UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creado por Ley Nº 25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA - SISTEMAS.

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

TESIS:

"MODELO DE ZONA DESMILITARIZADA Y EL CONTROL DE ACCESO EN LA RED DE DATOS DE LA CAMARA DE COMERCIO DE HUANCAYO"

LÍNEA DE INVESTIGACIÓN:

GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACION

PRESENTADO POR:

Bach. YARANGA MENDOZA FRANK CLAUDIO

Bach. LANDEO ROJAS MIRIAN LIZBETH

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

HUANCAVELICA, PERÚ

2021

UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creada por Ley N ° 25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA – SISTEMA

ACTA DE SUSTENTACIÓN DE PROYECTO DE INVESTIGACIÓN VIRTUAL

Mediante el aplicativo Google Meet con enlace: meet.google.com/nba-pfyu-ved, habilitado por Secretaría Docente de la Facultad de Ingeniería Electrónica – Sistemas, en mérito a la **Resolución de Consejo de Facultad Nº 143-2021-FIES-UNH** de fecha 18 de junio del 2021, a los 24 días del mes de junio del año 2021, a horas 11:00, se reunieron; el Jurado Calificador, conformado de la siguiente manera:

Presidente : Dr. John Fredy ROJAS BUJAICO
Secretario : Dr. Fernando Viterbo SINCHE CRISPÍN
Vocal : Mg. Roly Alcides CRISTOBAL LARA

Designados con Resolución N° 065-2019-DFIES-UNH, de fecha 30 de diciembre del 2019 del proyecto de investigación, Titulado:

"MODELO DE ZONA DESMILITARIZADA Y EL CONTROL DE ACCESO EN LA RED DE DATOS DE LA CÁMARA DE COMERCIO DE HUANCAYO"

Cuyo autor es el (los) graduado (s): Bachilleres:

Frank Claudio, YARANGA MENDOZA
Mirian Lizbeth, LANDEO ROJAS

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

Se dio inicio a la sustentación del proyecto de investigación en mención, a horas 11 con 02 minutos, concluyendo a horas 12 con 50 minutos.

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

APROBADO POR: MAYORÍA

Dr. John Fredy ROJAS BUJAICO
Presidente

Dr. Fernando Viterbo SINCHE CRISPIN
Secretario

Mg. Roly Alcides CRISTOBAL LARA
Vocal

TÌTULO

“MODELO DE ZONA DESMILITARIZADA Y EL CONTROL DE ACCESO EN LA RED DE DATOS DE LA CAMARA DE COMERCIO DE HUANCAYO”

AUTORES

Bach. YARANGA MENDOZA FRANK CLAUDIO

Bach. LANDEO ROJAS MIRIAN LIZBETH

ASESOR

DR. CARLOS ALCIDES ALMIDÓN ORTIZ

AGRADECIMIENTO

Queremos expresar nuestra gratitud a Dios, por ser nuestro guía y acompañarnos en el transcurso de nuestras vidas, brindándonos sabiduría y paciencia para culminar con éxito nuestras metas propuestas; agradecemos a nuestros padres: Gerardo y Ana; Gregorio y Carmen, a nuestros hermanos: Antony, Cristhian, Hanna; a nuestros familiares y amigos, por ser los pilares fundamentales y habernos apoyado incondicionalmente, pese a las adversidades. A la Prof. Elizabeth Vásquez Cabrera por ser la mejor maestra, amiga, madre y un ejemplo a seguir. Agradecemos a los docentes de la Escuela Profesional de Ingeniería de Sistemas, en especial al Dr. Fernando V. Sinche Crispin por motivarnos, por sus concejos, enseñanzas, apoyo y sobre todo amistad brindada en los momentos más difíciles de nuestras vidas.

Atentamente, los tesistas.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la investigación parte del problema: ¿Cuál es la influencia del modelo de zona desmilitarizada en el control de acceso en la red de datos de la cámara de comercio de Huancayo?; siendo el objetivo: Determinar la influencia del modelo de zona desmilitarizada en el control de acceso en la red de cámara de comercio, la investigación se ubica dentro del tipo Aplicada, nivel de investigación explicativo, con los métodos de investigación científico y explicativo, con un diseño de investigación pre experimental, con instrumento ficha de observación, y cuestionario. Se llegó a la conclusión, el Modelo de Zona Desmilitarizada influyó en el control de acceso a la red en un 66% en la autentificación de usuarios con una Sig.=0.00; Respecto a la sub variable Políticas de Acceso se pudo definir 6 protocolos asociados a 5 políticas con el uso del modelo de la zona desmilitarizada; Respecto a la sub variable Tráfico de paquetes través de su indicador Tráfico de Red se obtuvo una mejora en la velocidad de Descarga de datos de 13.02 Mbps y un mejora de 9.2 Mbps en la Carga de datos, con una Sig.=0.000.

Palabras clave: **Zona desmilitarizada; Red de datos; Cámara de Comercio, Tráfico de Red.**

ABSTRACT

The research starts with the problem: What is the influence of the demilitarized zone model on access control in the data network of the Huancayo chamber of commerce ?; The objective being: To determine the influence of the demilitarized zone model on access control in the chamber of commerce network, the research is located within the Applied type, explanatory research level, with scientific and explanatory research methods, with a pre-experimental research design, with observation sheet instrument, and questionnaire. It was concluded that the Demilitarized Zone Model influenced the network access control by 66% in the authentication of users with a Sig. = 0.00; Regarding the Access Policies sub-variable, it was possible to define 6 protocols associated with 5 policies with the use of the demilitarized zone model; Regarding the Packet Traffic sub-variable, through its Network Traffic indicator, there was an improvement in the data download speed of 13.02 Mbps and an improvement of 9.2 Mbps in the data load, with a Sig. = 0.000..

Keywords: Demilitarized zone; Data network; Chamber of Commerce, Network Traffic.

INTRODUCCION

El presente trabajo de investigación, trata sobre el control de acceso en la red de datos de la cámara de comercio de Huancayo. El modelo de zona desmilitarizara ayudara en el control de acceso en la red. Por ello el objetivo principal de la investigación es determinar la influencia del modelo de zona desmilitarizada en el control de acceso en la red de datos de la cámara de comercio.

La metodología general de la investigación es científica – aplicada, de nivel explicativo, el diseño es experimental, la técnica usada es la entrevista y como instrumento el cuestionario, la población está compuesta todos los hosts de la red de datos de la cámara de comercio de Huancayo. Para ello se tomó como muestra poblacional al total del host que pertenecen a la red de datos. A continuación, se detalla el esquema del contenido por capítulos:

En el capítulo I se da a conocer el planteamiento del problema, la formulación del problema, los objetivos, la justificación, el alcance y las limitaciones.

En el capítulo II se considera los antecedentes, las bases teóricas que sustentan nuestros resultados estadísticos, definición de términos básicos, el sistema de variables y sistema de hipótesis.

En el capítulo III se da a conocer, la referencia del marco metodológico.

En el capítulo IV se da a conocer los resultados y discusión, se presentan y se discuten los resultados obtenidos, es decir exposición de los resultados de la ejecución de la investigación. Finalmente, las conclusiones, referencias y anexos.

Los autores.

CAPITULO I:
PLANTEAMIENTO DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA:

El desarrollo tecnológico mundial ha generado la ferocidad del mercado actual, la volatilidad y fragilidad de las economías mundiales y la tendencia cambiante de las necesidades de consumo a nivel general, demandan innovación constante por parte de las organizaciones; El reto es inmenso: servicios cada vez más seguros, confiables y adaptables, puestos a disposición de los usuarios de manera ágil optimizando costos, no es una tarea fácil, lo anterior requiere de la disposición cada vez en mayor medida de investigación y tecnificación de procesos y capacidad de reingeniería constante

Así mismo, son innegables las bondades que supone la constante evolución de las tecnologías de información y comunicaciones (TIC's) para el entorno empresarial: difusión masiva, procesos de marketing cada vez más efectivos y de mayor alcance y mayor cobertura de los servicios a costos bajos son sólo algunos ejemplos de los innumerables beneficios que se pueden obtener al sacar provecho de la revolución de las TIC's.

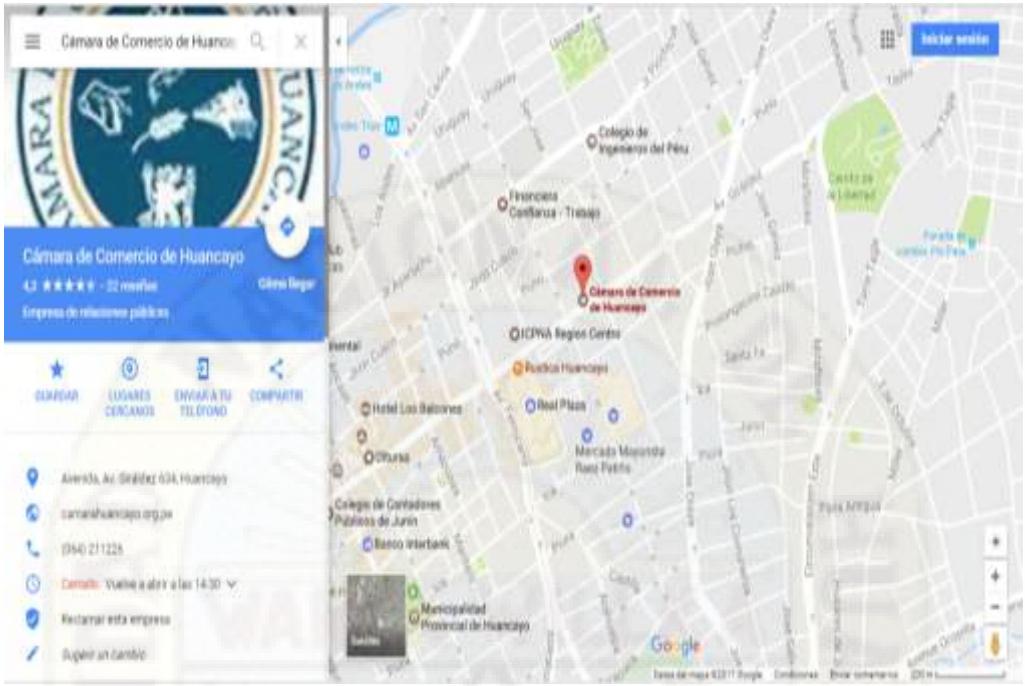
Ahora bien, hablando en términos de la importancia de la información como esencia pura e insumo básico de cualquier negocio, se pueden obtener invaluables ventajas al enfocar la cadena de valor y la planeación estratégica en

principios internacionales de buenas prácticas, principios estructurados cuya esencia es garantizar la integridad, disponibilidad y confidencialidad de la información: conservación de valores que históricamente se han materializado en el éxito de innumerables organizaciones en un sinnúmero de sectores de la industria.

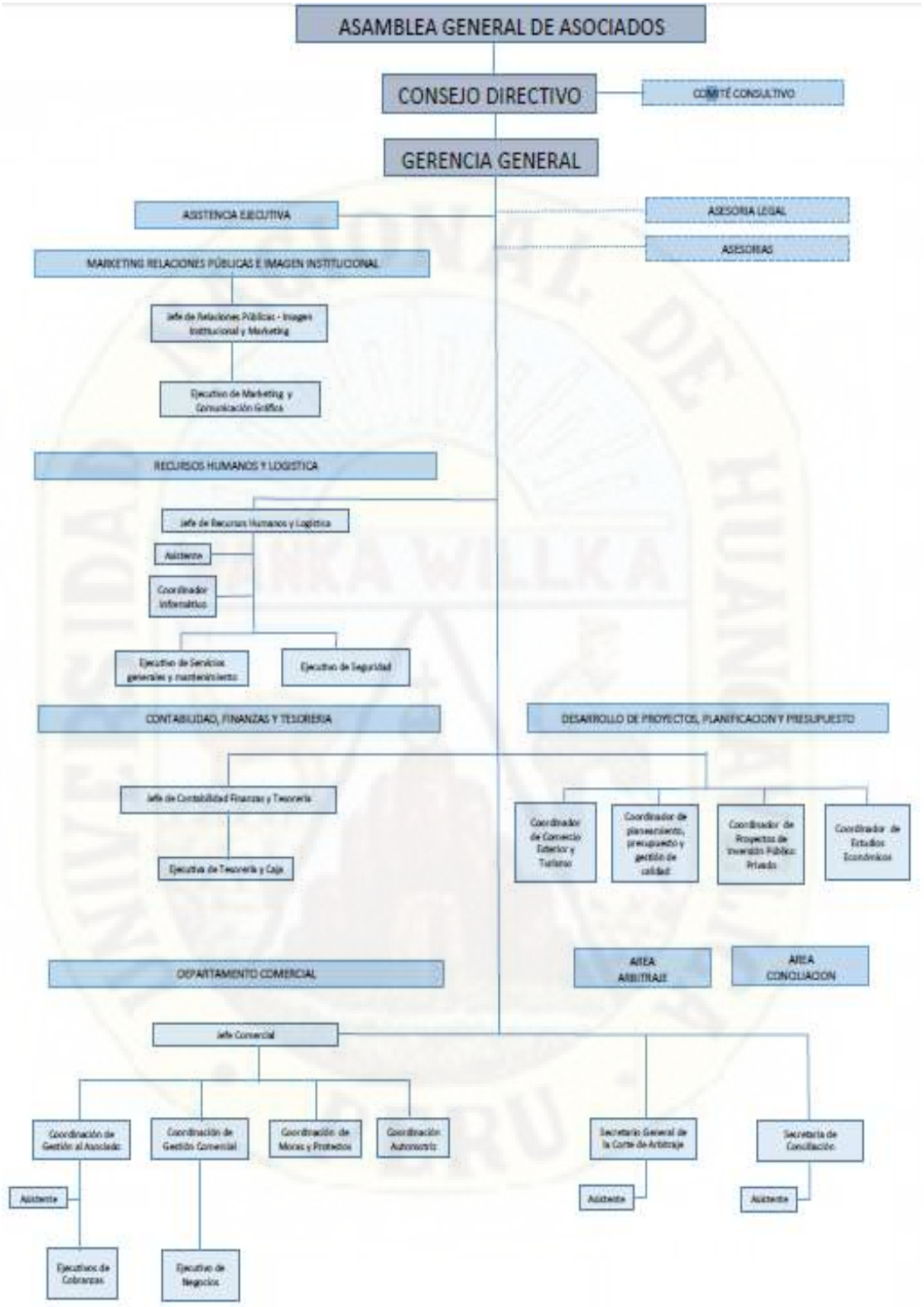
En el Perú el crecimiento tecnológico y el desarrollo económico sostenido ha traído la necesidad para muchas empresas de contar con más equipos de networking que provean conectividad a nuevas áreas, nuevas sucursales o simplemente la ampliación de red en las oficinas principales. Los sistemas de protección perimetral por lo general no son tomados en cuenta para proteger a las estaciones de trabajo y servidores, los cuales llegan a ser puntos perfectos para todo tipo de ataque.

La Cámara de Comercio de Huancayo como una asociación civil sin fines de lucro cuyo fin es impulsar el desarrollo empresarial sostenible a nivel local, regional y nacional, teniendo como ejes al ser humano y la empresa. Que contribuye al fortalecimiento empresarial mediante la asociatividad con responsabilidad social. Velando por los intereses del sector empresarial y promoviendo el desarrollo sostenible de la Región Central.

Como organización para cumplir sus fines la cámara de comercio tiene una infraestructura ubicada entre la calle Giráldez y Huancas – Huancayo.



Tiene la siguiente estructura organizacional.


ASAMBLEA GENERAL DE ASOCIADOS
CONSEJO DIRECTIVO
COMITÉ CONSULTIVO
GERENCIA GENERAL
ASISTENCIA EJECUTIVA
ASESORIA LEGAL
ASESORIAS
MARKETING RELACIONES PÚBLICAS E IMAGEN INSTITUCIONAL
Jefe de Relaciones Públicas - Imagen Institucional y Marketing
Ejecutivo de Marketing y Comunicación Gráfica
RECURSOS HUMANOS Y LOGISTICA
Jefe de Recursos Humanos y Logística
Asistente
Coordinador Informático
Ejecutivo de Servicios generales y mantenimiento
Ejecutivo de Seguridad
CONTABILIDAD, FINANZAS Y TESORERIA
DESARROLLO DE PROYECTOS, PLANIFICACION Y PRESUPUESTO
Jefe de Contabilidad Finanzas y Tesorería
Ejecutiva de Tesorería y Caja
Coordinador de Comercio Exterior y Turismo
Coordinador de planeamiento, presupuesto y gestión de calidad
Coordinador de Proyectos de Inversión Público Privado
Coordinador de Estudios Económicos
DEPARTAMENTO COMERCIAL
AREA ARBITRAJE
AREA CONCILIACION
Jefe Comercial
Coordinación de Gestión al Asociado
Coordinación de Gestión Comercial
Coordinación de Moras y Protestos
Coordinación Autoservicio
Secretario General de la Corte de Arbitraje
Secretaria de Conciliación
Asistente
Asistente
Asistente
Ejecutivos de Cobranzas
Ejecutivo de Negocios

La Cámara de Comercio de Huancayo tiene una infraestructura que consta de 3 bloques, una construcción de material Rustico de 2 pisos, una construcción de material noble de 3 pisos y en la parte posterior tiene un ambiente dividido en oficinas con material drywall, en estas construcciones viene funcionando la mayoría de oficinas.

Además, cuenta con una red de datos en el cual están interconectados los diferentes hosts como se describe a continuación:

- **Edificio de material rustico**

N° PISO	**NOMBRE DE LA OFICINA**	**N° HOST**
PISO 1	Sala de Directorio	2
	Asistente ejecutivo	2
	Gerencia Comercial	3
	contabilidad	3
	Datacenter	1
	Comercio Exterior y Turismo	2
	Modulo Comercial	8
	Cámaras modulo comercial	2
	Access point data center	1
PISO 2	Presidencia	2
	Gerencia General	3
	FEDACENTRO	3
	Secretaria General	2

	Contabilidad	2
	FOGAPI	3
	Access point Gerencia General	1
Total de Host		40

- **Edificio de material noble.**

N° PISO	**NOMBRE DE LA OFICINA**	**N° HOST**
PISO 1	sala de conciliación	2
	sala de conciliación exterior	2
	sala de audiencias	2
	corte de arbitraje	4
	Cámara exterior pasadizo	1
	Cámara exterior de arbitraje	1
	Cámara interior arbitraje	1
	acces point arbitraje	1
PISO 2	Auditorio menor	4
	Cámara Auditorio menor	1
	Access point auditorio menor	1
	Auditorio Junin	2
	Cámara Auditorio Junin	1
	acces point auditorio Junin	1

PISO 3	Auditorio Mayor	4
	Cámara Auditorio mayor	1
	Acces point auditorio mayor	1
Total de Host		30

- **Ambientes de la parte posterior**

N° PISO	**NOMBRE DE LA OFICINA**	**N° HOST**
PISO 1	Logística Entrega de Placas Caja	2
	Logística Entrega de Placas Almacén	2
	registro de protestos y mora	3
	Soporte Técnico	2
	Administración	2
	Cámara Logística Entrega de Placas	1
Total de Host		12

En esta plataforma tecnológica se cuenta con diferente software que pone a disposición de sus agremiados, estos están instalados en los servidores en el gabinete central de comunicaciones, esta infraestructura tecnológica tiene diversos problemas que se detallan a continuación:

- ✓ El acceso a la información es libre sin restricciones para el usuario que está conectado a la red de datos quedando vulnerable los diferentes aplicativos

informáticos y la información de la organización almacenada en los servidores.

- ✓ No se cuenta con políticas de acceso que garanticen la disponibilidad, integridad y confidencialidad de la información.
- ✓ Existen saturación de la red debido a los virus u otras intromisiones de usuarios no identificados debido a lo cual los servicios sufren un tiempo de inactividad.
- ✓ Usuarios descargan contenidos de la web (correos y archivos) sin restricción de tamaño, generando el colapso del tráfico de la red de datos.

1.2. FORMULACIÓN DEL PROBLEMA:

1.2.1. PROBLEMA GENERAL:

¿Cuál es la influencia del modelo de zona desmilitarizada en el control de acceso en la red de datos de la cámara de comercio de Huancayo?

1.2.2. PROBLEMAS ESPECÍFICOS:

a) ¿Cuál es la influencia del modelo de zona desmilitarizada en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo?

b) ¿Cuál es la influencia del modelo de zona desmilitarizada en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo?

c) ¿Cuál es la influencia del modelo de zona desmilitarizada en tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo?

1.3. OBJETIVOS:

1.3.1. OBJETIVO GENERAL

Determinar cuál es la influencia del modelo de zona desmilitarizada en el control de acceso en la red de datos de la cámara de comercio de Huancayo

1.3.2. OBJETIVOS ESPECÍFICOS

a) Determinar cuál es la influencia del modelo de zona desmilitarizada en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo
b) Determinar cuál es la influencia del modelo de zona desmilitarizada en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo.
c) Determinar cuál es la influencia del modelo de zona desmilitarizada en tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo

1.4. JUSTIFICACION

1.4.1. JUSTIFICACIÓN TEÓRICA

La investigación trata sobre la aplicación de un modelo de zona desmilitarizada en el control de acceso a la información y servicios en una red de datos.

Para ello se hace necesario desarrollar un marco teórico y conceptual revisando el material bibliográfico existente, contrastando las diversas corrientes, posiciones y estándares, a partir de ello comprobar su validez en la red de datos de la cámara de comercio de Huancayo, donde se realizó la investigación.

1.4.2. JUSTIFICACIÓN METODOLÓGICA

El tema de zonas desmilitarizadas en las redes de datos de las organizaciones es necesario para lograr la continuidad del negocio, la metodología aplicada ha sido la consulta a expertos del área de Tecnología de Información y Comunicaciones.

El proyecto de investigación a emprender expresa su justificación "metodológica" en el modo de mostrar una metodología de diseño de zonas desmilitarizadas en las redes de datos de las organizaciones.

1.4.3. JUSTIFICACIÓN PRÁCTICA

Para la cámara de comercio de Huancayo es muy importante determinar la manera óptima de administrar sus recursos, siendo el internet un recurso intangible importante en la actualidad, ya que permite el flujo de comunicaciones de las empresas con el resto del mundo. Sus clientes, proveedores y colaboradores, de no tener un control adecuado sobre este recurso, existen problema en el flujo de comunicaciones y podría estar siendo destinado a otras actividades diferentes a los intereses laborales de las empresas, perdiendo así rentabilidad, al no invertir este recurso de manera correcta.

En la actualidad el tema de la seguridad de la información es un tema determinante en la continuidad del negocio de las organizaciones. Los recursos de información (sistemas de información, base de datos, aplicaciones informáticas, redes informáticas, etc.) que sirven como apoyo para los empleados en su labor, deben estar disponibles. Por ello, el alcance de la investigación tiene repercusión práctica porque aporta información valiosa que servirá como modelo de como implementar zonas

desmilitarizadas para mejorar el control de acceso a la información y los servicios de las redes a nivel LAN y WAN de la organización.

CAPITULO II:
MARCO TEORICO

2.1. ANTECEDENTES

2.1.1. INTERNACIONALES

a) El ingeniero Diego Eduardo Cortés Robles (Universidad Andres Bello – Colombia - 2011), en su tesis: RED PERIMETRAL SEGURA DE LA CAMARA NACIONAL DEL COMERCIO. Concluye lo siguiente: "El siguiente Trabajo de Título, aborda el tema de la seguridad perimetral en redes empresariales, la cual hoy en día es importante desarrollar. La seguridad perimetral consiste en entregar algunos parámetros de seguridad como lo es, bloqueo de URL, paquetes, conexiones o aplicaciones, Anti-malware, anti-spam, o mantener vigilada nuestra red por medio de IPS. Cada uno de estos puntos son implementados según las amenazas detectadas en la Cámara Nacional de Comercio. Generando pruebas y recolectando información del funcionamiento de la red, se implementa un cortafuegos o más bien conocido en inglés como Firewa11, el cual fue elegido previo contrato existente antes de la realización de este proyecto, el cual realizará las funcionalidades que se necesitan para poder tener una red segura perimetralmente. Este dispositivo es un cortafuego WatchGuard, el cual posee las características necesarias para dar la solución de seguridad perimetral. Este dispositivo tiene la capacidad de

generar registros y con estos a su vez generar reportes entendibles para cualquier usuario que los desee revisar. Con esto podemos estar revisando la red y encontrar ciertas vulnerabilidades en algunos puntos de la red. Con esta red segura los usuarios pudieron aumentar su calidad de trabajo, ya que los sistemas mejoraron en tiempos de respuesta, al igual que los enlaces de intemet. Esto ayudo en mejorar el uso del ancho de banda hacia la nube".

b) El ingeniero David Mayorga Polo (Universidad Internacional SEK – Quito - 2008), en su tesis: ANALISIS, DISEÑO E IMPLEMENTACION DEL ESQUEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA UISEK. Concluye lo siguiente: "Las Instituciones educativas universitarias, además de perseguir el noble fin de educar a la gente, también tienen su parte administrativa, en la que se persiguen otros objetivos que vayan de la mano con el principal, que es educar. Las Universidades también son empresas, como cualquier otra, y necesitan proteger sus activos críticos de cualquier eventualidad que pueda suceder y afectar a su negocio. En la UISEK Ecuador Campus Miguel de Cervantes se consideran parte de los activos críticos los sistemas informáticos, no solo porque alojen información sensible, sino también porque son parte importante del proceso de educación de los alumnos y actualmente no se les da el suficiente resguardo, por lo que la presente investigación propone un esquema de seguridad perimetral para la red de datos del Campus; además del desarrollo de un manual de políticas de seguridad, así como un

plan de contingencia ante posibles desastres y un esquema de monitoreo proactivo de la seguridad perimetral establecida".

c) El Ingeniero Rodolfo Sirilo Córdova Gálvez, (UniversidadPolitécnica Católica del Ecuador - Ecuador – 2009), en su tesis: ANALISIS Y PROPUESTA DE MEJORAS PARA LA SEGURIDAD DE REDES INTERNAS LAN Y REDES PERIMETRALES (DMZ) UTILIZANDO TCP/IP Y GNU/LINUX EN PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES) DEL ECUADOR. Concluye lo siguiente: "Luego de las pruebas y evaluaciones realizadas, se determinó que ninguna de las herramientas libres por sí solas ofrece el 100% de seguridad, ni aun agregándoles todos los adicionales disponibles, cabe señalar que las herramientas propietarias tampoco ofrecen el 100% de seguridad, ya que encontramos vulnerabilidades de las mismas publicadas en el Internet. Agregando algunos adicionales a IPCOP (UrlFilter y CopFilter) se logra una seguridad del 89% en nuestra escala. De acuerdo al puntaje obtenido por IPCOP se concluye que, si existe una solución adecuada para los problemas relacionados con la seguridad perimetral en las redes DMZ y LAN de las pymes del Ecuador, y es la utilización de software libre basado en GNU/LINUX. La seguridad perimetral debe realizarse a nivel de red para prevenir ataques de hackers, las intrusiones o el robo de información en las conexiones remotas y a nivel de contenidos para prevenir el ingreso de código malicioso, spam y los contenidos web no deseados por las empresas. El nivel de seguridad implementado está directamente relacionado con las políticas y planes de seguridad que dispongan las

empresas ya que la seguridad no es un producto final, si no, es un proceso continuo".

2.1.2. NACIONAL

a) El ingeniero Jorge Luis Valenzuela Gonzales (Pontificia Universidad Católica del Perú – Lima. Perú - 2012), en su tesis: DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE UNA RED DE COMPUTADORAS PARA UNA PEQUEÑA EMPRESA. Concluye lo siguiente: "En el trabajo realizado se presenta una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. Se muestra además una simulación del diseño propuesto en un ambiente de pruebas controlado. En el primer capítulo se presenta el estado actual y riesgos de la información, y la importancia de la misma. Se presenta además la seguridad perimetral de la red de datos como parte de una problemática mayor. La seguridad de la información. En el segundo capítulo se muestra en detalle y de manera técnica, los riesgos, amenazas contra la integridad de una red de computadoras de una empresa pequeña y las contramedidas que pueden ser adoptadas. En el tercer capítulo se explica el escenario de trabajo, sus requerimientos y sus necesidades sin especificar aun producto alguno, sea software o hardware. En el cuarto capítulo se presentan los criterios que fueron tomados en consideración para la selección de la solución más idónea para el escenario planteado en el tercer capítulo. En el quinto capítulo, se desarrollan la política de seguridad que debe ser aplicada en la solución seleccionada en

el cuarto capítulo, se plasma en los componentes que la conforman y se evalúa su desempeño en un ambiente de pruebas. Finalmente se presenta las conclusiones que se desprenden del análisis del escenario planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado".

2.2. BASES TEÓRICAS.

2.2.1. CONTROL DE ACCESO A RED

Control de acceso a red (del inglés Network Access Control, NAC) es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red de acceso. (Cisco; 2013: 592)

a) Objetivo del Control de Acceso

El control de acceso a los nodos de la red de datos basado en puertos evita el eventual ingreso no autorizado de dispositivos de red. El control de acceso es logrado por el sistema, implementando autenticación de los Suplicantes que se conectan a los puertos controlados del sistema; a partir del resultado del proceso de autenticación, el sistema puede determinar si es o no el suplicante autorizado a acceder a sus servicios en ese puerto controlado. Si el suplicante no es autorizado para acceder, entonces tanto el sistema del Suplicante y el sistema del Autenticador ponen el estado de sus puertos controlados en no autorizado. En el estado no autorizado, el uso del puerto controlado está

restringido de acuerdo con el valor del parámetro OperControlledDirections asociado con ese puerto controlado, previniendo la transferencia de la información no autorizada entre el sistema Suplicante y los servicios ofrecidos por el sistema Autenticador.

El mecanismo definido puede ser aplicado para permitir que algún sistema se autentique a otro sistema, que está conectado a uno de sus puertos controlados. Los sistemas involucrados incluyen estaciones finales, servidores, routers y conmutadores.

b) Alcance de Operación del Control de Acceso por Puertos

La operación del control de acceso por puertos asume que los puertos en los cuales este opera, ofrecen una conexión punto a punto entre un único Suplicante y un único Autenticador. Es esta suposición que permite las decisiones de autenticación puedan ser realizadas por puerto. La autenticación de múltiples Suplicantes PAE conectados a un único Autenticador PAE está fuera del alcance de esta norma. Esta norma proporciona un protocolo para la información de autenticación de la comunicación entre un Suplicante que está conectado a un puerto de un sistema Autenticador y un Servidor Autenticador, y para controlar el estado de los puertos del sistema Autenticador y Suplicante, dependiendo del resultado de intercambio del protocolo. Esta norma no especifica la naturaleza de la información de autenticación que es intercambiado, ni las bases sobre el cual el servidor de Autenticación toma la decisión de su autenticación.

c) Definición de Sistemas y Puertos

Los Sistemas son dispositivos conectados a una LAN, que poseen uno o varios puntos de conexión, que se refieren como puertos de acceso a la red, o puertos. El puerto de un sistema provee la manera en el cual este puede acceder a los servicios ofrecidos por otros sistemas accesibles vía la LAN, y para suministrar la manera del cual este puede ofrecer servicios, o el acceso a los servicios suministrados por otros sistemas accesibles vía la LAN. El control de acceso a la red basado en puertos permite la operación de un puerto del sistema ser controlado a fin de garantizar que accedan a sus servicios, y/o accedan a los servicios de otros Sistemas, esto es solo permitido para sistemas que están autorizados a hacer eso.

Para los propósitos de describir la operación del control de acceso basado en puertos, un puerto de un sistema (o más exactamente, un PAE relacionado con un puerto) es capaz de adoptar uno o ambos de los dos distintos roles en una interacción de control de acceso:

- Autenticador: El puerto que hace cumplir la autenticación antes de permitir el acceso a los servicios que son permitidos vía ese puerto, adopta la función de Autenticador.
- Suplicante: El puerto que desea acceder a los servicios ofrecidos por el sistema del Autenticador, adopta la función de Suplicante. Una función adicional del sistema es descrita a continuación:
- Servidor de Autenticación: Realiza la función de autenticación necesaria para verificar las credenciales del Suplicante en representación del Autenticador e indica si el suplicante es autorizado para acceder a los servicios del Autenticador.

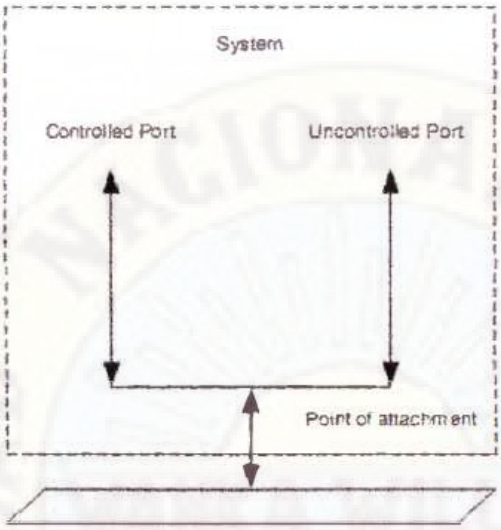
Como se puede ver desde estas descripciones, los tres roles son necesanos para completar un intercambio de autenticación. Un sistema dado puede ser capaz de adoptar uno o más de estos roles; por ejemplo, un Autenticador y un Servidor de Autenticación pueden estar localizados dentro del mismo sistema, permitiendo que el sistema ejecute la función de autenticación sin la necesidad de comunicarse con un servidor externo. Asimismo, un P AE puede adoptar el rol del Suplicante en algunos intercambios de autenticación, y el rol del Autenticador en otros. Un ejemplo de lo reciente puede ser encontrado en una red de área local conmutada, donde un nuevo conmutador adicionado a la red de área local necesitaría ser autenticado exitosamente por el P AE, asociado con el puerto del conmutador, el cual se conecta a la red de área local, antes que este pueda autenticar otros sistemas que se conectan a sus puertos.

d) Acceso Controlado y No Controlado

La figura 1. muestra que la operación del Control de Acceso por Puerto tiene el efecto de crear dos puntos de acceso distintos al punto del Sistema de conexión a la LAN. Un punto de acceso permite el intercambio no controlado de PDUs entre el Sistema y otros Sistemas en la LAN, independientemente del estado de autorización (puerto no controlado); el otro punto de acceso permite el intercambio de PDUs solo si el estado actual del puerto es autorizado (puerto controlado). Los puertos no controlado y controlado están considerado a ser parte del mismo punto de conexión a la LAN; cualquier trama recibido en el Puerto fisico es puesto a disposición de ambos puertos controlado y no controlado, sujeto al estado de autorización asociado con el puerto controlado.

Figura 1

Puertos controlado y no controlado



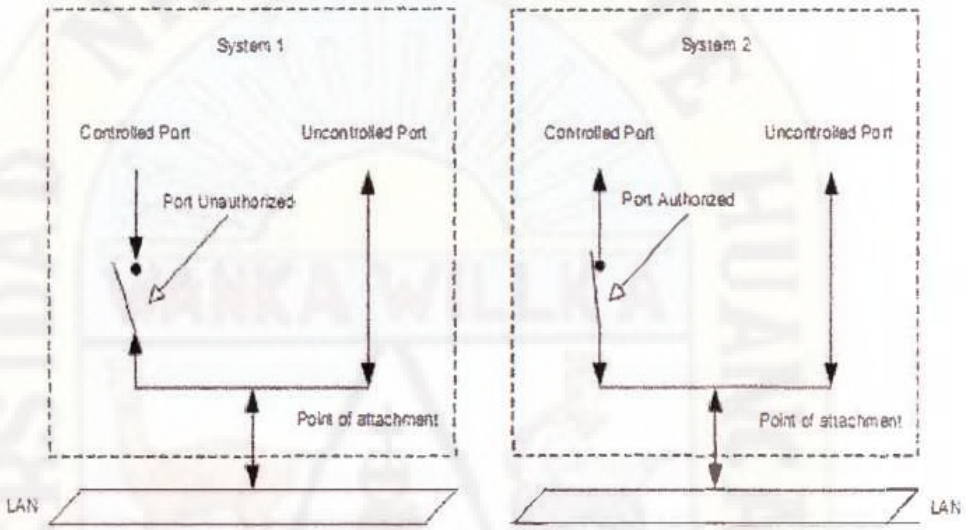
El punto de conexión a la LAN puede ser realizado mediante un puerto físico o lógico que puede proporcionar una conexión directa (punto a punto) a otro Sistema. Por ejemplo, el punto de conexión podría proveerse mediante una MAC en una infraestructura LAN conmutada. En los entornos LAN donde el método MAC permite la posibilidad de una relación punto-multipunto entre un Autenticador y un Suplicante (por ejemplo, en entornos de comunicación compartida), es necesaria la creación de una asociación distinta entre dos Sistemas para los mecanismos de control de acceso indicados. Un ejemplo es la asociación entre una estación y un punto de acceso inalámbrico JEEE 802.11.

La figura 2, muestra el efecto del AuthControlledPortStatus asociado con el Puerto controlado, representando aquel estado como un interruptor que puede ser conectado o desconectado, permitiendo o evitando el flujo de PDUs por dicho Puerto. La figura muestra dos sistemas, cada uno con un único Puerto; se asume que se ha fijado para ambos el parámetro OperControlledDirections. En el Sistema 1, el AuthControlledPortStatus asociado con el puerto controlado está no autorizado y por consiguiente está

deshabilitado (el interruptor esta desconectado); en el Sistema 2, el AuthControlledPortStatus está autorizado y por lo tanto habilitado (el interruptor está conectado).

Figura 2

Efecto del estado de autorización en puertos controlados



Además del AuthControlledPortStatus se tiene el parámetro AuthControlledPortControl asociado con el Puerto que permite el control administrativo sobre el estado de autorización del Puerto. Este parámetro puede tomar los valores ForceUnauthorized, Auto y ForceAuthorized; su valor defecto es Auto. La relación entre los parámetros AuthControlledPortStatus y AuthControlledPortControl es como sigue:

- El valor AuthControlledPortControl de ForceUnauthorized impone a la máquina de estados del Autenticador P AE a fijar el valor de AuthControlledPortStatus al nivel no autorizado.

- El valor AuthControlledPortControl de ForceAuthorized impone a la máquina de estados del Autenticador P AE a fijar el valor de AuthControlledPortStatus a nivel de autorizado.
- El valor AuthControlledPortControl de Auto permite a la máquina de estados del Autenticador P AE a controlar el valor de AuthControlledPortStatus para reflejar el resultado del intercambio de autenticación entre el Suplicante P AE, Autenticador P AE y el Servidor de Autenticación.

En los tres casos, el valor de AuthControlledPortStatus refleja directamente el valor de la variable portStatus asegurado por la máquina de estados del Autenticador P AE y Suplicante P AE. Tres factores contribuyen al valor de la variable portStatus:

- El estado de autorización de la máquina de estados del Autenticador P AE (sobrentendido como Autorizado si la máquina de estado no está implementada para ese puerto).
- El estado de autorización de la máquina de estados del Suplicante PAE (sobrentendido como Autorizado si la máquina de estado no está implementada para ese puerto).
- t) El estado del parámetro de control administrativo SuplicantAccessControl con Autenticador. Este parámetro tiene dos posibles valores Active e Inactive. El valor por defecto de este parámetro de control es Inactive; el soporte del valor Active es opcional. El valor de este parámetro surte efecto solo si ambas máquinas de estados Autenticador PAE y Suplicante PAE son

implementadas para este puerto. Si el valor del parámetro está en Inactive, entonces el valor del parámetro portStatus está determinado únicamente por el estado de autorización de la máquina de estados del Autenticador P AE. Si el valor del parámetro esta en Active, entonces el valor del parámetro porStatus está determinado por el estado de autorización de ambas máquinas de estado del Autenticador P AE y Suplicante P AE, si cualquiera de las máquinas de estado está en un estado no autorizado, entonces el valor de porStatus es no autorizado.

El valor del parámetro AuthControlledPortControl para cada puerto de un sistema puede ser anulado mediante el parámetro SystemAuthControl. Este parámetro puede tomar los valores Enabled y Disabled; su valor por defecto es Disabled.

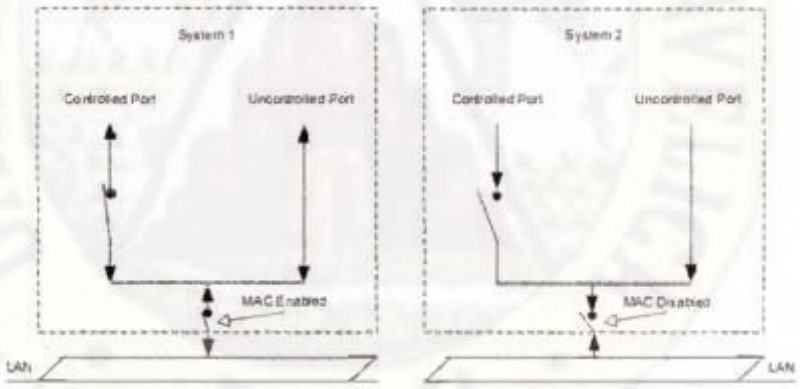
Si se fija SystemAuthControl como Enabled, entonces se permite la autenticación para el sistema, y el estado de autorización de cada Puerto es controlado de acuerdo al valor del parámetro AuthControlledPortControl del Puerto. Si se fija SystemAuthControl. como Disabled, entonces todos los puertos se comportan como si su parámetro AuthControlledPortControl estuviera fijado a ForceAuthorized. De hecho, colocar el parámetro SystemAuthControl a Disabled causa que se deshabilite la autenticación en todos los puertos, y fuerza a que todos los puertos controlados sean autorizados. Cualquier acceso a la LAN está sujeta al estado administrativo y operacional de la MAC asociado con el puerto, además a AuthControlledPortStatus. Si la MAC esta física o administrativamente inoperable, entonces no puede darse

ningún intercambio de protocolo de cualquier clase usando esa MAC en el puerto controlado o no controlado.

Esto está ilustrado en la figura 1.3; en el sistema 1, ambos puertos controlado y no controlado están aptos para accesar a la LAN, ya que el puerto controlado está autorizado, y la MAC abastece el punto de conexión a la LAN que esta operable. En el sistema 2 ni el puerto controlado ni el no controlado pueden acceder a la LAN, ya que la MAC que abastece el punto de conexión a la LAN esta inoperable. El estado inoperable de la MAC también ha causado al Autenticador P AE la transición del puerto controlado al estado no autorizado, como muestra en la figura 3.

Figura 3

Efecto de estados habilitado/deshabilitado MAC

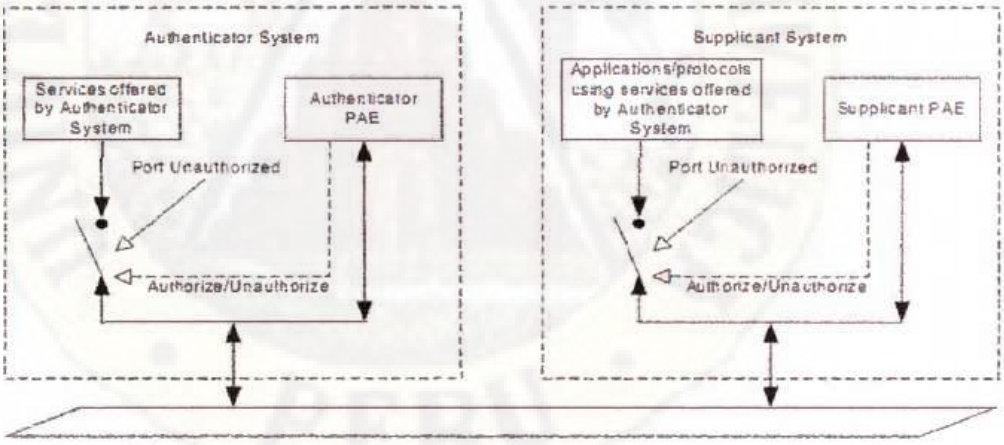


Los Autenticadores y Suplicantes P AE utilizan el puerto no controlado para el intercambio de información de protocolo con otro Suplicante o Autenticador P AE. El intercambio de protocolo entre el Autenticador PAE y el Servidor de autenticación (si el servidor no está colocado con el Autenticador P AE) se puede dar vía uno o varios de los Puertos controlados o no controlados del Sistema.

Se espera que la mayoría de los intercambios de protocolos conducidos por otras funciones del Sistema hagan uso de uno o varios de los puertos controlados del Sistema. Sin embargo, un protocolo dado puede necesitar evitar la función de autorización y hacer uso del Puerto no controlado. La figura 4 muestra el uso de los puertos controlados y no controlados en un sistema Autenticador y un sistema Suplicante, y la capacidad de los P AEs para cambiar el estado de autorización del puerto controlado dependiendo del resultado de un intercambio de autenticación; la figura también da un ejemplo de las entidades del protocolo (las P AEs) que requieren el uso de un puerto no controlado de acuerdo al comportamiento del intercambio de sus protocolos.

Figura 4

Uso de los puertos controlado y no controlado

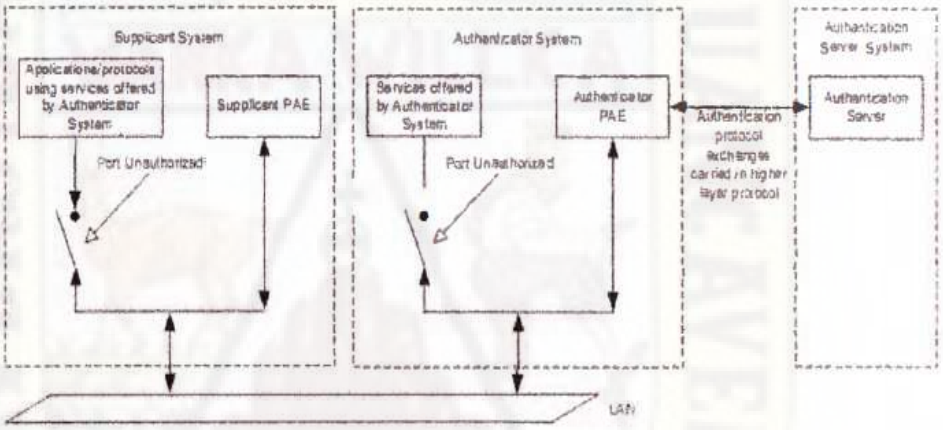


La figura 5, muestra las relaciones entre el Suplicante, Autenticador y Servidor de Autenticación, y el intercambio de información entre ellos. En esta muestra, ambos puertos controlados del Autenticador y del Suplicante están en el estado no autorizado y por consiguiente son deshabilitados desde el punto de vista del acceso por el sistema del Suplicante a los servicios ofrecidos por el

sistema del Autenticador. Los dos P Aes hacen uso de sus puertos no controlados para comunicarse el uno al otro, usando un protocolo de autenticación transportado en la capa de enlace de datos, y el Autenticador P AE se comunica con el Servidor de Autenticación usando un protocolo autenticación transportado en un protocolo de capa superior.

Figura 5

Roles Autenticador, Suplicante y Servidor Autenticación



La comunicación entre el Autenticador y el Servidor de Autenticación puede hacer uso del servicio de una LAN, o puede usar algún otro canal de comunicación. En caso que el Servidor de Autenticación sea colocado con el Autenticador, el intercambio del protocolo de autenticación entre estas dos entidades no será necesario.

e) Control de Transmisión y Recepción

El grado al que toma lugar el intercambio de protocolo en el puerto controlado está afectado por el estado de autorización que es determinado por dos parámetros de dirección controlada, asociado con cada puerto controlado: un parámetro AdminControlledDirections y un parámetro OperationalControlledDirections. Estos parámetros determinan si un puerto controlado que no es autorizado ejerce el control de la comunicación en ambas direcciones (deshabilitando las tramas entrantes y salientes), o solo en la dirección de entrada (deshabilitando solo la recepción de tramas entrantes). Los parámetros de dirección controlados pueden tomar uno de dos valores posibles, Both y In. La relación entre estos dos parámetros, y el significado de sus valores, es como sigue:

- AdminControlledDirections = Both. Esto indica que se requiere que el control sea aplicado sobre ambos tráficos de entrada y salida a través del puerto de control. El valor de OperControlledDirnctions es absolutamente puesto igual para Both si AdminControlledDirections es puesto igual para Both.
- AdminControlledDirections = In. Indica que se requiere que el control sea aplicado sólo sobre el tráfico de entrada a través del puerto controlado. Si se fija AdminControlledDirections a In, el valor de OperControlledDirections es puesto a In en la inicialización y cuando la MAC del puerto esté operable. Sin embargo, se fija el valor de OperControlledDirections a Both, si se dá alguna de las siguientes condiciones:

- El puerto es un puerto del conmutador, y la máquina de estado de detección del conmutador, detecta la presencia de otro conmutador conectado al puerto.
- El puerto es un puerto del conmutador y el parámetro de puerto Edge Port es falso.
- La MAC del puerto no es operable.

f) Entidad de Acceso por Puerto (P AE)

Una Entidad de Acceso por Puerto (P AE) maneja los algoritmos y protocolos asociados con el Protocolo de Control de Acceso por Puerto. Un P AE existe para cada puerto de un sistema que soporta la funcionalidad del control de acceso por puerto en la función Suplicante, la función Autenticador, o ambos. En la función Suplicante, un P AE es responsable de proporcionar la información a un Autenticador que establecerá sus credenciales. Un P AE que realiza el papel Suplicante en un intercambio de autenticación se conoce como un Suplicante P AE. En la función Autenticador, un P AE es responsable de la comunicación con un Suplicante, y el envío de la información recibida del Suplicante a un servidor de autenticación para la verificación de credenciales y consiguiente estado de autorización. Un P AE que realiza el papel Autenticador en un intercambio de autenticación se conoce como un Autenticador P AE.

Ambas funciones P AE controlan el estado autorizado/no autorizado del puerto controlado dependiendo del resultado del proceso de autenticación. Si un puerto controlado dado tiene ambas funcionalidades tanto Autenticador P

AE como Suplicante P AE asociadas a este, ambos P AEs deben estar en el estado Autorizado para que el puerto controlado sea Autorizado.

2.2.2. ZONA DE SEGURIDAD

Una zona es una colección de uno o más segmentos de la red que comparten los requisitos de seguridad idénticos. Para los segmentos de red del grupo dentro de una zona, debe asignar interfaces lógicas desde el dispositivo a una zona.

Las zonas permiten la segregación de seguridad de red. Las políticas de seguridad se aplican entre las zonas para regular el tráfico a través de la seguridad plataforma que ejecuta el sistema operativo Junos. Por defecto, todas las interfaces de red pertenecen a la zona nula definida por el sistema. Todo el tráfico hacia o desde la zona nula se rechaza. Interfaces especiales, incluyendo la gestión de la interfaz Ethernet presente en fxp0 algunas plataformas SRX Series, interfaces de tela clúster de chasis, y las interfaces del sistema em0 internos no pueden ser asignados a una zona.

Zonas e Interfaces

Puede asignar una o más interfaces lógicas a una zona. También puede asignar una o más interfaces de lógicas a una instancia de enrutamiento.

No se puede asignar una interfaz lógica a múltiples zonas o múltiples instancias de enrutamiento. También debe asegurarse de que todos los de una zona es interfaces lógicas están en una sola instancia de enrutamiento.

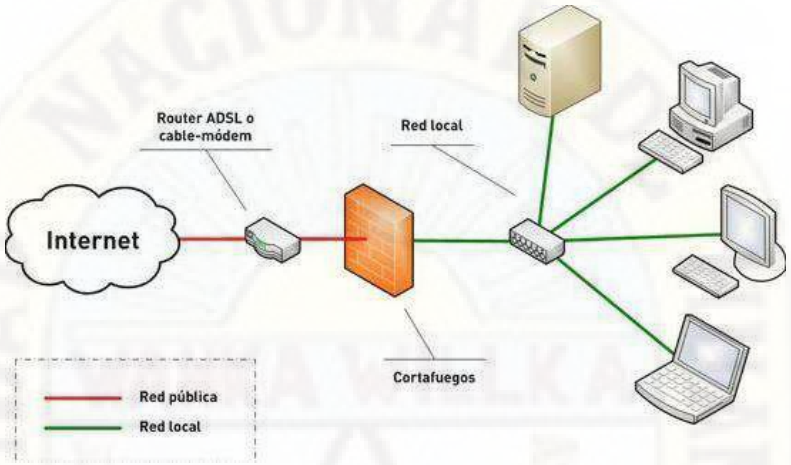
Tipos de zona de seguridad

Las zonas dentro del sistema operativo Junos se pueden subdividir en dos categorías definidas por el usuario y definida por el sistema. Puede configurar zonas definidas por el usuario, pero no se puede configurar zonas definidas por

el sistema. Se puede subdividir la categoría definida por el usuario en la seguridad y zonas funcionales. Este grafico lo podemos observar en la figura

Figura 6

Security zones



Las zonas de seguridad son una colección de uno o más segmentos de red que requiere regulación del tráfico entrante y saliente a través del uso de políticas. La seguridad en las zonas se aplica al tráfico de tránsito, así como el tráfico destinado a cualquier interfaz perteneciente a la zona de seguridad. Son necesario una o más políticas de seguridad para regular la intra-zona y el tráfico interzonal.

Functional Zones

Las zonas funcionales son zonas de propósito especial que no se pueden especificar en las políticas de seguridad. Tenga en cuenta que el tráfico en tránsito no utiliza zonas funcionales. Mientras que la interfaz Ethernet gestión fxp0 está fuera de banda por defecto, la zona de gestión que permite asignar

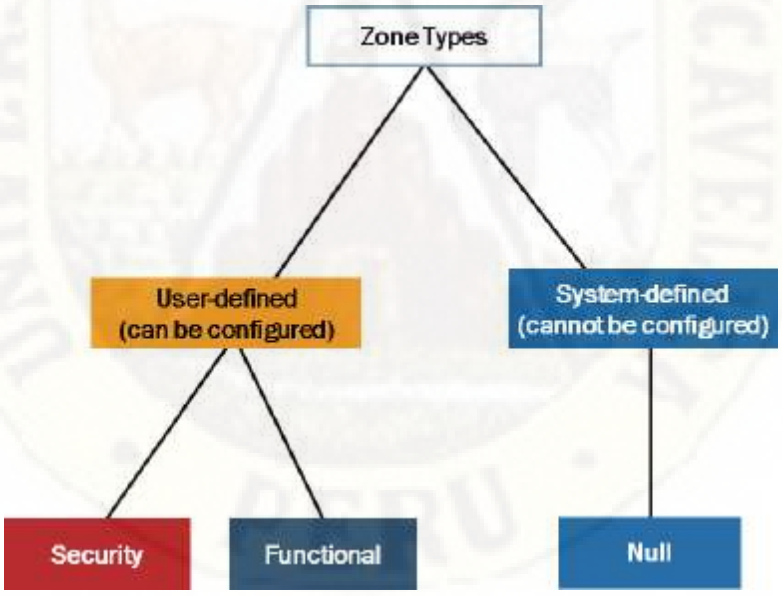
otras interfaces de red el mismo comportamiento de aislar el tráfico de gestión del tráfico de tránsito.

Zone Null

Actualmente existe una sola zona definida por el sistema, la zona Null. Por defecto, todas las interfaces pertenecen a la zona Null. No se puede configurar dicha zona. Cuando se elimina una interfaz de una zona, el software asigna de nuevo a la zona Null. El sistema operativo Junos rechaza todo el tráfico hacia y desde las interfaces que pertenece a la zona Null. 20 32

Figura 7

Esquema de los tipos de zona Fuente: juniper jncis-sec



Políticas de Seguridad

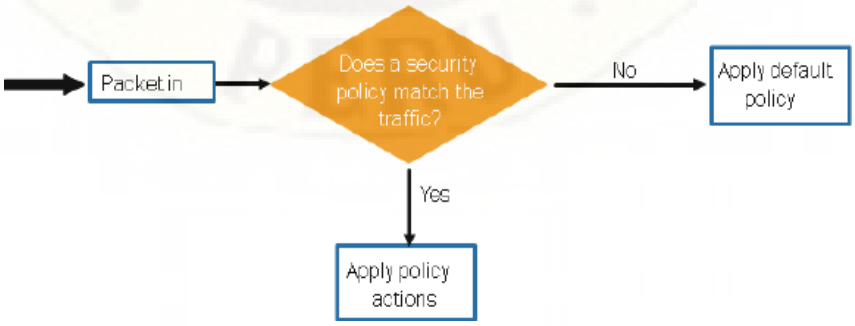
Una política de seguridad es un conjunto de instrucciones que controla el tráfico de una fuente específico a un destino específico utilizando un determinado Servicio. Si llega un paquete que coincida con esas

especificaciones, el dispositivo de la serie SRX realiza la acción en la póliza. Las políticas de seguridad de la red son de gran valor para la funcionalidad de red segura. Las políticas de seguridad de red contorno de toda la red recursos dentro de una empresa y el nivel de seguridad requerido para cada recurso. El sistema operativo Junos proporciona un conjunto de herramientas para poner en práctica una política de seguridad de la red dentro de su organización. Hace cumplir las políticas de seguridad de un conjunto de reglas para el tráfico de tránsito, identificar las que el tráfico puede pasar a través del servidor de seguridad y las medidas tomadas en el tráfico a medida que pasa a través del firewall.

El sistema operativo Junos para las plataformas de seguridad siempre se examina el tráfico de tránsito mediante el uso de políticas de seguridad. Como se ilustra en el gráfico, en caso de Ningún resultado existe en la política de seguridad, la política de seguridad predeterminada se aplica al paquete como podemos apreciar en la figura 8

Figura 8

Esquema de la exanimación del paquete Fuente juniper jncis-sec



Políticas de seguridad por defecto. En la configuración por defecto de fábrica en las plataformas tiene tres políticas de seguridad pre configuradas las cuales son:

1. Trust-to-trust zonepolicy: Permite todo el tráfico intra-zona dentro de la zona de confianza;
2. Trust-to-untrustzonepolicy: Permisos de todo el tráfico de la zona Trust a la zona Untrust; y
3. Untrust-to-trust zonepolicy: niega todo el tráfico de la zona Untrust a la zona Trust.

Contextos de políticas de seguridad.

Al definir una política, debe asociarlo con una zona de origen, cuyo nombre este en la zona. Además, debe definir una zona de destino. Dentro de una dirección de las zonas de origen y de destino, puede definir más de una póliza, se refiere como un conjunto ordenado de las políticas, que el sistema operativo Junos se ejecuta en el orden de su configuración. Recordemos que una zona es una colección de múltiples interfaces lógicas con los requisitos de seguridad idénticos. El sistema operativo Junos siempre comprueba todo el tráfico de tránsito intra-zona-y-interzona mediante el uso de políticas de seguridad.

Componentes de una política de seguridad.

Dentro del título del contexto definido, cada política está marcada con un nombre definido por el usuario, el nombre definido por el usuario es una lista de coinciden con los criterios y las acciones especificadas, similar a un Junos política de enrutamiento. Una diferencia importante es que cada política de

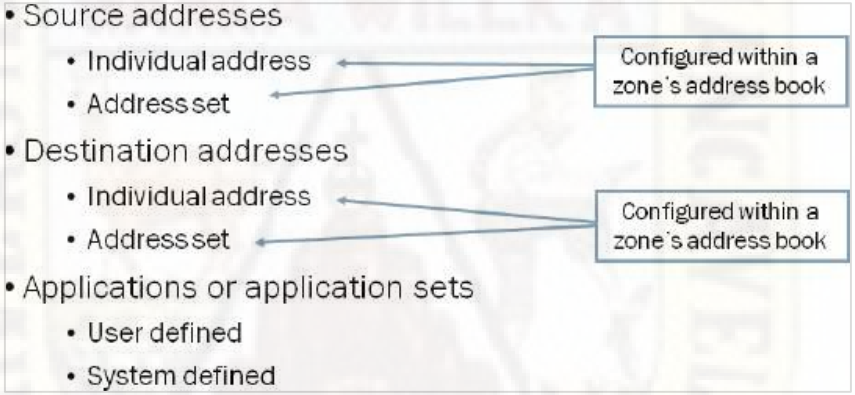
seguridad debe contener una dirección de origen coincidente, dirección de destino y aplicación. Acciones para tráfico que coincide con los criterios especificados incluir permiso, negar, rechazar, registro, o contar.

El sistema operativo Junos también utiliza la política para invocar la aplicación de políticas de prevención y detección de intrusión (IDP).

Gestión de características (UTM) para dispositivos de rama y la autenticación de servidor de seguridad.

Figura 9

Componentes de una política Fuente: juniper jncis-sec 20 35



Cada una de las políticas definidas debe incluir los siguientes criterios:

- Direcciones de origen: Este criterio puede ser en forma de conjunto de direcciones o direcciones individuales. Puede agrupar direcciones individuales en conjuntos de direcciones.
- Direcciones de destino: Este criterio puede ser en forma de conjunto de direcciones o direcciones individuales. Puede agrupar direcciones individuales en conjuntos de direcciones.
- Las aplicaciones o conjuntos de aplicaciones: Este criterio puede ser definida por el usuario o por el sistema. Los soportes del sistema

operativo Junos de aplicaciones por defecto y los conjuntos de aplicaciones, se hace referencia con el formato junos-aplicación, donde la aplicación es el nombre de la aplicación real. También podemos definir nuestras propias aplicaciones.

- Acciones básicas de una política.
- Cada política tiene una lista de acciones básicas asociadas con ella. Las acciones son las siguientes:
- Permit: Permite que el flujo de tráfico;
- Deny: Resultados en una caída de paquetes.
- Reject: Resultados en una gota de paquetes y el envío de un mensaje de control de Internet Protocolo (ICMP) inalcanzable mensaje para el tráfico UDP y el mensaje de un tiempo de opresión de registro TCP reset (RST) para el tráfico TCP.

2.3. DEFINICIÓN DE TÉRMINOS.

a) Red. - Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes. En inglés se le conoce como Network. El internet está compuesto de miles de redes, por lo tanto, al internet también se le conoce como "la red" (Cisco; 2012: 10)

b) Servicio. - El conjunto de funciones ofrecidas al usuario por una organización constituye un servicio. (ITU; 2008: 04)

c) Tecnología. - Con frecuencia conocimiento científico, pero también conocimiento organizado en otra forma, aplicado sistemáticamente a la producción y distribución de bienes y servicios. (Lemarchad; 2008: 23)

2.4. SISTEMA DE HIPÓTESIS.

2.4.1 HIPÓTESIS GENERAL

El modelo de zona desmilitarizada influye positivamente en el control de acceso en la red de datos de la cámara de comercio de Huancayo.

2.4.2 HIPÓTESIS ESPECÍFICAS

a) Un modelo de zona desmilitarizada influye positivamente en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo.

b) Un modelo de zona desmilitarizada influye positivamente en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo.

c) Un modelo de zona desmilitarizada influye positivamente en el tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo

2.5. SISTEMA DE VARIABLES.

Y=F(X)

a. Y= Control de acceso en la red de datos de la cámara de comercio de Huancayo**.** Variable dependiente

b. **X =** Modelo de zona desmilitarizada**.**

MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES.

VARIABLES	CONCEPTUALIZACÍON	OPERACIONALIZACION			
		DIMENSIONES	INDICADORES	TÉCNICA DE RECOLECCIÓN DE DATOS	INSTRUMENTO
Variable Independiente Modelo de zona desmilitarizada	Modelo de zona desmilitarizada Es un modelo protección de red de computadoras que permite aislar la zona de servidores, usuario y el internet (Cisco; 2013: 592)	• Sin presencia • Con presencia		• Técnica de la Observación	• Fichas de observación.

Variable dependiente Control de acceso a la red	**Control de acceso** Control de acceso a red (del inglés Network Access Control, NAC) es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales TANENBAUM; 2003: 347	• Autentificación de usuarios	• % Acceso de paquetes de usuarios no autorizados a nivel LAN • % Acceso de paquetes de usuarios no autorizados a nivel WAN	Observación	• Fichas de observación.
		• Políticas de acceso	• Nro. de políticas de acceso. • Nro. de protocolos asociados a las políticas		
		• Trafico de paquetes.	• Trafico de red.		

CAPITULO III:
MATERIALES Y MÉTODOS

3.1. AMBITO DE ESTUDIO

El estudio se desarrollará en la red de datos de la cámara de comercio de Huancayo.

3.2. TIPO DE INVESTIGACIÓN:

El tipo de investigación es Aplicada, porque la obtención de la información necesaria para la presente investigación además será realizada por medio de una **investigación explicativa y tecnológica,** aplicando conocimiento científico y tecnológico. A respecto (Vargas Cordero, 2009), define: "Consiste en mantener conocimientos y realizarlos en la práctica además de mantener estudios científicos con el fin de encontrar respuesta a posibles aspectos de mejora en situación de la vida cotidiana.*"*

3.3. NIVEL DE INVESTIGACION:

En el nivel de investigación se plantea explicativo; debido a que se realizará una evaluación de del servicio actual de la infraestructura de redes actual y luego se implementaran redes privadas virtuales para evaluar su influencia en la calidad de servicio, al respecto (Arias, 2006) define: "La investigación explicativa se encarga de buscar el porqué de los hechos mediante el establecimiento de relaciones causa-efecto.

En este sentido, los estudios explicativos pueden ocuparse tanto de la determinación de las causas (investigación post facto), como de los efectos (investigación experimental), mediante la prueba de hipótesis. sus resultados y conclusiones constituyen el nivel más profundo de conocimientos.”.

3.4. MÉTODO DE INVESTIGACIÓN:

Método general: Método científico.

Método específico: Método explicativo.

3.5. DISEÑO DE INVESTIGACIÓN

La investigación pertenece al diseño Pre Experimental, según los autores, (Palella Stracuzzi & Martins Pestana, 2012) define: *“*El diseño pre experimental es aquel según el cual el investigador manipula una variable experimental no comprobada, bajo condiciones estrictamente controladas. Su objetivo es describir de qué modo y porque causa se produce o puede producirse un fenómeno”.

Esquemáticamente el diseño es:

$$G \quad = O_1 \quad X \quad O_2$$

Donde:

G = Significa grupos de sujetos

O1 = Pre_test

O2 = Pos_test

X = Aplicación de la variable Independiente (Modelo de Zona desmilitarizada)

3.6. POBLACIÓN, MUESTRA Y MUESTREO

Población: todos los hosts de la red de datos de la cámara de comercio de Huancayo.

Muestra: todos los hosts de la red de datos de la cámara de comercio de Huancayo.

3.7. TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS

TÉCNICAS

Entrevista: con el objetivo de realizar una serie de preguntas y obtener como resultado el número de consultas que este tuvo que ejecutar para poder obtener la información que se necesita.

INSTRUMENTO

Cuestionario de entrevista: Un instrumento formado por una serie de preguntas en su mayoría cerradas que se contestan de manera individual y personal por escrito a fin de obtener la información necesaria para la realización de una investigación.

Ficha de observación: Sirve para recolectar datos sobre una temática específica, estos datos se obtienen mediante la observación.

3.8. TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS

Estadística Descriptiva: es un conjunto de técnicas numéricas y gráficas para describir y analizar un grupo de datos, sin extraer conclusiones (inferencias) sobre la población a la que pertenecen. En este tema se introducirán algunas técnicas descriptivas básicas, como la construcción de tablas de frecuencias, la elaboración de gráficas y las principales medidas descriptivas de centralización, dispersión y forma que permitirán realizar la descripción de datos.

Estadístico de la R de Pearson: En estadística, el coeficiente de correlación de Pearson es una medida de dependencia lineal entre dos variables aleatorias cuantitativas. A diferencia de la covarianza, la correlación de Pearson es independiente de la escala de medida de las variables.

De manera menos formal, podemos definir el coeficiente de correlación de Pearson como un índice que puede utilizarse para medir el grado de relación de dos variables siempre y cuando ambas sean cuantitativas y continuas.

3.9. DESCRIPCIÓN DE LA PRUEBA DE HIPÓTESIS

Para contrastar la descripción de la prueba de la hipótesis se utilizó la prueba de la "t" para una muestra relacionada. Siguiendo los siguientes pasos:

a) Planteamiento de las hipótesis

b) Elección del tipo de prueba

c) Decisión estadística

d) Nivel de significancia

e) C5alculo del valor de “z”

f) Contrastación de hipótesis

g) Decisión

CAPITULO IV
DISCUSIÓN DE RESULTADOS

4.1 PRESENTACIÓN E INTERPRETACIÓN DE DATOS.

En esta fase de estudio se realizó el diseño del modelo de zona desmilitarizada, luego se presentará e interpretará los datos obtenidos para lo cual se utilizó diferentes aplicaciones para su mayor confiabilidad tales como: Packet Tracert 7.1, Excel y SPSS. Los datos se obtuvieron a través de pruebas realizadas en la red WAN y LAN de la cámara de comercio Huancayo, donde se evaluó el control de accesos a la red como está ahora y luego con el modelo de red propuesto utilizando Zona desmilitarizada, que consistió en medir los parámetros de control de acceso establecidas por la Unión Internacional de Telecomunicaciones (ITU). A continuación, presentamos el diseño del modelo.

4.1.1 DISEÑO DEL MODELO DE ZONA DESMILITARIZADA.

La Cámara de Comercio de Huancayo fue fundada el 15 de enero de 1924 como una asociación civil sin fines de lucro cuyo fin es impulsar el desarrollo empresarial sostenible a nivel local, regional y nacional, teniendo como ejes al ser humano y la empresa.

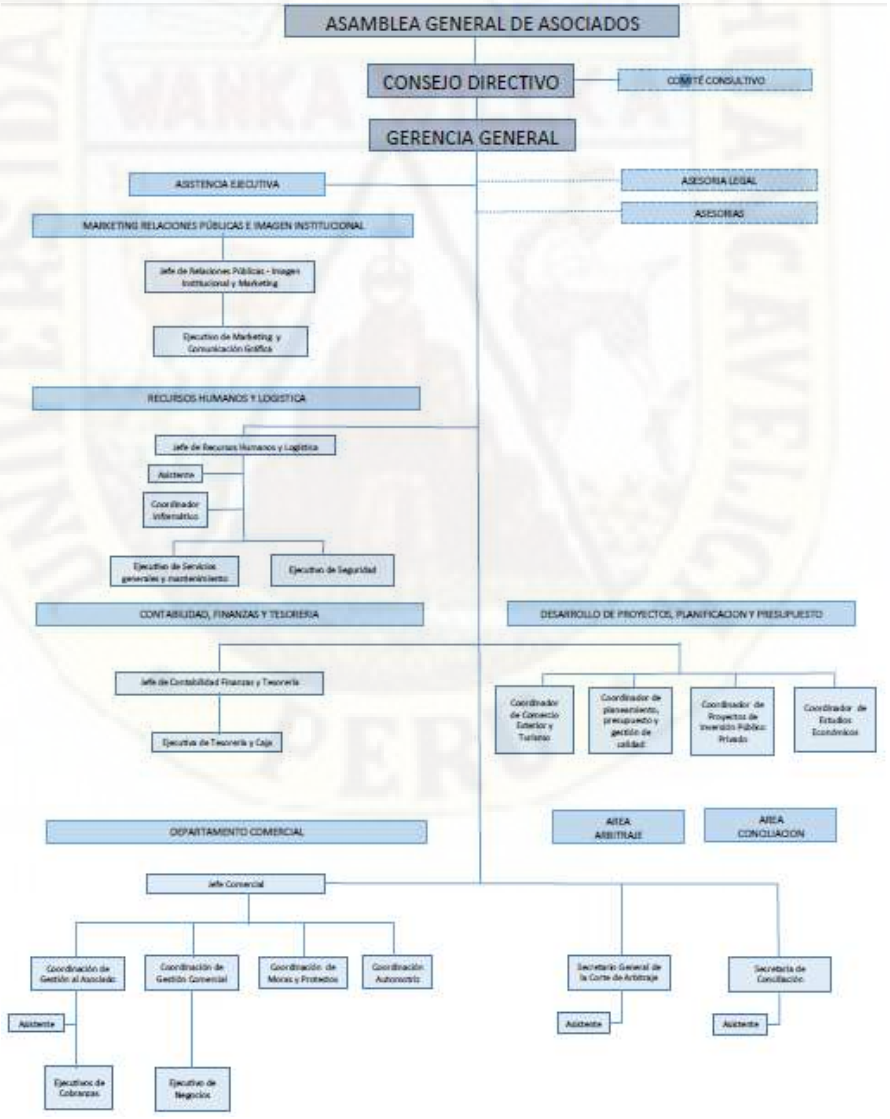
El 19 de diciembre de 1988, en Sesión Extraordinaria, de Junta Directiva se constituye y aprueba los Estatutos de la Cámara reconociéndosele como Asociación Civil Gremial, Persona Jurídica de Derecho Privado, sin fines de lucro, constituida con

arreglo a la libertad de Asociación que ampara la Constitución Política del Perú y el Código Civil.

MISIÓN

Somos un gremio empresarial, que contribuye al fortalecimiento empresarial mediante la asociatividad con responsabilidad social. Velando por los intereses del sector empresarial y promoviendo el desarrollo sostenible de la Región Central.

Organigrama



A) DIAGNÓSTICO DE LA RED ACTUAL.

La Cámara de Comercio de Huancayo tiene una infraestructura que consta de 3 bloques una construcción de material Rustico de 2 pisos, una construcción de material noble de 3 pisos y en la parte posterior tiene un ambiente dividido en oficinas con material drywall, en estas construcciones viene funcionando la mayoría de oficinas, de acuerdo a lo descrito estas construcciones no considera ducteria para las redes de datos y comunicación es así que la instalación de red de datos es sobre la infraestructura a través de canaletas porque no existe ducteria interna.

- **Descripción detallada la situación actual de la red, tal y como se encuentra.**

La situación actual de la red de datos en las construcciones de la cámara de comercio es inadecuada en gran parte de las oficinas y en algunos deplorable debido a que la instalación se realizó en forma artesanal sin ningún tipo de planificación y mucho menos diseño.

Figura 10

Foto de la red de datos actual en oficina de construcción de drywall

Figura 11

Foto de la red de datos actual en la oficina de comercio exterior y turismo.

Figura 12

Foto de la red de datos actual en oficina de contabilidad.

- **Verificar si se tiene documentado la infraestructura física de la red.**

  Se solicitó documentos de la infraestructura física de la Red de Datos, la respuesta fue que no se tiene ningún tipo de documento de la red de datos, por lo cual se infiere que no se tiene ningún documento de cómo está instalado físicamente y mucho menos la distribución física de la red de datos.

- **Verificar si se tiene documentado la infraestructura lógica de la red.**

  Se solicitó documentos de la infraestructura lógica de la Red de Datos, la respuesta fue que no se tiene ningún tipo de documento de la red de datos, por lo cual se infiere que no se tiene ningún documento del funcionamiento lógico de la red de datos

- **Verificar si la infraestructura física y lógica cumple con los estándares internacionales.**

  Al realizar la evaluación de la instalación física, la distribución física de la red de datos, se puede determinar que no se tuvieron en cuenta ningún tipo de estándar internacional como en este caso la de cableado estructurado.

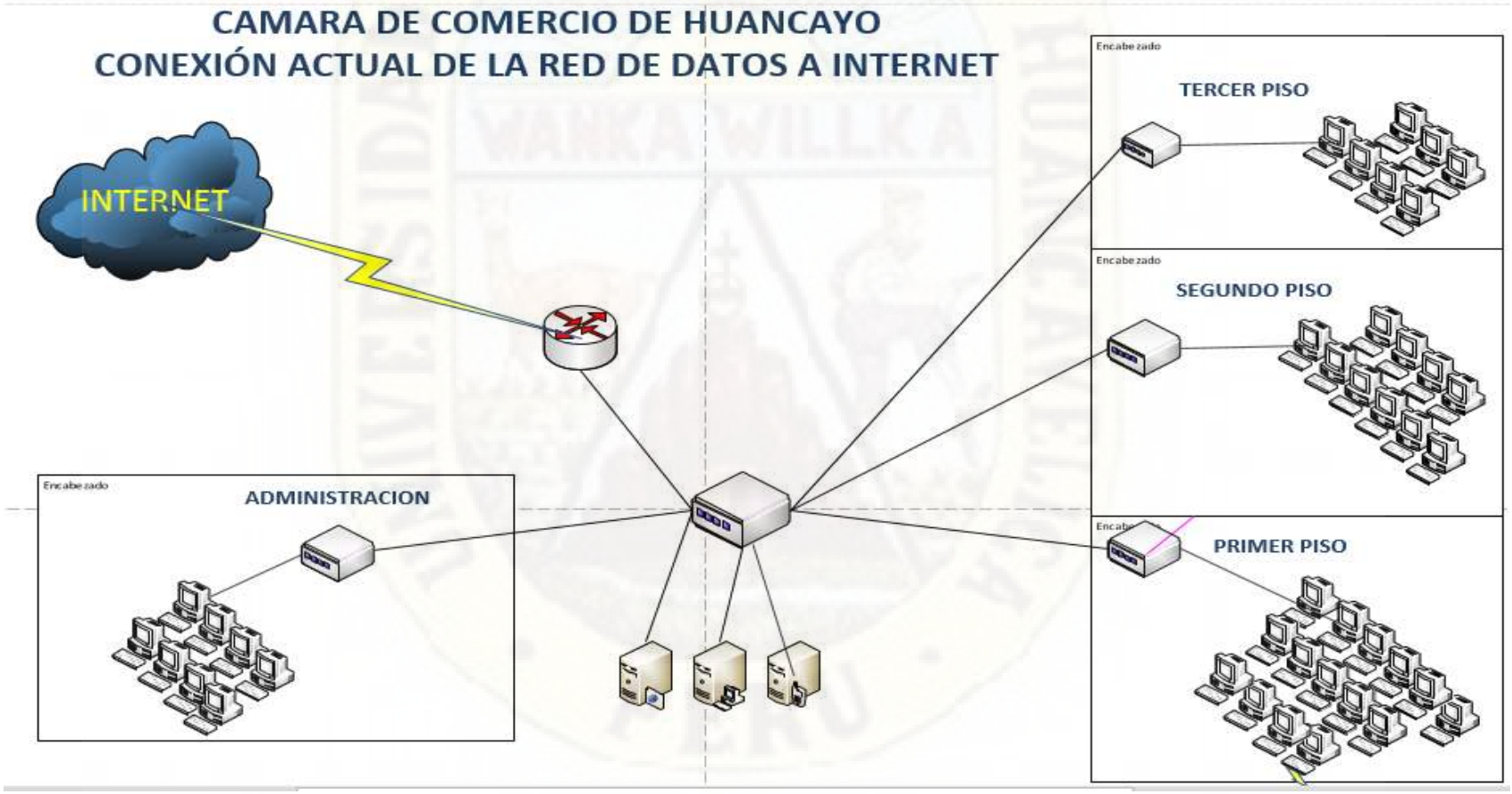
  Al realizar la evaluación de la configuración lógica se determinó que no existe ningún tipo de configuración, por ende, no existe ningún tipo de seguridad, entonces no cumple con ningún estándar de calidad de servicio y seguridad.

CONEXIÓN LÓGICA ACTUAL DE LA RED DE DATOS A INTERNET

A continuación, se muestra la conexión actual de la red de datos a internet, donde se puede observar que no se tiene ningún tipo de seguridad, ni firewall u otra herramienta de seguridad, además podemos observar que todo los hosts se encuentran en el mismo segmento de los servidores y físicamente también están conectado a través de concentradores.

Figura 13

conexión actual de la red de datos a internet



En la Figura 13, se evidencia claramente que la infraestructura local, el switch principal está conectada directamente al router del proveedor de internet. El router de la LAN, no tiene seguridad alguna, una sola red da servicios a las áreas administrativas, siendo una red plana Haciendo un análisis a nivel de capa física, el medio de transmisión es híbrido, con fibra óptica y par trenzado, o fibra óptica y enlace inalámbrico. Este último utiliza protocolo de encriptación de datos como WPA. Cada edificio consta con un switch marca Dlink modelo DGS-1024D de 24 puertos de 10/100/1000 no gestionables, en la sala de reuniones se encuentra uno de iguales características.

En base a la infraestructura de red y el diseño actual del campus se detectan algunas deficiencias que comprometen el desempeño de la misma.

- No existe un servidor de puerta de enlace (Proxy) y dominio que permita establecer permisos a los usuarios de la red.
- No hay configuración de VLAN a nivel de Switch para separar la red o un switch de capa 3 para enrutar las redes y de esa manera separarlas de manera lógica.
- La clase de red implementada en todo el campus es Clase C) para el edificio D y Clase C para el resto de los edificios, debido a que hay un router intermedio recibiendo una clase nateada. Para la red de Wifi si es clase B por el rango de IP que se maneja.
- La red no está segmentada, lo que hace que aumente considerablemente el tráfico de broadcast y colisiones en la red.
- La seguridad de la red está en un nivel muy bajo o nula y no se puede administrar, además de no ser administrable, no es escalable.

- El diseño de red es no jerárquico imposibilitando la redundancia, lo que hace que el servicio sea deficiente y no permita la escalabilidad de la red.

B. DISEÑO DE LA ZONA DESMILITARIZADA.

Tabla 1

Edificio de material rustico

N° PISO	NOMBRE DE LA OFICINA	N° HOST
	Sala de Directorio	2
	Asistente ejecutivo	2
	Gerencia Comercial	3
	contabilidad	3
PISO 1	Datacenter	1
	Comercio Exterior y Turismo	2
	Modulo Comercial	8
	Cámaras modulo comercial	2
	Access point data center	1
	Presidencia	2
	Gerencia General	3
	FEDACENTRO	3
PISO 2	Secretaria General	2
	Contabilidad	2
	FOGAPI	3
	Access point Gerencia General	1
Total de Host		40

Tabla 2

Edificio de material noble**.**

N° PISO	NOMBRE DE LA OFICINA	N° HOST
PISO 1	sala de conciliación	2
	sala de conciliación exterior	2
	sala de audiencias	2
	corte de arbitraje	4
	Cámara exterior pasadizo	1
	Cámara exterior de arbitraje	1
	Cámara interior arbitraje	1
	acces point arbitraje	1
PISO 2	Auditorio menor	4
	Cámara Auditorio menor	1
	Access point auditorio menor	1
	Auditorio Junin	2
	Cámara Auditorio Junin	1
	acces point auditorio Junin	1
PISO 3	Auditorio Mayor	4
	Cámara Auditorio mayor	1
	Acces point auditorio mayor	1
Total, de Host		30

Tabla 3

Ambientes de la parte posterior

N° PISO	NOMBRE DE LA OFICINA	N° HOST
PISO 1	Logística Entrega de Placas Caja	2
	Logística Entrega de Placas Almacén	2
	registro de protestos y mora	3
	Soporte Técnico	2
	Administración	2
	Cámara Logística Entrega de Placas	1
Total, de Host		12

Descripciones De Flujos De Datos, Simples Y Compuestos

Aquí explicaremos cuanto ancho de banda consumen los equipos de la cámara de comercio de Huancayo cuando están en uso los 66 host actualmente. Este cálculo se realiza mediante un programa llamado "WIRESHARK", que nos ayuda a calcular con exactitud el consumo de ancho de banda de cada computadora de la institución.

Actualmente cuenta con 02 servicios de internet cuyo ancho de banda es de 8 MB de ancho de banda que ofrece la empresa telefónica (al 30% en la transferencia de archivos), en las diferentes oficinas la cámara de comercio de Huancayo para diferentes tipos de uso.

a) Requerimiento de ancho de banda a nivel WAN

En la oficina de logística se procede a convertir los 8 MB en Bits que nos ofrece telefónica al 30% para la conexión a internet

2(1000) (1000) bits = 8 000 000 bits/

Al 30% (Asegura Telefónica) = 2 400 000 bits

Esto se divide equitativamente entre el tiempo de subida y bajada se detalla a continuación:

Tabla 4

Tiempo de subida y descarga de información

TIEMPO DE SUBIDA	TIEMPO DE DESCARGA
1 200 000 bits	**1200 000 bits**
1200 Kbps	**1200 Kbps**

Para saber cuánto puede transmitir cada máquina se divide el total de la línea de internet expresado en bits ofrecidos por telefónica en con el total de computadoras existentes, En total se tiene 66 computadoras.

Entonces:

$$T_{T=} \quad \frac{1200 \text{ Kbps}}{66 \text{ pc}}$$

$$T_{T=} \quad 18.18 \text{ Kbps}$$

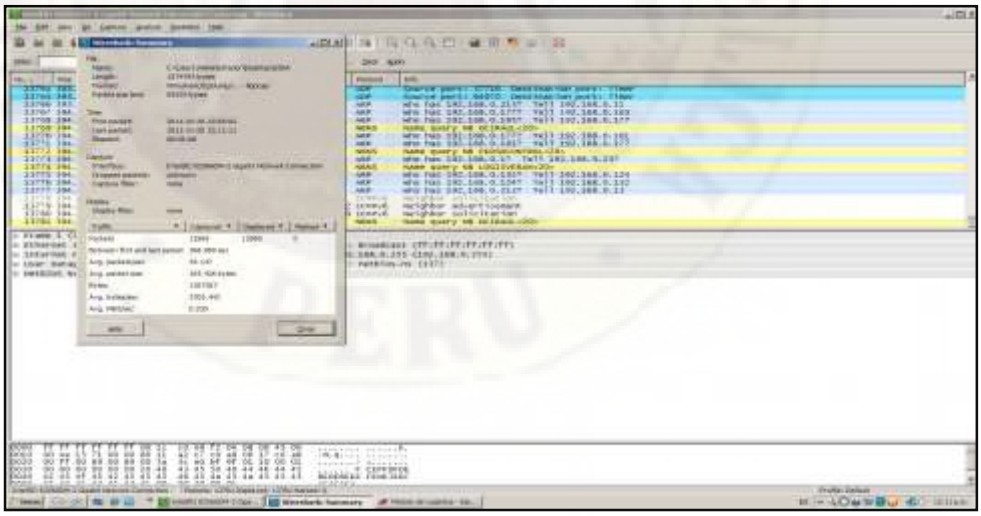
Entonces en el momento que todas las computadoras estén en uso trasfiriendo archivos en el mismo momento, se transmitirá a 18.18 Kbps por cada computador a nivel WAN.

Pero las computadoras que tienen conexión a internet utilizan diferentes servicios de internet como, correo electrónico, redes sociales (Facebook, otros), búsqueda de información, banca por internet, descarga de videos (youtube), otros servicios, cada uno de estos servicios utilizan el ancho de banda siguiente a nivel WAN según un estudio realizado con el software Wireshark:

- Correo electrónico 12 kbps
- Redes sociales (Facebook, solo imágenes, audio, video) 12 kbps, 16 kbps, 30kbps a más. Respectivamente
- Búsqueda de información 8kbps
- Banca por internet 15 kbps
- Descarga de videos (youtube) 30kbps a mas

Figura 14

Ancho de banda utilizado por el correo electrónico.



El ancho de banda mínimo requerido para trabajar todos los programas a la vez es de 107 kbps por host a nivel WAN, determinando un requerimiento mínimo de ancho banda WAN para toda la red es de 66 host * 107 kbps, un total 7062 kbps total de toda la Red de la cámara de comercio de Huancayo para cubrir la necesidad WAN.

Aquí se ve que el ancho de banda requerido a nivel WAN (7062 kbps) es mucho mayor del ancho de banda que se tiene 2400 kbps, teniendo un déficit de 4662 kbps (7062-2400) motivo por el cual se tiene continua saturación del ancho de banda a nivel WAN.

También mencionar que no todos tienen necesidad de salir a la WAN, esto ocurre porque no hay una infraestructura de red diseñada y mucho menos administrado.

b) Requerimiento de ancho de banda a nivel LAN

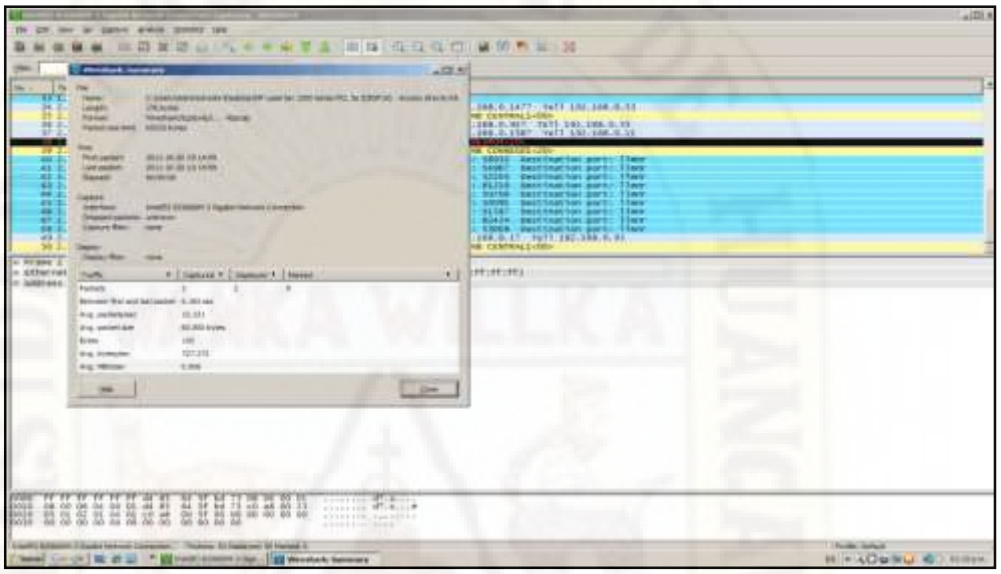
Evaluando el ancho de banda a nivel LAN, se realizó evaluando los servicios de red a nivel local, se tiene el servicio de impresoras en red la cual al evaluar el ancho de banda requerido se tiene que una impresora compartida utiliza es 10 kbps.

Evaluando el ancho de banda a nivel LAN, se encontró que debido a que se tiene instalado varios Hub (concentradores) en cascada estos provocan saturación debido a que son equipos que solo repiten la señal que se transmite y lo hacen a todos los puertos que tiene generando saturación del ancho de banda LAN lo cual conlleva a que este equipo se bloquee, generando caída de la red de datos constantemente, generando descontento en el personal por que

pierden la información que están trabajando o simplemente no pueden acceder a algún servicios solicitado

Figura 15

Ancho de banda utilizado por impresora compartida en una LAN.



c) Definición de Ubicación de host.

Para realizar este proceso recabamos información del funcionamiento actual de la cámara de comercio de Huancayo plasmando este funcionamiento tal y como está en los planos de ubicación de cada uno de los host, debemos resaltar que en un inicio la cámara de comercio de Huancayo instalo las computadoras según necesidad, se compraba, se instalaba en las oficinas y luego se tendía un cable para conectarlo a un hub (concentrador) y luego conectarse a internet, si 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 host.

d) Identificar y determinar los servicios que se desea implementar.

Se evaluó y se determinó que los servicios a implementar en la infraestructura de red son:

- Servidor de archivos para los sistemas de información LAN como sistema de contabilidad, control de personal, trámite administrativo, inventario, caja y otros.
- Servidor Proxy para el control de acceso a internet.
- Servidor de video vigilancia IP
- Servidor Asterisk telefonía IP.
- Servidor de Impresoras
- Servidor de correo.
- Servidor radios para control inalámbrica de acceso a internet.
- Servidor WEB.
- Servidor de video conferencia.

e) Asignación de Direcciones IP Distribución de Subredes y Hosts.

- **Asignación de Direcciones IP Privadas**

  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 asignado unos rangos de direcciones IP para su funcionamiento interno.

Estos son:

Figura 16

Clasificación de redes

Clase	Redes
A	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0 hasta 172.31.0.0
C	192.168.0.0 hasta 192.168.255.0

Estas direcciones IP no son utilizadas por los routers para su comunicación con Internet, y se utilizan solo dentro de la organización. Estas redes (Intranet) tienen la ventaja de ser mucho menos accesibles a ataques desde el exterior. Son visibles únicamente por otros hosts de su propia red. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas. Para nuestra organización en particular, hemos tomado como dirección IP, base principal, la siguiente:

Dirección de Red IP Privada en formato decimal: 192.168.10.0

IP Privada formato binario: 11000000.10101000.00001010.00000000

Máscara de Red: 255.255.255.0

El ultimo octeto de la dirección de red clase C (8 bits) son los de Host. En este caso se tomaron 8 bits últimos para direcciones de host.

Máscara de subred en binario: 11111111.11111111.11111111.00000000

Máscara de subred formato decimal: 255.255.255.0.

Entonces los números IP que se asignaran al host estará en el intervalo de 192.168.10.1 hasta 192.168.10.254

- **Creación de VLAN's**

Para una mejor administración de la red se debe implementar Redes virtuales de Área Local VLANs que nos permitirá tener una mejor gestión y seguridad en nuestra red, permitiendo una mejor segmentación en grupos y reducir el congestionamiento de la red. La red quedara de la siguiente manera creándose las VLAN`S en las subredes ya implementadas dentro de la red de datos de la cámara de comercio de Huancayo, se llevarán a cabo los siguientes pasos para su configuración.

Designando las VLAN que alberga áreas y ubicación de cada una de éstas existente la infraestructura de la cámara de Comercio Huancayo.

Tabla 5

Vlans con su respectivo nombre y áreas que alberga

VLAN	AREAS	OFICINAS	PISO	# HOST	HOST VLAN
VLAN 10	Tics	Tecnologías de información y comunicación	Piso 1, Piso 2, piso 3,	08	11
		Soporte Técnico	Piso 1	02	
		Datacenter	Piso 1	01	
		Sala de Directorio	Piso 1	02	
VLAN 20	Gerencia	Presidencia	Piso 02	02	12
		Gerencia Comercial	Piso 1	03	
		Asistente ejecutivo	Piso 1	02	
		Gerencia General	Piso 02	03	
VLAN 30	Administración	Administración	Piso 1	02	13
		contabilidad	Piso 1	03	
		Modulo Comercial	Piso 1	08	
VLAN 40	Organizaciones	FEDACENTRO	Piso 2	03	05
		Comercio Exterior y Turismo	Piso 1	02	
VLAN 50	Conciliación	sala de conciliación	Piso 1	02	08
		corte de arbitraje	Piso1	04	
		sala de audiencias	Piso 1	02	
VLAN 60	Placas	Entrega de Placas Caja	Piso 1	02	07
		Entrega de Placas Almacén	Piso 1	02	
		registro de protestos y mora	Piso 1	03	
VLAN 70	Auditorios	Auditorio menor	Piso 2	06	11
		Auditorio Mayor	Piso 3	03	
		sala de conciliación exterior	Piso 1	02	
VLAN 80	Cámaras	Cámara Entrega de Placas	Piso 1	01	09
		Cámara Auditorio menor	Piso 2	02	
		Cámaras modulo comercial	Piso 1	02	
		Cámara pasadizo principal	Piso 1	01	
		Cámara interior arbitraje	Piso 1	01	
		Cámara exterior arbitraje	Piso 1	01	
		Cámara auditorio mayor	Piso 3	01	
VLAN 55	Inalámbrico	ACCES POINT INALAMBRICO			06
VLAN 90	Servidores	SERVIDORES			09
TOTAL, HOST					91

Tabla 6

Resumen de las VLANS y su número IP asignado

VLAN	AREAS	IP ASIGNADO	MASCARA DE RED
VLAN 10	Tics	192.168.10.2-12	/25
VLAN 20	Gerencia	192.168.10.13-24	/25
VLAN 30	Administración	192.168.10.25-37	/25
VLAN 40	Organizaciones	192.168.10.38-42	/25
VLAN 50	Conciliación	192.168.10.43-50	/25
VLAN 60	Placas	192.168.10.51-57	/25
VLAN 70	Auditorios	192.168.10.58-68	/25
VLAN 80	Cámaras	192.168.10.69-77	/25
VLAN 55	Inalámbrico	192.168.10.144-151	/29
VLAN 90	Servidores	192.168.10.128-143	/28

- **Modelo de zona desmilitarizada red de datos.**

A continuación, se muestra el modelo de zona desmilitarizada que tiene las siguientes características, En el gráfico siguiente se puede apreciar la configuración de la DMZ, la cual se conecta a una interface pública mediante la interface GE 1/0/1, mientras que internamente se ha configurado una interface desmilitarizada en la Lan tomando una interface GE1/0/6 donde se conecta el web server para que responda las peticiones que vienen desde internet y sean contestadas sin ningún tipo de bloqueo.

Se deben tomar en cuenta ciertas políticas de seguridad para la red interna ya que al estar dentro de la infraestructura cualquier intensión de intromisión

desde esa red DMZ debe ser bloqueada, cualquier tipo de petición sospechosa debe ser rechazada utilizando una lista de control de acceso.

En la segunda parte del diseño, como protección adicional, se coloca otro Appliance NGFW o UTM luego del IDS para filtrar las amenazas detectadas por el IDS. Este Appliance tiene una conexión a una consola SYSLOG que almacenará los eventos que se presenten. El segundo NGFW - UTM está conectado a una consola IPS de Siguiente Generación (NGIPS), la cual, a su vez estará conectada a la consola SYSLOG, pero que a diferencia del UTM (el cual almacena información), el NGIPS extrae información de la consola para prevenir una posible filtración del UTM.

La NGIPS estará conectada al switch de la red local de los usuarios (Network – Lan Users), a su vez, estará conectado un Servidor Endpoint de Antivirus al mismo switch. De esta manera, el Endpoint recibirá las definiciones de del NGIPS y actuará preventivamente.

El Endpoint será la última barrera de protección antes de ingresar a las Vlans de los usuarios. Garantizando una red más segura. El Endpoint también tendrá una lógica de filtrado web, que a su vez enviará estas definiciones a los dispositivos de prevención. Con esto se logra que la navegación realizada por los equipos de los usuarios tenga seguridad, principalmente para el departamento de finanzas, quienes constantemente acceden a páginas de entidades financieras.

La tercera parte se utiliza un tercer Appliance NGFW – UTM. Este se conecta a la red de servicios (Network – LAN Core – Services) y a la red de aplicaciones (Network LAN Application). El tercer Appliance se pondrá entre

la red de servicios / la red de aplicación y la red de usuarios. De este modo, cuando la red de usuarios quiera consumir servicios de las aplicaciones, llegarían a este tercer Cortafuegos. Es, por tanto, que este último equipo controla lo que las aplicaciones necesiten para consumir servicios.

Para tener un mayor control y seguridad de los datos de la empresa, se contrata un servicio de Cloud Anti Spam, esta sería la primera línea de la defensa de toda la red de datos, ya que estaría conectada entre los equipos de los proveedores de internet, y al primer Appliance NGFW – UTM.

- **RouterISP Redundante**

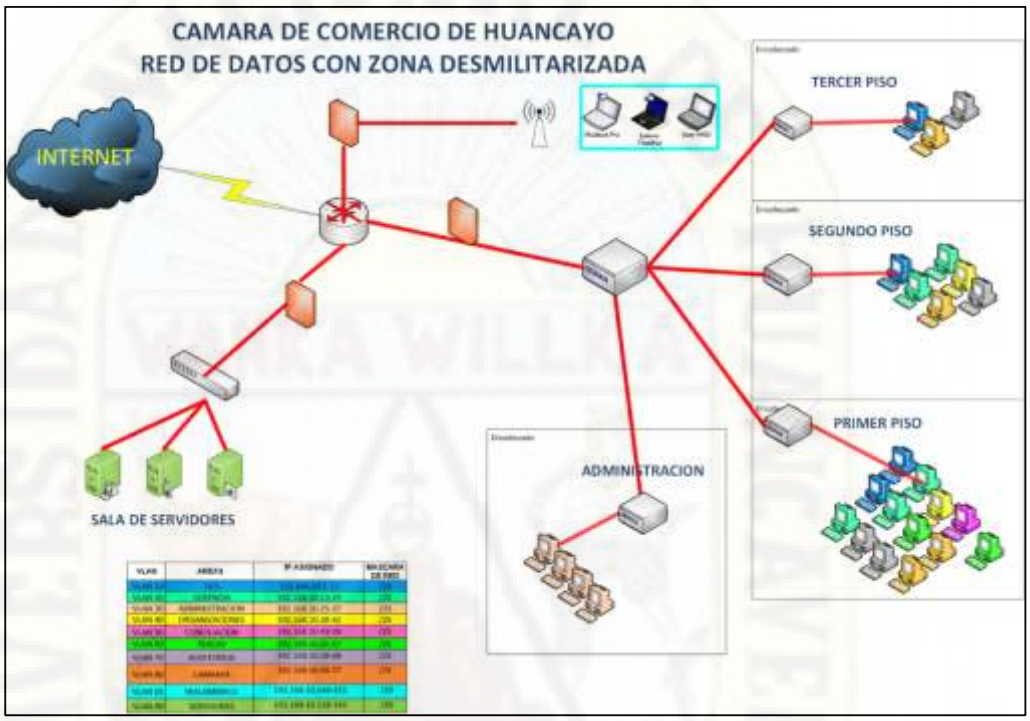
Con vista a brindar una mayor seguridad en cuanto a la continuidad de negocio, es tomado en cuenta una alta disponibilidad o redundancia en los routers de ISP, esto permite tener el servicio de internet de manera constante, en el caso de haber una caída por el lado del enlace principal se sufriría una pérdida del servicio de internet por menos de 5 minutos ya que existen dos conexiones al ISP desde internet con un enlace Backup.

Adicionalmente se configura un enlace de datos por medio de una VPN creada por el ISP para la comunicación con otra sucursal o campus. Se agrega un switch entre los router y el firewall, en este switch se han creado VLans para separar ambas redes la de internet y la de datos.

En cada VLan se conectan los routers y a su vez la conexión hacia el firewall, ambas conexiones funcionan dependiendo de la disponibilidad, teniendo como prioridad el enlace declarado como principal. De igual manera en el enlace de datos, las interfaces de cada router en la cual está configurado

el enlace de datos llega a la VLan asignada y de esta VLan una conexión al firewall el cual internamente o lógicamente tiene las Rutas estáticas para enlazarse a las sucursales o campus correspondientemente.

Figura 17



Diseño lógico de la red de la cámara de comercio

4.2 ANÁLISIS DE RESULTADOS:

En esta parte se muestra los resultados obtenidos según las fichas de observación realizadas al control de acceso a la red de datos con y sin el Modelo de zona desmilitarizada. El cual se realizará siguiendo la operacionalización de la variable.

- Control de acceso a red	• Autentificación de usuarios	• % Acceso de paquetes de usuarios no autorizados a nivel LAN • % Acceso de paquetes de usuarios no autorizados a nivel WAN
	• Políticas de acceso	• Nro. de políticas de acceso. • Nro. de protocolos asociados a las políticas.
	• Trafico de paquetes.	• Trafico de red

4.2.1. RESULTADOS DE LA DIMENSIÓN AUTENTIFICACIÓN DE USUARIOS.

a) **Indicador:** % Acceso de paquetes de usuarios no autorizados a nivel LAN

A continuación, presentamos los resultados obtenidos a nivel LAN.

En el Pre_Test y o Pos_Test

Tabla 7

% Acceso de paquetes de usuarios no autorizados a nivel LAN en el Pre_Test

Red sin DMZ 20 días monitoreo	Cantidad de paquetes LAN solicitando acceso	Cantidad de paquetes LAN Autorizados	% Acceso de paquetes de usuarios no autorizados a nivel LAN
día 1	152685	142450	93%
día 2	130630	115693	89%
día 3	120862	103245	85%
dia 4	139589	132374	95%
dia 5	130369	103012	79%
dia 6	147987	112928	76%
dia 7	117534	109658	93%
dia 8	130634	127353	97%
dia 9	140862	109175	78%
dia 10	134648	120454	89%
dia 11	130463	108930	83%
dia 12	120269	108892	91%
dia 13	132274	118692	90%
dia 14	120963	108464	90%
dia 15	130863	105598	81%
dia 16	125296	107891	86%
dia 17	107593	98814	92%
dia 18	137599	128964	94%
dia 19	133749	128840	96%
dia 20	130963	115253	88%
		PROMEDIO	88%

Tabla 8

% Acceso de paquetes de usuarios no autorizados a nivel LAN en el Pos_Test

Red con DMZ 20 días monitoreo	Cantidad de paquetes LAN solicitando acceso	Cantidad de paquetes LAN Autorizados	% Acceso de paquetes de usuarios no autorizados
dia 1	120586	4862	4%
dia 2	134607	4887	4%
dia 3	118697	4687	4%
dia 4	124739	11203	9%
dia 5	119968	3770	3%
dia 6	133681	4292	3%
dia 7	123275	3666	3%
dia 8	123793	12193	10%
dia 9	105114	3667	3%
dia 10	98258	3510	4%
dia 11	127146	4444	3%
dia 12	120328	4473	4%
dia 13	107887	3945	4%
dia 14	95885	3651	4%
dia 15	132628	4456	3%
dia 16	109119	3915	4%
día 17	100524	4477	4%
dia 18	112460	3545	3%
dia 19	96186	4745	5%
dia 20	112543	4710	4%
		PROMEDIO	**4%**

- Análisis comparativo del % Acceso de paquetes de usuarios no autorizados a nivel LAN en el Pos_Test y Pre_Test.

Tabla 9

Análisis comparativo del % Acceso de paquetes

% Acceso de paquetes de usuarios no autorizados a nivel LAN		**Promedio de Mejora**
red sin DMZ 20 días monitoreo	red con DMZ 20 días monitoreo	
88%	4%	**84%**

De la Tabla 9, se puede apreciar que el uso del modelo de zona militarizada influyó en la Red LAN restringiéndose el acceso de paquetes a los usuarios no autorizados en un 84%, con lo que se confirma la utilidad del modelo.

b) Indicador: % Acceso de paquetes de usuarios no autorizados a nivel WAN

A continuación, presentamos los resultados obtenidos a nivel LAN. En el Pre_Test y Pos_Test

Tabla 10

% Acceso de paquetes de usuarios no autorizados a nivel WAN en el Pre_Test

Red sin DMZ 20 días monitoreo	Cantidad de paquetes WAN solicitando acceso	Cantidad de paquetes WAN Autorizados	% Acceso de paquetes de usuarios no autorizados a nivel WAN
dia 1	28066263	20598447	73%
dia 2	27137284	22688446	84%
dia 3	25827206	21800830	84%
dia 4	28227085	24507482	87%
dia 5	24102127	20748047	86%
dia 6	27136279	23861141	88%
dia 7	23705574	17876333	75%
dia 8	27483618	16408224	60%
dia 9	23609447	16661756	71%
dia 10	24916797	20808955	84%
dia 11	25034610	18280987	73%
dia 12	26481110	19752343	75%
dia 13	24334888	20092915	83%
dia 14	26178121	16665780	64%
dia 15	25926852	20346447	78%
dia 16	26568483	20757763	78%
dia 17	23530788	20686221	88%
dia 18	26475563	23566764	89%
dia 19	24936905	20621176	83%
dia 20	26755903	19441315	73%
	PROMEDIO		**79%**

Tabla 11

% Acceso de paquetes de usuarios no autorizados a nivel WAN en el Pos_Test

Red con DMZ 20 días monitoreo	Cantidad de paquetes WAN solicitando acceso	Cantidad de paquetes WAN Autorizados	% Acceso de paquetes de usuarios no autorizados a nivel WAN
dia 1	28974179	5291111	18%
dia 2	26608107	2973042	11%
dia 3	28349495	4848364	17%
dia 4	29034498	3483890	12%
dia 5	28622632	4989010	17%
dia 6	29514607	2709844	9%
dia 7	26584422	3079513	12%
dia 8	26226368	3090461	12%
dia 9	28104155	4350929	15%
dia 10	29019472	3667835	13%
dia 11	29091842	4658694	16%
dia 12	27293832	2683123	10%
dia 13	27347543	2690008	10%
dia 14	28027401	3793050	14%
dia 15	26818546	1886975	7%
dia 16	27932753	2238844	8%
dia 17	28963005	4436211	15%
dia 18	28871645	3747656	13%
dia 19	29765113	4472663	15%
dia 20	28784929	3609935	13%
		PROMEDIO	**13%**

- Análisis comparativo del % Acceso de paquetes de usuarios no autorizados a nivel WAN en el Pos_Test y Pre_Test.

Tabla 12

Análisis comparativo del % Acceso de paquetes de usuarios

% Acceso de paquetes de usuarios no autorizados a nivel WAN		Promedio de Mejora de seguridad
red sin DMZ 20 días monitoreo	red con DMZ 20 días monitoreo	
79%	13%	66%

De la Tabla 12, se puede apreciar que el uso del modelo de zona militarizada influyó en la Red WAN restringiéndose el acceso de paquetes a los usuarios no autorizados en un 66 %, con lo que se confirma la utilidad del modelo.

4.2.2. RESULTADOS DE LA DIMENSIÓN POLICÍAS DE ACCESO.

a) INDICADOR NUMERO DE POLÍTICAS DE ACCESO.

- **Red Actual:**

Tabla 13

Cantidad de políticas de acceso de Red Actual

RED EVALUADA	Red Actual
DIMENSION	Politicas de Acceso
INDICADOR 1	Numero de politicas de acceso

TIPO DE RED	CANTIDAD DE POLITICAS DE SEGURIDAD Y ACCESO
Red actual	0

- **Zona Desmilitarizada:**

Tabla 14

Cantidad de políticas de acceso de Zona Desmilitarizada.

RED EVALUADA	Zona Desmilitarizada
DIMENSION	Politicas de Acceso
INDICADOR 1	Numero de politicas de acceso

POLITICAS	DESCRIPCION	CANTIDAD
DE SEGURIDAD Y ACCESO	FIREWALL NGFW	1
DE SEGURIDAD Y ACCESO	FIREWALL UTM	1
DE SEGURIDAD Y ACCESO	NGIPS	1
DE SEGURIDAD Y ACCESO	ENDPOIT SECURITY	1
DE SEGURIDAD Y ACCESO	CLOUD ANTI SPAM	1
	TOTAL DE POLITICAS	5

b) INDICADOR NUMERO DE PROTOCOLOS ASOCIADOS A LAS POLÍTICAS.

➢ Red Actual

Tabla 15

Cantidad de protocolos asociados a las políticas de acceso de Red Actual

RED EVALUADA	Red Actual
DIMENSION	Politicas de Acceso
INDICADOR 2	Numero de protocolos asociados a las politicas

TIPO DE RED	POLITICAS SEGURIDAD Y ACCESO	CANTIDAD
Red actual	0	0

➢ Zona Desmilitarizada

Tabla 16

Cantidad de protocolos asociados a las políticas de acceso de Zona Desmilitarizada.

RED EVALUADA	Zona Desmilitarizada
DIMENSION	Politicas de Acceso
INDICADOR 2	Numero de protocolos asociados a las politicas

POLITICAS DE SEGURIDAD Y ACCESO	CANTIDAD DE PROTOCOLOS
FIREWALL NGFW	1
FIREWALL UTM	1
NGIPS	2
ENDPOINT	1
CLOUD ANTI SPAM	1
TOTAL	6

4.2.3. DIMENSIÓN TRÁFICOS DE PAQUETES.

a) INDICADOR TRAFICO DE RED.

- **Red Actual**

Tabla 17

Tráfico de la red actual

N°	Host	Nombre de Oficina - Area	Trafico red Mbps	
			Descarga	Carga
1	Maquina 01	sala de conciliación	6.4	5.6
2	Maquina 02	sala de conciliación exterior	7.2	4.5
3	Maquina 03	sala de audiencias	6.0	3.8
4	Maquina 04	corte de arbitraje	7.8	4.6
5	Maquina 05	Cámara exterior pasadizo	7.4	4.7
6	Maquina 06	Cámara exterior de arbitraje	7.7	4.9
7	Maquina 07	Cámara interior arbitraje	8.0	4.2
8	Maquina 08	Acces Point arbitraje	6.7	4.3
9	Maquina 09	Auditorio menor	6.2	3.7
10	Maquina 10	Cámara Auditorio menor	6.5	3.8
11	Maquina 11	Access Point auditorio menor	6.9	4.6
12	Maquina 12	Auditorio Junín	6.1	4.7
13	Maquina 13	Cámara Auditorio Junín	6.6	4.9
14	Maquina 14	Acces Point auditorio Junín	6.2	4.4
15	Maquina 15	Auditorio Mayor	6.3	4.5
16	Maquina 16	Cámara Auditorio mayor	6.0	4.6
17	Maquina 17	Acces Point auditorio mayor	6.3	4.8
18	Maquina 18	Logística Entrega de Placas Caja	6.8	4.6
19	Maquina 19	Logística Entrega de Placas Almacén	6.9	3.6
20	Maquina 20	registro de protestos y mora	7.4	3.8
21	Maquina 21	Soporte Técnico	7.2	4.2
22	Maquina 22	Administración	6.9	4.3
23	Maquina 23	Cámara Logística Entrega de Placas	7.3	3.7
Promedio			**6.82**	**4.4**

El tráfico de red, sin el modelo de zona militarizada refleja que la transferencia de datos (descargas y cargas) de Red Actual se encuentran en 6.82 Mbps 4.4 Mbps respectivamente, evidenciando dificultades de transferencia de datos en la cámara de comercio.

- **Trafico de Red - Zona Desmilitarizada**

Tabla 18

Trafico de Red - Zona Desmilitarizada

N°	Host	Nombre de Oficina - Area	Trafico red Mbps	
			Descarga	Carga
1	Maquina 01	sala de conciliación	18.3	12.6
2	Maquina 02	sala de conciliación exterior	19	13.5
3	Maquina 03	sala de audiencias	15.6	13.2
4	Maquina 04	corte de arbitraje	16	11.8
5	Maquina 05	Cámara exterior pasadizo	15.4	12.4
6	Maquina 06	Cámara exterior de arbitraje	16.0	15.3
7	Maquina 07	Cámara interior arbitraje	22.3	14.9
8	Maquina 08	acces point arbitraje	24.5	13.1
9	Maquina 09	Auditorio menor	28.6	13.2
10	Maquina 10	Cámara Auditorio menor	25.4	14.7
11	Maquina 11	Access point auditorio menor	19.4	14.8
12	Maquina 12	Auditorio Junin	9.6	12.4
13	Maquina 13	Cámara Auditorio Junin	19	11.9
14	Maquina 14	acces point auditorio Junin	23	10.3
15	Maquina 15	Auditorio Mayor	32.0	14.5
16	Maquina 16	Cámara Auditorio mayor	15.8	14.7
17	Maquina 17	Acces point auditorio mayor	16.7	11.6
18	Maquina 18	Logística Entrega de Placas Caja	15.6	11.4
19	Maquina 19	Logística Entrega de Placas Almacén	18	14.8
20	Maquina 20	registro de protestos y mora	16.4	15.2
21	Maquina 21	Soporte Técnico	17.2	13.8
22	Maquina 22	Administración	16.9	12.7
23	Maquina 23	Cámara Logística Entrega de Placas	21.3	15.8
Promedio			**19.22**	**13.4**

De la Tabla podemos apreciar que el tráfico de red, con el modelo de zona militarizada refleja que la transferencia de datos (descargas y cargas) de Red Actual se encuentran en 19.22 Mbps 13.4 Mbps respectivamente, garantizando una mejor transferencia de datos en la cámara de comercio.

- **Análisis comparativo del Tráfico de Red en el Pre_Test (Red actual) y Pos_Test (Red DMZ).**

Tabla 19

Análisis comparativo del Trafico red (Mbps)

Trafico red (Mbps)					
Descarga			**Carga**		
Red Actual	Red DMZ	**Mejora**	Red Actual	Red DMZ	**Mejora**
6.82	19.84	**13.02**	4.4	13.6	**9.2**

De la Tabla 19, podemos apreciar que el tráfico de red, con el modelo de zona militarizada mejora la transferencia de datos (descargas y cargas) en la cámara de comercio, esto se evidencia al tener una mejora del 13.02 Mbps en la descarga y una mejora de velocidad de 9.2 Mbps en la carga de datos.

4.3 CONTRASTACIÓN DE HIPÓTESIS

4.3.1 DE LA HIPÓTESIS ESPECÍFICA 1.

Para llevar a cabo la contrastación de las Hipótesis, se realizó el siguiente procedimiento.

Paso 1. Lo primero es presentar el resumen de datos consolidados respecto a la autenticación de usuarios tanto del Pre_Test como del Pos_Test. Para la red LAN como para la Red WAN.

	Red LAN		Red WAN	
Día	**% Acceso de paquetes de usuarios no autorizados**		**% Acceso de paquetes de usuarios no autorizados**	
	Red sin DMZ	Red con DMZ	Red sin DMZ	Red con DMZ
1	93%	4%	7%	18%
2	89%	4%	8%	11%
3	85%	4%	8%	17%
4	94%	9%	9%	12%
5	79%	3%	9%	17%
6	76%	3%	9%	9%
7	93%	3%	8%	12%
8	97%	10%	6%	12%
9	77%	3%	7%	15%
10	89%	4%	8%	13%
11	83%	3%	7%	16%
12	90%	4%	7%	10%
13	89%	4%	8%	10%
14	89%	4%	6%	14%
15	80%	3%	8%	7%
16	86%	4%	8%	8%
17	91%	4%	9%	15%
18	93%	3%	9%	13%
19	96%	5%	8%	15%
20	88%	4%	7%	13%

Paso N° 02: (Redactar la hipótesis)

H_0= Un modelo de zona desmilitarizada no influye en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo.

H_1= Un modelo de zona desmilitarizada influye positivamente en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo.

Paso N° 03: (definir el α)

Alfa = 0.05 = 5%

Paso N° 04: (Prueba de Normalidad)

Para elegir el estadístico de contrastación de hipótesis se realizó la prueba de normalidad, obteniéndose los siguientes resultados.

Tabla 20

Prueba de normalidad - Hipótesis especifica 1

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
LAN_Red_sin_DMZ	,174	20	,114	,938	20	,223
LAN_Red_con_DMZ	,403	20	,059	,598	20	,108
WAN_Red_sin_DMZ	,233	20	,066	,878	20	,096
WAN_Red_con_DMZ	,107	20	,200*	,975	20	,846

*. Este es un límite inferior de la significación verdadera.

a. Corrección de la significación de Lilliefors

Como se puede apreciar, la prueba de normalidad nos muestra que los datos provienen de una distribución normal porque las Sig. > 0.05, por ello se eligió como prueba de hipótesis la prueba de la t-Student con muestras relacionadas.

A continuación, se presenta el procedimiento efectuado.

Paso N° 05: (Decisión Estadística)

El criterio para decidir la contrastación de la hipótesis es el siguiente:

Si la Sig. > α, entonces se acepta Ho y se rechaza Ha

Si la Sig. <= α, entonces se rechaza Ho y se acepta Ha

Tabla 21

Prueba de muestras relacionadas Hipótesis Especifica 1

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	LAN_Red_sin_DMZ - LAN_Red_con_DMZ	83,6000	5,2955	1,1841	81,1216	86,0784	70,602	19	,000
Par 2	WAN_Red_sin_DMZ - WAN_Red_con_DMZ	-5,0500	3,3321	,7451	-6,6095	-3,4905	-6,778	19	,000

Decisión

De la prueba realizada se puede comprobar que el valor de la Sig .es = 0.000 en todas las variables. Por tanto, como la Sig. < 0.05, se rechaza Ho y se acepta Ha.

Afirmando que "Un modelo de zona desmilitarizada influye positivamente en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo".

4.3.2 DE LA HIPÓTESIS ESPECÍFICA 2

Planteamiento de la hipótesis

H_0 = Un modelo de zona desmilitarizada no influye en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo.

H_1 = Un modelo de zona desmilitarizada influye positivamente en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo.

Para demostrar la hipótesis se procedió a realizar un análisis comparativo de la cantidad de políticas implementadas, del número de protocolos asociados a las políticas, tanto en la Red Actual como en la Red con Zona Desmilitarizada. A continuación, se presenta el análisis comparativo.

Tabla 22

Cantidad de Políticas de Seguridad y acceso-Hipótesis 2

Cantidad de Políticas de Seguridad y acceso			
Re Actual		**Red con Zona Desmilitarizada**	
Descripción de la Política	**Cantidad**	**Descripción de la Política**	**Cantidad**
--.--	0	Firewall NGFW	1
		Firewall UTM	1
		NGIPS	1
		ENDPOIT SECURITY	1
		CLOUD ANTI SPAM	1
Total	**0**	**Total**	**5**

Tabla 23

Número de protocolos asociados a las políticas-Hipótesis 2.

Cantidad de protocolos			
Re Actual		**Red con Zona Desmilitarizada**	
Descripción de la Política	**Cantidad de protocolos**	**Descripción de la Política**	**Cantidad de protocolos**
--.--	0	Firewall NGFW	1
		Firewall UTM	1
		NGIPS	2
		ENDPOIT SECURITY	1
		CLOUD ANTI SPAM	1
Total	**0**	**Total**	**6**

Decisión

De la prueba realizada se puede comprobar que en la Red de datos con Zona desmilitarizada se implementó 5 políticas de seguridad y acceso a los datos, 06 protocolos para respaldar las políticas. Mientras que en la red actual no existe evidencia de alguna política implementada mucho menos de un protocolo.

Por tanto, podemos afirmar que “Un modelo de zona desmilitarizada influye positivamente en el tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo”.

4.3.3 DE LA HIPÓTESIS ESPECIFICA 3

Para llevar a cabo la contrastación de la Hipótesis, se realizó el siguiente procedimiento.

Paso 1. Lo primero es presentar el resumen de datos consolidados respecto al tráfico de paquetes, evaluado a través del tráfico de red tanto para la Descarga, como para la Carga de datos. Mostramos los datos obtenidos en el Pre_Test como en el Pos_Test.

Tabla 24

Resumen del Tráfico de red - Hipótesis 3

Día	Tráfico de Red		Tráfico de Red	
	Descarga		Carga	
	Red sin DMZ	Red con DMz	Red sin DMZ	Red con DMz
1	6.4	18.3	5.6	12.6
2	7.2	19	4.5	13.5
3	6.0	15.6	3.8	13.2
4	7.8	16	4.6	11.8
5	7.4	15.4	4.7	12.4
6	7.7	16.0	4.9	15.3
7	8.0	22.3	4.2	14.9
8	6.7	24.5	4.3	13.1
9	6.2	28.6	3.7	13.2
10	6.5	25.4	3.8	14.7
11	6.9	19.4	4.6	14.8
12	6.1	9.6	4.7	12.4
13	6.6	19	4.9	11.9
14	6.2	23	4.4	10.3
15	6.3	32.0	4.5	14.5
16	6.0	15.8	4.6	14.7

17	6.3	16.7	4.8	11.6
18	6.8	15.6	4.6	11.4
19	6.9	18	3.6	14.8
20	7.4	16.4	3.8	15.2
21	7.2	17.2	4.2	13.8
22	6.9	16.9	4.3	12.7
23	7.3	21.3	3.7	15.8

Paso N° 02: (Redactar la hipótesis)

H_0= Un modelo de zona desmilitarizada no influye en el tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo.

H_1= Un modelo de zona desmilitarizada influye positivamente en el tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo.

Paso N° 03: (definir el α)

Alfa = 0.05 = 5%

Paso N° 04: (Prueba de Normalidad)

Para elegir el estadístico de contrastación de hipótesis se realizó la prueba de normalidad, obteniéndose los siguientes resultados.

Tabla 25

Prueba de Normalidad-Hipótesis 3

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Traf_Red_Descarga_sin_DMZ	,111	23	,200*	,949	23	,278
Traf_Red_Descarga_con_DMZ	,235	23	,002	,910	23	,142
Traf_Red_Carga_sin_DMZ	,144	23	,200*	,939	23	,170

Traf_Red_Carga_con_DMZ	,158	23	,140	,957	23	,408

*. Este es un límite inferior de la significación verdadera.

a. Corrección de la significación de Lilliefors

Como se puede apreciar, la prueba de normalidad nos muestra que los datos provienen de una distribución normal porque las Sig. > 0.05, por ello se eligió como prueba de hipótesis la prueba de la t-Student con muestras relacionadas.

A continuación, se presenta el procedimiento efectuado.

Paso N° 05: (Decisión Estadística)

El criterio para decidir la contrastación de la hipótesis es el siguiente:

Si la Sig. > α, entonces se acepta Ho y se rechaza Ha

Si la Sig. <= α, entonces se rechaza Ho y se acepta Ha

Tabla 26

Prueba de la Hipótesis 3

Prueba de muestras relacionadas

	Diferencias relacionadas					t	gl	Sig. (bilateral)
	Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
				Inferior	Superior			
Traf_Red_Descarga_sin_DMZ - Traf_Red_Descarga_con_DMZ	-86,8261	88,690	18,4932	-125,17	-48,4735	-4,695	22	,000

Traf_Red_Carga_sin_DMZ - Traf_Red_Carga_con_DMZ	-90,3478	17,499	3,6489	-97,915	-82,7804	-24,760	22	,000

Decisión

De la prueba realizada se puede comprobar que el valor de la Sig .es = 0.000 en todas las variables. Por tanto, como la Sig. < 0.05, se rechaza Ho y se acepta Ha.

Afirmando que "Un modelo de zona desmilitarizada influye positivamente en el tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo".

4.3.4 DE LA HIPÓTESIS GENERAL.

Habiendo comprobado que el modelo de zona desmilitarizada influyó sobre el control de acceso a la red medido a través de sus sub variables; Se comprobó una mejora del 66% en la autentificación de usuarios con una Sig.=0.00; Respecto a la sub variable Políticas de Acceso se pudo definir 6 protocolos asociados a 5 políticas con el uso del modelo de la zona desmilitarizada; Respecto a la sub variable Tráfico de paquetes medido a través de su indicador del Tráfico de Red se pudo comprobar una mejora en la Descarga de datos de 13.02 Mbps y un mejora de 9.2 Mbps en la Carga de datos, con una Sig.=0.000.

Con lo expuesto se confirma que el Modelo de Zona Desmilitarizada influyó positivamente en el Control de acceso a la Red de datos de la cámara de comercio de Huancayo.

4.4 DISCUSIÓN DE RESULTADOS

Respecto al objetivo "Determinar cuál es la influencia del modelo de zona desmilitarizada en la autentificación de usuarios en la red de datos". Se comprobó una mejora de seguridad del 66% al Acceso de paquetes de usuarios no autorizados a nivel WAN y un porcentaje de mejora de seguridad del 84% al Acceso de paquetes de usuarios no autorizados a nivel LAN. Obteniéndose una Sig.=0.00, en la autentificación de usuarios. Coincidiendo con los resultados obtenidos por Cortes (2011) quien afirma que en una red segura los usuarios pueden aumentar su calidad de trabajo, ya que los sistemas mejoraron en tiempos de respuesta, al igual que los enlaces de Internet.

Respecto al objetivo “Determinar cuál es la influencia del modelo de zona desmilitarizada en las políticas de acceso en la red de datos”. se pudo definir 6 protocolos asociados a 5 políticas con el uso del modelo de la zona desmilitarizada, los resultados fueron similares a los de Mayorga (2008) quien afirma que definir políticas de seguridad, así como un plan de contingencia ante posibles desastres y un esquema de monitoreo proactivo de seguridad perimetral establecida son elementos que se debe definir en este proceso.

Respecto al objetivo “Determinar cuál es la influencia del modelo de zona desmilitarizada en el tráfico de paquetes en la red de datos” De la prueba realizada se puede comprobar que el valor de la Sig .es = 0.000 en todas las variables. Por tanto, como la Sig. < 0.05, se rechaza Ho y se acepta Ha. Así mismo, a través de su indicador del Tráfico de Red se pudo comprobar una mejora en la Descarga de datos de 13.02 Mbps y una mejora de 9.2 Mbps en la Carga de datos, en contrastación con los resultados obtenidos por c5órdova (2009) este afirma que la seguridad perimetral mejora la velocidad de Internet, como previene de ataques ataques de hackers

CONCLUSIONES

1. El modelo de zona desmilitarizada en la autentificación de usuarios en la red de datos Influyó en la seguridad del 66% al Acceso de paquetes de usuarios no autorizados a nivel WAN y un porcentaje de mejora de seguridad del 84% al Acceso de paquetes de usuarios no autorizados a nivel LAN. Obteniéndose una Sig.=0.00, en la autentificación de usuarios. Afirmando que en una red segura los usuarios pueden aumentar su calidad de trabajo.
2. De igual modo el modelo de zona desmilitarizada influyó en las políticas de acceso de la red de datos, definiéndose 6 protocolos asociados a 5 políticas afirmando que definir políticas de seguridad, así como un plan de contingencia ante posibles desastres y un esquema de monitoreo proactivo de seguridad perimetral establecida son elementos que se debe definir en este proceso.
3. Respecto a la influencia del modelo de zona desmilitarizada en el tráfico de paquetes en la red de datos, se obtuvo un valor de Sig . = 0.000 en todas las variables. Así mismo, a través de su indicador del Tráfico de Red se pudo comprobar una mejora en la Descarga de datos de 13.02 Mbps y una mejora de 9.2 Mbps en la Carga de datos, en contrastación con los resultados obtenidos por c5órdova (2009) este afirma que la seguridad perimetral mejora la velocidad de Internet, como previene de ataques ataques de hackers.
4. Finalmente podemos concluir que el Modelo de Zona Desmilitarizada influyó en el control de acceso a la red de datos de la Cámara de Comercio de la provincia de Huancayo

RECOMENDACIONES

1. . Se recomienda masificar el uso del modelo. de red con DMZ.
2. Establecer como política de administración de la red de datos, que solo las personas que administran y dan mantenimiento a la red de datos tengan acceso a los equipos de interconexión de red,
3. Implementar acciones de revisión física de la red, descartando equipos conectados sin autorización.
4. Implementar plan de contingencia para diferentes situaciones, para evitar una incidencia dentro de la red de datos

REFERENCIA BIBLIOGRÁFICA

Álvaro Gómez Vieites - Enciclopedia de la Seguridad Informática, 2ºed., 2011.

María del Pilar Alegre Ramos, Seguridad Informática, España 2011.

"Programa de Certificacion CISCO Asociado a Redes CCNA V 5.0" SECURITY CISCO NETWORK ACADEMY Editorial: Pearson Vue 2015

"Programa de Certificación CISCO Asociado a Redes CCNA V 5.0" DATA CENTER CISCO NETWORK ACADEMY Editorial: Pearson Vue 2015

"Programa de Certificación CISCO Asociado a Redes CCNA V 5.0" WIRELESS CISCO NETWORK ACADEMY Editorial: Pearson Vue 2015.

"Programa de Certificación CISCO Asociado a Redes CCNA V 5.0" CLOUD CISCO NETWORK ACADEMY Editorial: Pearson Vue 2015.

Enciclopedia de la Seguridad Informática - Alvaro Gómez Vieites, 8va Edición, 2013.

Seguridad informática - Ethical Hacking-Marion Agé, Sebastian Baudru, 2da Edición, 2013.

"PRACTICAL COMPUTER NETWORK ANALYSIS AND DESIGN" James McCABE 2011

Telemática Aplicada. Rubén Jorge Fusario. Volumen I. Editorial: Mc Grawhi

Tesis desarrolladas

"Diseño e implementación de una red RF Indoor en el Hospital de emergencia pediátricas para mejora de cobertura" Tesis para optar el Título de Ingeniero de las Telecomunicaciones. Presentado por el bachiller: Aldo Duarte Vera

Tudela. Universidad: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ. Año: 2013

Páginas web

1. https://www.osiptel.gob.pe/
2. https://www.ieee.org/index.html
3. https://es.wikipedia.org/wiki/Protocolo_de_comunicaciones
4. http://www.gilat.com/SkyEdge-II

ANEXOS

1.1 **ANEXO 1. MATRIZ DE CONSISTENCIA**

Formulación del problema	**Objetivos de investigación**	**Hipótesis**	**Variables**	**Metodología**
Problema general. ¿Cuál es la influencia del modelo de zona desmilitarizada en el control de acceso en la red de datos de la cámara de comercio de Huancayo? **Problemas específicos** a) ¿Cuál es la influencia del modelo de zona desmilitarizada en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo?	**Objetivo General.** Determinar cuál es la influencia del modelo de zona desmilitarizada en el control de acceso en la red de datos de la cámara de comercio de Huancayo **Objetivos Específicos.** a) Determinar cuál es la influencia Cuál es la influencia del modelo de zona desmilitarizada en la autentificación de usuarios en la	**Hipótesis General** El modelo de zona desmilitarizada influye positivamente en el control de acceso en la red de datos de la cámara de comercio de Huancayo **Hipótesis Específicas** a) Un modelo de zona desmilitarizada influye positivamente en la autentificación de usuarios en la red de datos de la cámara de comercio de Huancayo.	**Variable independiente** Modelo de zona Desmilitarizada **Variable dependiente** Control de Acceso a Red	**1. Métodos de investigación** **Método general:** Método científico **Método específico** Método descriptivo **Tipo de investigación** Aplicada **Nivel de investigación** Explicativo **Diseño de investigación** Pre experimental **Población Y Muestra** **Población**: todos los hosts de la red de datos de la cámara de comercio de Huancayo.

b) ¿Cuál es la influencia del modelo de zona desmilitarizada en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo? c) ¿Cuál es la influencia del modelo de zona desmilitarizada en tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo?	red de datos de la cámara de comercio de Huancayo b) Determinar cuál es la influencia del modelo de zona desmilitarizada en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo. c) Determinar cuál la influencia del modelo de zona desmilitarizada en tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo	b) Un modelo de zona desmilitarizada influye positivamente en las políticas de acceso en la red de datos de la cámara de comercio de Huancayo. c) Un modelo de zona desmilitarizada influye positivamente en el tráfico de paquetes en la red de datos de la cámara de comercio de Huancayo.		**Muestra:** todos los hosts de la red de datos de la cámara de comercio de Huancayo. **Técnicas de recolección de datos** Ficha de observación Entrevista Observación **Instrumentos de recolección de datos** Cuestionario de entrevista Ficha de observación **Técnicas de procesamiento de datos** - **Estadística Descriptiva** - **Prueba de la "t"**