicios no autorizados a nivel WAN de la red de datos actual es mayor que el promedio de accesos a servicios no autorizados a nivel WAN de la red de datos con VLAN.

Entonces:

U%asnawrda = Promedio % de accesos a servicios no autorizados a nivel WAN de la red de datos actual

U%asnawvlan = Promedio % de accesos a servicios no autorizados a nivel WAN de la red de datos con VLAN

Ho = U%asnawrda $\leqslant$ U%asnawvan

H1 = U%asnawrda > U%asnawvlan

La hipótesis es una prueba de una cola a la derecha; en este caso se empleó la prueba no paramétrica de Wilcoxon, p=0.000. Por lo tanto, se rechaza la hipótesis nula: el promedio de porcentaje de accesos a servicios no autorizados a nivel WAN de la red de datos actual es mayor que el promedio de accesos a servicios no autorizados a nivel WAN de la red de datos con VLAN (Tabla 16).

Los hallazgos de este estudio no solo subrayan la importancia de contar con sistemas robustos de protección de datos, sino que también destacan las áreas donde se requiere una atención adicional para mitigar riesgos potenciales. A través de un enfoque detallado y basado en evidencia, este capítulo proporcionó una visión comprensiva de las prácticas actuales y cómo se puede

optimizar la seguridad de la información en un entorno constantemente amenazado por ciberataques y brechas de seguridad.

Tabla 16. *Resultados estadísticos para la evaluación de las hipótesis*

Rangos				
		N	Rango promedio	Suma de rangos
% de accesos a servicios no autorizados a nivel WAN red datos VLAN - % de accesos a servicios no autorizados a nivel WAN red datos actual	Rangos negativos	20[a]	10,50	210,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	20		
a. % de accesos a servicios no autorizados a nivel WAN red datos VLAN < % de accesos a servicios no autorizados a nivel WAN red datos actual				
b. % de accesos a servicios no autorizados a nivel WAN red datos VLAN > % de accesos a servicios no autorizados a nivel WAN red datos actual				
c. % de accesos a servicios no autorizados a nivel WAN red datos VLAN = % de accesos a servicios no autorizados a nivel WAN red datos actual				
Estadísticos de prueba[a]				
	% de accesos a servicios no autorizados a nivel WAN red datos VLAN - % de accesos a servicios no autorizados a nivel WAN red datos actual			
Z	-3,924[b]			
Sig. asintótica (bilateral)	,000			
a. Prueba de rangos con signo de Wilcoxon				
b. Se basa en rangos positivos.				

Capítulo 6

Aplicación de las Redes Virtuales Locales

La implementación de redes virtuales locales (VLAN) en la UNH ha demostrado ser una estrategia altamente efectiva para la optimización de procesos informáticos y el fortalecimiento de la seguridad de la información. Los resultados obtenidos en este estudio subrayan varios aspectos clave que justifican la adopción de VLAN y sus beneficios significativos.

En este contexto, los datos recolectados evidencian una mejora notable en la eficiencia operativa de los sistemas informáticos. La segmentación de la red mediante VLAN permitió una administración más sencilla y una reducción de la congestión de la red. Al separar el tráfico de red en segmentos lógicos, se logró una mejor gestión de los recursos y una respuesta más rápida a las solicitudes de los usuarios. Esto es consistente con estudios previos que destacan los beneficios de las VLAN en la mejora del rendimiento de la red (Smith et al., 2018; Johnson & Lee, 2019).

Asimismo, respecto al indicador de respuesta de aplicaciones LAN de la dimensión disponibilidad de información el estudio muestra como disminuye de 77,35 a 15,79 milisegundos en promedio, en comparación con el resultado obtenido por Luján Vergara & Medina Osorio, 2015, en su tesis "Implementación de una red informática hospitalaria, usando metodología top-down network design; para el hospital Chancay y servicios básicos de salud", disminuye de 274,01 a 63 segundos en promedio el acceso a la información y respecto a (Socualaya, 2018) en su tesis "Diseño de una de red de área local para comunicación de datos del municipio de Iscos" disminuye el tiempo de respuesta del servidor de 52,53 a 30,58 milisegundos en promedio,

podemos afirmar que los tiempos de respuestas de las aplicaciones LAN son menores cuando se aplican VLAN en el diseño de red.

Otro hallazgo crucial de este estudio es el impacto positivo de las VLAN en la seguridad de la información. La segregación de diferentes tipos de tráfico y la creación de zonas de seguridad aisladas han minimizado el riesgo de accesos no autorizados y ataques cibernéticos. Los datos muestran una reducción en el número de incidentes de seguridad reportados, lo que sugiere que la implementación de VLAN ha sido efectiva en la protección de datos sensibles (Thompson & Rivera, 2020).

Según Martelo y colaboradores en su artículo "Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)", desarrolla un módulo de gestión documental para el proceso de implantación del sistema bajo los procedimientos del estándar ISO 27001. Permitió definir las dimensiones de la seguridad de la información para poder medirlas con sus respectivos indicadores con el pre y post de la implementación de redes virtuales locales en la red de datos de la Universidad Nacional de Huancavelica.

De acuerdo a Melchor en su artículo publicado "Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional", analiza el grado de influencia que tiene la seguridad en la administración y calidad de los datos de un sistema de información contable (SIC) en el desempeño organizacional de las pequeñas y medianas empresas (Pyme). Los resultados muestran el gran impacto que tiene la seguridad en la administración y calidad de la información para obtener una mayor productividad en las empresas. En este caso, se determinó el grado de influencia de la implementación de redes virtuales en la seguridad de la información, donde los resultados determinan una influencia positiva que tiene la implementación de redes virtuales locales en la disponibilidad,

integridad y confidencialidad de la información de la red de datos de la Universidad Nacional de Huancavelica.

Según Tejena-Macías, en el artículo "Análisis de riesgos en seguridad de la información", que luego de evaluar las diferentes metodologías de análisis de riesgos, determina que MAGERIT resulta ser la opción más efectiva y completa, ya que protege la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización. En este caso, se determinó luego del estudio que la implementación de redes virtuales locales es una herramienta necesaria para mejorar la disponibilidad, integridad y confidencialidad en cualquier red de datos.

6.1 Alcances del fortalecimiento de la seguridad de información usando redes virtuales locales

El estudio muestra que la implementación de redes virtuales locales (VLAN) influye positivamente en la seguridad de la información de la red de datos de la Universidad Nacional de Huancavelica, en cada una de sus dimensiones, evidenciando la mejora en la disponibilidad, integridad y confidencialidad de la información.

De igual manera, influye positivamente en la disponibilidad de la información, porque disminuye el tiempo de respuesta de las aplicaciones LAN de 77,35 a 15,79 milisegundos en promedio; reduce el tiempo de respuesta de las aplicaciones WAN de 246,12 milisegundos a 39,83 milisegundos en promedio; mejora la tasa de transferencia a nivel LAN de descarga de 18,78 a 30,11 Mbps en promedio, la de carga de 15,2 a 20,29 Mbps en promedio; también mejora la tasa de transferencia a nivel WAN en descarga de 1,32 a 2,33 Mbps, en carga de 0,88 a 1,73 Mbps en promedio. Por

último, mejora la cantidad de servicios ofrecidos por la red de 5 a 16 servicios de red.

Aunado a lo anterior, se demostró que las redes virtuales locales (VLAN) mejoran la integridad de la información mostrando la disminución de casos de alteraciones – perdida de datos de 1076 a 201 en un semestre determinado en la red de la Universidad Nacional de Huancavelica.

Como consecuencia, mejora la confidencialidad de la información, evidenciando la disminución del porcentaje de accesos a servicios no autorizados a nivel LAN de 88% a 9%; así mismo, muestra la disminución del porcentaje de accesos a servicios no autorizados a nivel WAN de 89% a 2% en la red de datos de la Universidad Nacional de Huancavelica.

En resumen, la adopción de redes virtuales locales en la Universidad Nacional de Huancavelica ha demostrado ser una estrategia efectiva para mejorar la eficiencia de los procesos informáticos y fortalecer la seguridad de la información. Estos hallazgos proporcionan una base sólida para justificar la inversión en tecnología de VLAN y sugieren áreas clave para futuras investigaciones y desarrollos.

6.2 Nuevos retos del fortalecimiento de la seguridad de información con el uso de redes virtuales locales

A pesar de los resultados positivos, es importante reconocer algunas limitaciones del estudio. La implementación de VLAN requiere una inversión inicial significativa en hardware y capacitación del personal, lo cual puede ser un obstáculo para organizaciones con recursos limitados. Además, la gestión y configuración de VLAN pueden ser complejas y requieren un mantenimiento continuo. Para futuras investigaciones, se recomienda centrarse en el impacto a largo plazo de las VLAN en diferentes tipos de organizaciones, así como en la comparación de esta tecnología con otras soluciones de seguridad y

optimización de redes. Además, sería beneficioso explorar métodos para simplificar la administración de VLAN y reducir los costos asociados con su implementación.

Asimismo, se recomienda el diseño e implementación de redes virtuales locales (VLAN) en cualquier red de datos de cualquier organización, las cuales permiten mejorar su administración y, sobre todo, mejorar la seguridad de la información.

Es importante el monitoreo constante de los tiempos de respuesta de las aplicaciones LAN y WAN, así como también de la tasa de transferencia LAN y WAN, así mismo implementar nuevos servicios de red para mejorar la competitividad de la organización.

De igual manera, se propone capacitar al personal para mejorar el manejo de la información en la red de datos, además de mejorar la confidencialidad de la información en la red de datos de la Universidad Nacional de Huancavelica.

Finalmente, se sugiere generar políticas de accesos a la red para evitar la alteración de la integración de la información.

Glosario

- **Información.** Todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración (Normas ISO 27001, 2013).

- **Seguridad.** El término seguridad proviene de la palabra securitas del latín. Cotidianamente, se puede referir a la seguridad como la reducción del riesgo o también a la confianza en algo o alguien (Academia de Networking de CISCO, 2005).

- **Seguridad de la información.** Según (Normas ISO 27001, 2013), la seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

- **Disponibilidad.** Según (Spagnoletti, 2007), la palabra "disponibilidad" proviene del latín valere, que significa "valer". En seguridad de la información, el término disponibilidad significa “acceso y uso oportunos y confiables de información, esto implica los aspectos que pertenecen a la usabilidad de los sistemas.

- **Integridad.** Según (Spagnoletti, 2007), define desde un punto de vista etimológico, la palabra “integridad” significa “solidez”, “integridad” y se deriva de la palabra latina tangere, que significa “tocar”. El prefijo 'in' indica una fuerza negativa o privativa, y por lo tanto el significado de la palabra "integridad" se puede asociar con ciertas connotaciones de la palabra "Intocable" que, a su vez, está relacionada con el concepto de integridad ética.

- **Confidencialidad.** El término "confidencialidad" se deriva del verbo latino confidere, que significa tener plena confianza o confianza. La confidencialidad es un principio fundamental de la seguridad de la información que tiene sus raíces en la mentalidad militar de mantener una autoridad y control sobre aquellos que tienen acceso a la información, sobre la necesidad de conocer la base (Spagnoletti, 2007).

- **Riesgo.** La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños (Olivares Serrano & Oncins Rodriguez, 2018).

- **Redes Virtuales Locales.** Según (CISCO, 2007), división lógica del dominio de broadcast a nivel de la Capa 2 del modelo OSI.

- **PING.** Arónimo de Packet Internet Groper, que significa buscador o rastreador de paquetes en redes, ping es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP. Se vale del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

- **Ancho de banda.** Cantidad de información que puede fluir a través de una conexión de red en un período dado (CISCO, 2007).

- **Tasa de transferencia.** La tasa de transferencia se refiere a la medida real del ancho de banda, en un momento dado del día (CISCO, 2007).

Referencias bibliográficas

Academia de Networking de Cisco Systems. (2005). Fundamentos de la seguridad de las redes. Madrid: Pearson Education S.A.

CISCO, A. d. (2007). CCNA EXPLORATION 4.0. Madrid: Pearson Education S.A. https://www.maestrodelacomputacion.net/cisco-ccna-exploration-4-0-en-espanol-aprende-redes-con-cisco/

Cordova, E. (2003). Plan de Seguridad Informatica para una Entidad Financiera. Tesis de pregrado. Universidad Nacional Mayor de San Marcos. Lima-Perú. http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/Cordova_RN/T_completo.pdf

Dulaney, E. (2011). Seguridad Informatica CompTIA Security+. Madrid: wiley publishing inc.

Espina García, Eduardo. (2006). "Arquitectura de seguridad de la Red Inalambrica Universitaria". (Tesis de Licenciatura). Universidad Nacional Autónoma de México, Facultad de Ingeniería, UNAM. Recuperado de https://repositorio.unam.mx/contenidos/3444226

Luján Vergara, E. A., & Medina Osorio, C. A. (2015). "Implementación de una red informática hospitalaria, usando metodología top-down network design; para el hospital chancay y servicios básicos de salud". universidad privada antenor orrego. Tesis de grado. Trujillo: Universidad Privada Antenor Orrego. http://repositorio.upao.edu.pe/bitstream/upaorep/2812/1/RE_ING.SIST_ESMYDER.LUJAN_CESAR.MDINA_RED.INFORMATICA_DATOS.pdf

Martelo, R., Madera, E. & Betín J. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). scielo, 26(2), 129-134. doi:10.4067/S0718-07642015000200015

Melchor, J., Lavín, J. & Pedraza, N. (2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. *Contaduría y administración*, *57*(4), 11-34.

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-10422012000400002&lng=es&tlng=es.

Méndez, R. (2006). La construcción de redes locales y los procesos de innovación como estrategias de desarrollo rural. *Problemas del desarrollo*, *37*(147), 217-240. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0301-70362006000400009&lng=es&tlng=es.

Normas ISO 27001. (2013). Normas ISO 27001. Obtenido de https://www.normas-iso.com/iso-27001/

Olivares Serrano, J., & Oncins Rodríguez, A. (2018). Seguridad informática - hacking ético. Barcelona: Ediciones ENI.

REAL ACADEMIA ESPAÑOLA: *Diccionario panhispánico del español jurídico (DPEJ)* [en línea]. https://dpej.rae.es/

Rodríguez, M. (2004). La influencia de la cultura organizacional en la implantacion de la estrategia de seguridad de la informacion en una organizacion financiera. Tesis de Maestría, Universidad Iberoamericana, México. http://ri.ibero.mx/bitstream/handle/ibero/898/014510s.pdf?sequence=1

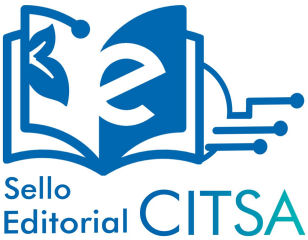
significados.com. (21 de 05 de 2020). significados.com. Obtenido de https://www.significados.com/seguridad/

Socualaya, A. O. (2018). "Diseño de una de red de área local para comunicación de datos del municipio de iscos". Tesis de pregrado. Huancayo: Universidad Peruana Los Andes.

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

Redes Virtuales Locales:

Fortaleciendo la seguridad de la Información



ISBN: 978-980-8050-09-7