

**UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**



Presentado por

BEQUER BRAYAN OROSCO PAHUARA

“IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL”

ASESOR:

DR. JULIO CESAR HUANCA MARIN

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

ANDAHUAYLAS – APURÍMAC – PERÚ

2018



APROBACION DEL ASESOR

Quién suscribe:

Dr. Julio Cesar Huanca Marín por la presente:

CERTIFICA,

Que, el Bachiller en Ingeniería de Sistemas, BEQUER BRAYAN OROSCO PAHUARA ha culminado satisfactoriamente el informe final de tesis intitulado: "IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL" para optar el Título Profesional de Ingeniero de Sistemas.

Andahuaylas, 14 de Diciembre de 2018

Dr. Julio Cesar Huanca Marín
Asesor

Bequer Brayan Orosco Pahuara
Tesista



APROBACIÓN DEL JURADO DICTAMINADOR



LA TESIS: IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL, para optar el Título Profesional de INGENIERO DE SISTEMAS, ha sido evaluada por el Jurado Dictaminador conformado por:

PRESIDENTE: ING. JUAN JOSE ORÉ CERRÓN

PRIMER MIEMBRO: MSc. HUMBERTO SILVERA REYNAGA

SEGUNDO MIEMBRO: MSc. MAGALY ROXANA ARANGÜEÑA YLLANES

Habiendo sido aprobado por UNANIMIDAD/MAYORIA, en la ciudad de Andahuaylas el día 19 del mes de Noviembre de 2018

Andahuaylas, 14 de Diciembre de 2018.

ING. JUAN JOSE ORÉ CERRÓN
PRESIDENTE DEL JURADO DICTAMINADOR

MSc. HUMBERTO SILVERA REYNAGA
PRIMER MIEMBRO DEL JURADO DICTAMINADOR

MSc. MAGALY ROXANA ARANGÜEÑA YLLANES



FACULTAD DE INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

En la Av. José María Arguedas del Local Académico SL01 (Ccoyahuacho) en el auditorio de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 09:00 horas del día 19 de noviembre del año 2018, se reunieron los docentes: Ing. Juan José Oré Cerrón, Mg. Humberto Silvera Reynaga, MSc. Magaly Roxana Arangüena Yllanes, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL", cuyo autor es el Bachiller en Ingeniería de Sistemas **BEQUER BRAYAN OROSCO PAHUARA**, el asesor Dr. Julio César Huanca Marín, con el propósito de proceder a la sustentación y defensa de dicha tesis.

Luego de la sustentación y defensa de la tesis, el Jurado Evaluador **ACORDÓ: APROBAR** por **UNANIMIDAD** al Bachiller en Ingeniería de Sistemas **BEQUER BRAYAN OROSCO PAHUARA**, obteniendo la siguiente calificación y mención:

Nota escala vigesimal		Mención
Números	Letras	
15	Quince	Bueno

En señal de conformidad, se procedió a la firma de la presente acta en 03 ejemplares.

Ing. Juan José Oré Cerrón
Presidente del Jurado Evaluador

Mg. Humberto Silvera Reynaga
Primer Miembro del Jurado Evaluador

MSc. Magaly Roxana Arangüena Yllanes
Segundo Miembro del Jurado Evaluador

DEDICATORIA:

A mis padres, hermanos y familiares a quienes aprecio mucho, y estaré siempre agradecido por todo ese amor, fe, confianza y su muestra de apoyo incondicional.

AGRADECIMIENTO

A Dios, reconociendo que todo lo que somos y tenemos es porque él lo permite, inclusive nuestra vida. A mis padres, por su constancia y entusiasmo en seguir adelante.

Al Dr. Julio Cesar Huanca Marín, por su apoyo, enseñanza, dedicación y sobre todo por impulsarme a terminar la tesis.

A la Ing. Yovana Flores Ccorisapra, por brindarme su tiempo y colaboración en todo momento para el desarrollo de la tesis.

Finalmente, a la Universidad Nacional José María Arguedas, por su aporte considerable en mi formación y desarrollo profesional.

ÍNDICE

APROBACION DEL ASESOR	ii
APROBACION DEL JURADO DICTAMINADOR	iii
COPIA DEL ACTA DE SUSTENTACION	iv
DEDICATORIA	v
AGRADECIMIENTO	vi
RESUMEN	xii
ABSTRACT	xiii
CHUMASQA	xiv
CAPITULO 1: INTRODUCCIÓN	1
1.1 DATOS GENERALES	2
1.1.1. Título del proyecto	2
1.1.2. Autor del proyecto	2
1.1.3. Asesor del proyecto	2
1.1.4. Línea de investigación	2
1.1.5. Área priorizada del proyecto	2
1.1.6. Lugar de ejecución del proyecto	2
1.1.6.1 Localidad	2
1.1.6.2 Establecimiento	2
1.1. PLANTEAMIENTO DEL PROBLEMA	3
1.1.2. Realidad Problemática	3
1.1.1. Árbol de Problemas	5
1.2. Formulación del problema	6
1.3. Objetivos	6
1.3.1. Objetivo General	6
1.3.2. Objetivos específicos	6
1.4. Justificación	6
1.5. Viabilidad	8
1.6. Viabilidad económica	8
1.6.1. Presupuesto económico para el análisis e implementación	9
1.7. Viabilidad técnica	9
1.8. Viabilidad Operativa	10
1.9. Limitación del estudio	11
CAPÍTULO 2: MARCO TEÓRICO	11
2.1. Marco teórico	11
2.1.1. Antecedentes	11
2.2. Marco Conceptual	13
2.2.1. Cacti	13
2.2.1.1. Monitoreo con CACTI	14
2.2.1.2. Aplicación de CACTI	15
2.2.2. Performance de la red	15
2.2.3. Comparación de Equipos de Red Firewall UTM	15
2.2.4. Fortinet	16
2.2.4.1 Fortigate UTM	16
2.2.5. Redes Privadas Virtuales	17
2.2.6. Aplicaciones de las Redes Privadas Virtuales	18
2.2.7. Implementación de las Redes Privadas Virtuales	19
2.2.8. Requerimientos básicos para una VPN	19
2.2.9. Arquitecturas de VPN	20
2.2.9.1 VPN Sitio a cliente	20
2.2.9.2 VPN Sitio a Sitio	20
2.2.10. El Protocolo IPSec	21

2.2.11. Análisis del rendimiento de la red	21
2.2.12. Latencia	22
2.2.13. Protocolo ICMP	22
CAPITULO 3: MATERIALES Y MÉTODOS	24
3.1 Metodología PPDIOO	24
3.2 Fases para la administración de la red - PPDIOO	25
3.2.1 Preparación	25
3.2.2 Planeación	27
3.2.3 Diseño	28
3.3 Técnicas e instrumentos de recolección de datos	29
3.3.1 Método de la medición	30
3.4 Forma de determinar el ancho de banda a contratar	30
3.4.1 Entidad y ancho de banda de Internet contratado	30
3.4.2 Entidad y cantidad de matriculados	31
3.5. Forma de recomendar el equipo y modelo a utilizar	32
CAPITULO 4: RESULTADOS Y DISCUSIÓN	33
4.1 Presentación general de resultados	33
4.1.1 Pruebas del servicio a nivel LAN	33
4.1.2 Resultados obtenidos de las pruebas a nivel LAN	37
4.1.3 Conclusiones de las pruebas a nivel LAN	39
4.1.4 Pruebas del servicio a nivel WAN	39
4.1.5 Conclusiones de las pruebas a nivel WAN	43
4.1.6 Diagrama para las pruebas de funcionamiento	45
4.1.7 Máquinas virtuales utilizadas	45
4.1.8 Modo de configuración de los segmentos de red	47
4.1.9 Configuración de la VM con el Fortigate remoto	47
4.1.10 Configuración de la VM en el windows remoto	48
4.1.11 Configuración de la VM en el FortiAnalyzer	48
4.2 Enrutamiento	48
4.2.1 Configuración del enrutamiento en un equipo Fortigate	48
4.2.2 Verificación de los parámetros de las rutas	49
4.2.3 Verificaciones y monitoreo del enrutamiento por CLI	49
4.3 Link Monitor	50
4.3.1 Configuración de Link Monitor en el equipo Fortigate	51
4.3.2 Monitoreo y pruebas del Link Monitor	51
4.4 Balanceo de carga	52
4.4.1 Creación de la política para el balanceo de carga	53
4.4.2 Pruebas y monitoreo del balanceo de carga configurado	53
4.5 Alta disponibilidad (HA)	54
4.6 Filtro Web	57
4.7 Control de aplicaciones	61
4.8 Traffic Shaping	62
4.9 4.9 VPN y Acceso remoto a equipo Fortigate	62
CONCLUSIONES	63
RECOMENDACIONES	64
REFERENCIAS BIBLIOGRÁFICAS	65
ANEXOS	67
SOLICITUD DE ACCESOS Y DOCUMENTACIÓN A LA OSI	68
SOLICITUD DE ACCESOS Y DOCUMENTACIÓN RECIBIDO	69
CONSTANCIA DE TRABAJOS REALIZADOS EMITIDO POR LA OSI	70

CONTENIDO DE GRAFICOS

Gráfico 01: Redes privadas virtuales	1
Gráfico 02: Modo de interconexión de las sedes de la UNAJMA 2018	4
Gráfico 03: Diagrama de red actual – UNAJMA	7
Gráfico 04: Diagrama de una VPN en una organización	12
Gráfico 05: Funcionamiento de CACTI	14
Gráfico 06: Comparativa de Equipo de Seguridad	16
Gráfico 07: Integración de soluciones en una sola plataforma Fortigate	17
Gráfico 08: Fases de la Metodología PDDIO	24
Gráfico 09: Diagrama de interconexión de los locales de la UNAJMA	27
Gráfico 10: Ubicación de Central Yeastar instalada	33
Gráfico 11: Configuración de la Central Yeastar	33
Gráfico 12: Configuración del Teléfono IP Yeastar	34
Gráfico 13: Puertos disponibles en router Mikrotik – Sistemas	34
Gráfico 14: Puerto utilizado para conexión de Teléfono IP	35
Gráfico 15: Teléfono IP instalado y configurado	35
Gráfico 16: Configuración de enrutamiento en central telefónica	36
Gráfico 17: Anexos registrados en PBX central telefónica	36
Gráfico 18: Pruebas ICMP hacia teléfono IP instalado en local remoto	36
Gráfico 19: Pruebas ICMP hacia teléfono IP instalado en local central	37
Gráfico 20: Pruebas ICMP hacia Gateway de router en local central	37
Gráfico 21: Pruebas ICMP hacia Gateway de router en local remoto	38
Gráfico 22: Pruebas ICMP hacia IP WAN de router en local remoto	38
Gráfico 23: Test de Velocidad del servicio dedicado Movistar	39
Gráfico 24: Puertos en router y los servicios de Internet contratados	40
Gráfico 25: Pruebas de ICMP hacia los DNS de Telefónica	40
Gráfico 26: Valores de tiempo de respuesta hacia los DNS de Telefónica	41
Gráfico 27: Pruebas ICMP hacia los DNS de Google	42
Gráfico 28: Pruebas de tracert hacia los DNS de google	43
Gráfico 29: Datos de pool de IP publica contratado con Movistar	43
Gráfico 30: Pruebas de ICMP hacia los DNS de Telefónica	44
Gráfico 31: Diagrama de Red propuesto para la UNAJMA 2018	45
Gráfico 32: Topología diseñada para pruebas de funcionamiento	46
Gráfico 33: Fase 1 - Editar la configuración de las máquinas virtuales	47
Gráfico 34: Fase 2 - Editar la configuración global y LAN Segments	47
Gráfico 35: Fase 3 - Parámetros que contendrá cada VM	47
Gráfico 36: Modo de crear un enrutamiento estático	49
Gráfico 37: Parámetros de una ruta estática en el equipo FG	50
Gráfico 38: Muestra la tabla de enrutamiento con 2 rutas por defecto	51
Gráfico 39: Diagrama de funcionamiento de Link monitor	52
Gráfico 40: Muestra el tráfico saliente de acuerdo al destino disponible	53
Gráfico 41: Muestra el enrutamiento para el balanceo de carga	53
Gráfico 42: Muestra el tráfico saliente de acuerdo al segmento de red	54
Gráfico 43: Muestra el funcionamiento del HA	55
Gráfico 44: Diseño del diagrama para las pruebas de HA	55
Gráfico 45: Configuración del HA modo interfaz	56
Gráfico 46: Acceso configuración HA en Fortigate remoto	57
Gráfico 47: Muestra por interfaz el funcionamiento del HA por interfaz	58
Gráfico 48: Muestra la licencia de Filtro Web	58
Gráfico 49: Muestra Filtro web por default	58
Gráfico 50: Muestra las categorías del Filtro Web	59

<i>Gráfico 51: Muestra una regla que contiene el filtro web</i>	59
<i>Gráfico 52: Muestra habilitado el Filtro web en la regla</i>	59
<i>Gráfico 53: Muestra la acción al aplicar la regla</i>	60
<i>Gráfico 54: Muestra el mensaje de bloqueo con Filtro web</i>	60
<i>Gráfico 55: Muestra el mensaje de alerta y acceso por Filtro web</i>	60
<i>Gráfico 56: Muestra el modo de activar la autenticación de acceso</i>	61
<i>Gráfico 57: Muestra la alerta de acceso modo autenticación</i>	61
<i>Gráfico 58: Muestra el modo de verificar accesos y trafico web</i>	61
<i>Gráfico 59: Muestra el perfil por defecto de control de aplicaciones</i>	62
<i>Gráfico 60: Muestra el modo de añadir una aplicación al perfil</i>	62
<i>Gráfico 61: Muestra la acción que puede tomarse sobre la aplicación</i>	62
<i>Gráfico 62: Muestra el modo aplicar el perfil a una regla</i>	62
<i>Gráfico 63: Muestra el modo agregar el perfil a una regla</i>	63
<i>Gráfico 64: Muestra el modo de acceso por VPN portal</i>	64
<i>Gráfico 65: Muestra el modo de acceso por cliente</i>	64
<i>Gráfico 66: Muestra la sesión iniciada por la VPN</i>	64

CONTENIDO DE TABLAS

<i>Tabla 1: Relación de proveedor de Internet y tipo de servicio</i>	3
<i>Tabla 2: Relación de servicio de Internet y ancho de banda contratado</i>	28
<i>Tabla 3: Relación entre la entidad y el ancho de banda contratado</i>	30
<i>Tabla 4: Relación de entidad y cantidad de matriculados por periodo</i>	31
<i>Tabla 5: Instituciones y empresa con equipos Fortigate en el Perú</i>	32

RESUMEN

El presente proyecto tuvo como propósito evaluar y determinar las causas de la baja calidad en la comunicación de voz, video y datos en la Universidad Nacional José María Arguedas y para ello se realizó el levantamiento de la información del estado situacional actual a nivel de redes y comunicaciones que tiene la Universidad. Posteriormente, se realizó la implementación de una red privada virtual utilizando equipos Fortigate y una central VoIP PBX Yeastar para las pruebas de voz y llamadas entre locales remotos. Se verificó que la latencia y tiempos de respuesta entre los equipos utilizados para la interconexión de los locales, mantienen parámetros en rango aceptables, pero eventualmente estos presentan tiempos de desconexión. En las pruebas de llamadas telefónicas realizadas entre el local de la facultad de Sistemas y el local central de la Universidad, se verificó que las llamadas se establecen sin interferencias ni entrecortes siempre en cuando no se tenga latencia alta ni tiempos de espera en respuesta al local remoto. Para poner en prueba el funcionamiento de las características de los equipos Fortigate se utilizó máquinas virtuales y una topología de red orientada exclusivamente a equipos virtuales con la finalidad de demostrar y aplicar las reglas y políticas de seguridad que proporcionan estos equipos, adicionalmente se propuso que modelo y equipo Fortigate a utilizar. También se planteó un diagrama de red para la Universidad de acuerdo al alcance y el dimensionamiento de equipos.

Se logró determinar la causa de la baja calidad en la comunicación de voz, video y datos en la Universidad Nacional José María Arguedas, y finalmente, se recomendó que tipo de Internet y que ancho de banda debe contratarse para la operativa optima de la Universidad.

Palabras clave: Fortinet, RPV, Rendimiento, Metodología PPDIOO, Comunicaciones Voz, Video, Datos.

ABSTRAC

The purpose of this project was to evaluate and determine the causes of the low quality of voice, video and data communication in the National University José María Arguedas, and for this purpose the information on the current situation at the network and communications of the University was gathered. subsequently, the implementation of a virtual private network using Fortigate equipment and a VoIP PBX Yeastar for voice tests and calls, between remote buildings, was carried out. It was verified that the latency and response times between the equipment used for the interconnection of the buildings, maintain parameters in acceptable range, but eventually there was disconnection times. In the tests of telephone calls made between buildings of the faculty of Systems and the central building of the University, it was verified that the calls are established without interferences or interruptions whenever there is no high latency or waiting times in response to the local remote. In order to test the Fortigate equipment features, virtual machines and a network topology, oriented exclusively to virtual teams, was used, demonstrating and apply the security rules and policies provided by these equipments. Additionally, the model and Fortigate equipment to use was proposed. A network diagram for the University was also established according to the scope and dimensioning of the equipment. It was possible to determine the cause of the low quality of voice, video and data communication in the National University José María Arguedas, and finally, it was recommended what kind of Internet and what bandwidth is recommendable for the optimal operation of the University.

Palabras clave: Fortinet, RPV, Performance, PPDIOO Methodology, Voice Communications, Video, Data.

CHUMASQA

Kay qillqam yachachichwan mana allin kasqanta internet Universidad José María Arguedas. Chaypaqmi ruwarqaniku qayakunapaq comunicacion yachanapaq imaynan llankasqantan.

Chayrayqu ruwakurqa huk red privada virtualta universidadpaq, utilizarqaniku Fortigate equipukunata chaymi VoIP PBX Yeastar.

Hawachirqaniku mana allin internet kasqanta Universidadpi. Chaymi tarirqaniku sasachakuyta equipukunapi, chaynallataq tarirqaniku sasachakuyta internet contratasqapi, qinaqtimpi recomendarqaniku qayka interneta yapananpaq.

CAPITULO 1: INTRODUCCIÓN

En los últimos veinte años, el mundo ha experimentado grandes cambios. Ahora, un gran número de empresas, en vez de ocuparse sencillamente de cuestiones locales o regionales, tienen que pensar en mercados globales y en logística. Muchas disponen de instalaciones por todo el país o incluso el mundo. Aunque todas las empresas necesitan lo mismo: una forma de mantener comunicaciones rápidas, seguras y fiables no importa dónde se encuentren sus oficinas. (Cisco Systems Inc. 2008)

El uso que hacemos de Internet ha variado considerablemente desde su inicio, no sólo en los objetivos que nos acercan a esta herramienta, sino también en el ancho de banda que ocupamos cuando navegamos (Stolk, 2009)

Esto lleva al desarrollo continuo de tecnologías de la información y actualización de las ya existentes con el fin de satisfacer las necesidades de dichas organizaciones en este mundo globalizado. Las Redes Privadas Virtuales (VPN) constituyen una tecnología a la cual se le está dando cada vez mayor importancia puesto que permiten la transmisión de información a grandes distancias sin necesidad de implementar una compleja y costosa infraestructura de red. (Gonzales, 2006)

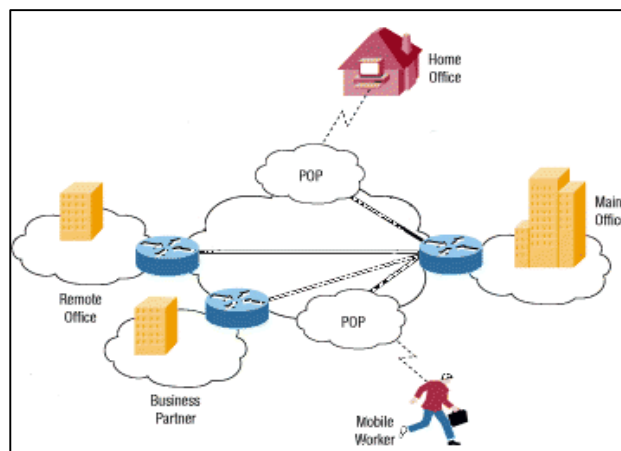


Gráfico 01: Redes privadas virtuales
Fuente: Cisco Systems Inc (2008)

1.1 DATOS GENERALES

1.1.1. Título del proyecto

Implementación y evaluación del performance de la comunicación de voz, video y datos entre los locales de la Universidad Nacional José María Arguedas mediante una red privada virtual.

1.1.2. Autor del proyecto

Nombres y apellidos : Bequer Brayan Orosco Pahuara
Escuela Profesional : Ingeniería de Sistemas
E-mail : Bequer.orosco@gmail.com

1.1.3. Asesor del proyecto

Nombres y apellidos : Dr. Julio Cesar Huanca Marín
Departamento Académico : Ingeniería y tecnología Informática
Categoría docente : Asociado a DE.
Modalidad : Ordinario
E-mail : apujulio@gmail.com

1.1.4. Línea de investigación

04 03 02 02 - Desarrollo de aplicaciones en sistema de comunicación (hardware y software)

1.1.5. Área priorizada del proyecto

04 03 02 02 - Desarrollo de aplicaciones en sistema de comunicación

1.1.6. Lugar de ejecución del proyecto

1.1.6.1 Localidad

Distrito Andahuaylas - Provincia Andahuaylas - Departamento Apurímac.

1.1.6.2 Establecimiento

En la Universidad Nacional José María Arguedas (SL01, SL02 y SL03)

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1. Realidad Problemática

En el Perú, diversas empresas e instituciones logran alcanzar una mayor productividad y agilizar sus procesos manteniendo sus sedes interconectadas, con una buena calidad en la comunicación de voz, video y datos.

La Universidad Nacional José María Arguedas cuenta con un local central ubicado en Andahuaylas y sus locales remotos de Santa Rosa y Ccoyahuacho, estos separados geográficamente por 06 KM y 04 KM respectivamente. Los locales se encuentran interconectados mediante enlaces inalámbricos. Actualmente las sedes remotas tienen acceso a internet mediante la sede central, y la Universidad no cuenta con una red privada virtual que integre la comunicación de voz, video y datos.

La Oficina de Sistemas de Información (OSI) de la UNAJMA recibe diariamente de los usuarios reportes de intermitencia en la red y la indisponibilidad de la comunicación de voz, video y datos. En este sentido se evidencia que actualmente se tiene una baja calidad en la comunicación de voz, video y datos en la UN Universidad Nacional José María Arguedas.

Cabe señalar que para poder garantizar la disponibilidad de la red y una calidad de servicio constante también es necesario evaluar el estado del servicio de Internet actualmente contratado por la Universidad.

Se detallada la información del servicio de Internet actualmente contratado por la Universidad Nacional José María Arguedas con cada proveedor de Internet.

Tabla 1: Relación de proveedor de Internet y tipo de servicio

Servicio de Internet actualmente Contratado - UNAJMA			
Proveedor	Tipo	BW	Garantía
Movistar	Int + Telf	20 Mb	40%
Movistar	Int + Telf	20 Mb	40%
Movistar	Int + Telf	15 Mb	40%
Movistar	Int + Telf	15 Mb	20%
Movistar	Int + Telf	08 Mb	20%
Movistar	Int + Telf	20 Mb	100%
Movistar	Fibra Óptica	20Mb	100%
Bitel	Fibra Óptica	05 Mb	100%

Fuente: Elaboración Propia

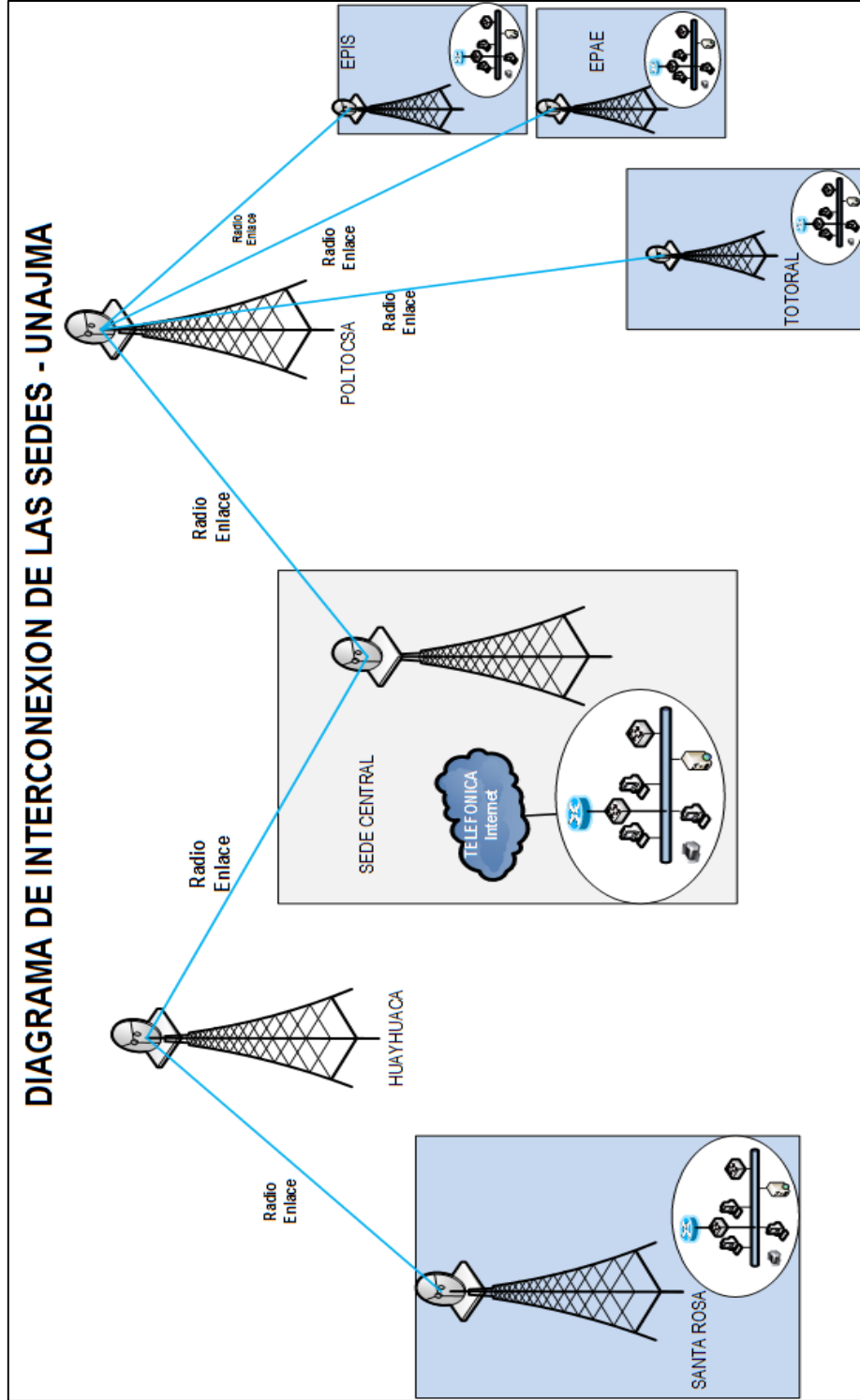
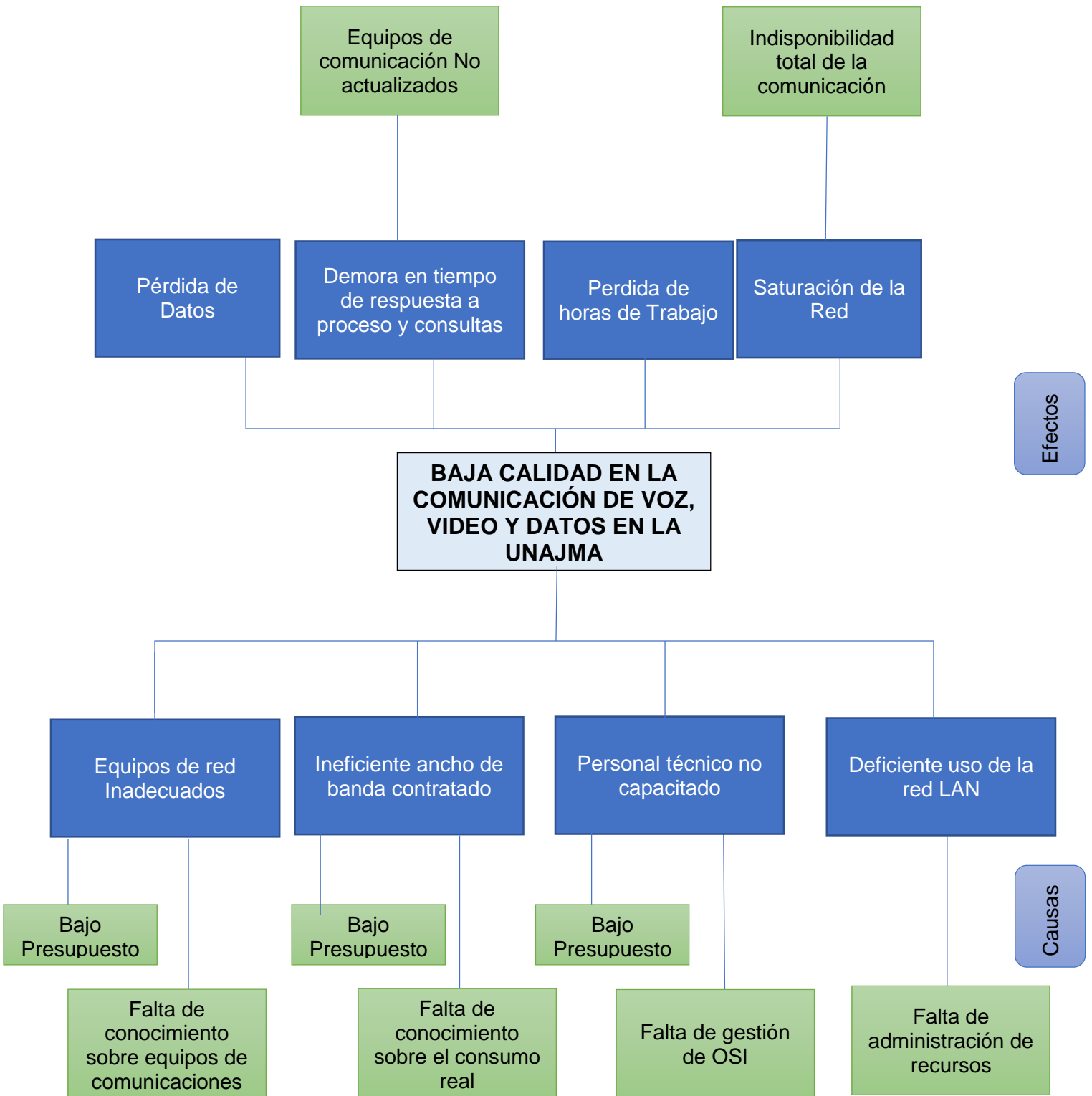


Grafico 02: Modo de interconexión de las sedes de la UNAJMA 2018

Fuente: Elaboración Propia

1.1.1 Árbol de problemas



1.2 Formulación del problema

¿Por qué existe baja calidad en la comunicación de voz, video y datos en la Universidad Nacional José María Arguedas?

1.3 Objetivos

1.3.6 Objetivo General

Implementar una red privada virtual con equipos Fortigate, para evaluar y determinar la calidad de la comunicación de voz, video y datos en la Universidad Nacional José María Arguedas.

1.3.7 Objetivos específicos

- a) Identificar la situación actual a nivel de red y comunicaciones de la Universidad.
- b) Realizar pruebas de comunicación de voz, video y datos entre los locales de la Universidad.
- c) Determinar la causa de la baja calidad en la comunicación de voz, video y datos en la Universidad.

1.4 Justificación

Actualmente la Universidad Nacional José María Arguedas mantiene una infraestructura de comunicación de voz, video y datos concentrada en su sede principal, es decir la conexión a internet de los locales de Santa Rosa y Ccoyahuacho dependen de la disponibilidad y la calidad de servicio del local principal. Adicionalmente los servicios y aplicaciones que se ejecutan en la sede principal son limitados y no tienen alcance hacia los locales de Santa Rosa y Ccoyahuacho, por consecuencia esto genera pérdida de datos, demora en tiempo de respuesta a procesos y consultas, pérdida de horas de trabajo y tiende a generar una saturación en la red al no tener equipos actualizados correctamente, inclusive generar una indisponibilidad total de la comunicación de voz, video y datos en la Universidad.

De acuerdo a esto se plantea que es de suma importancia determinar si el servicio de internet actualmente contratado es el óptimo y necesario para garantizar la conectividad y performance de la comunicación de voz, video y datos entre los locales de la UNAJMA, y evaluar el performance de la comunicación.

Se plantea implementar una red privada virtual mediante equipos Fortigate, el cual conectará y unificará los servicios y aplicaciones en la red, de manera que garantizará que la comunicación de voz, video y datos entre los locales de la Universidad sea optima y mejore los procesos y la operativa de la Universidad.

Esta interconexión de red entre los locales de la Universidad brinda inclusive la posibilidad de una comunicación del usuario de una oficina del local principal con los usuarios de las oficinas de otras facultades, a nivel de voz mediante llamadas telefónicas, video mediante la visualización de cámaras y/o videoconferencias, datos mediante la transferencia y acceso a los archivos, y adicionalmente el poder conectarse a los servicios de la institución desde sitios y localidades remotas de manera segura y confiable.

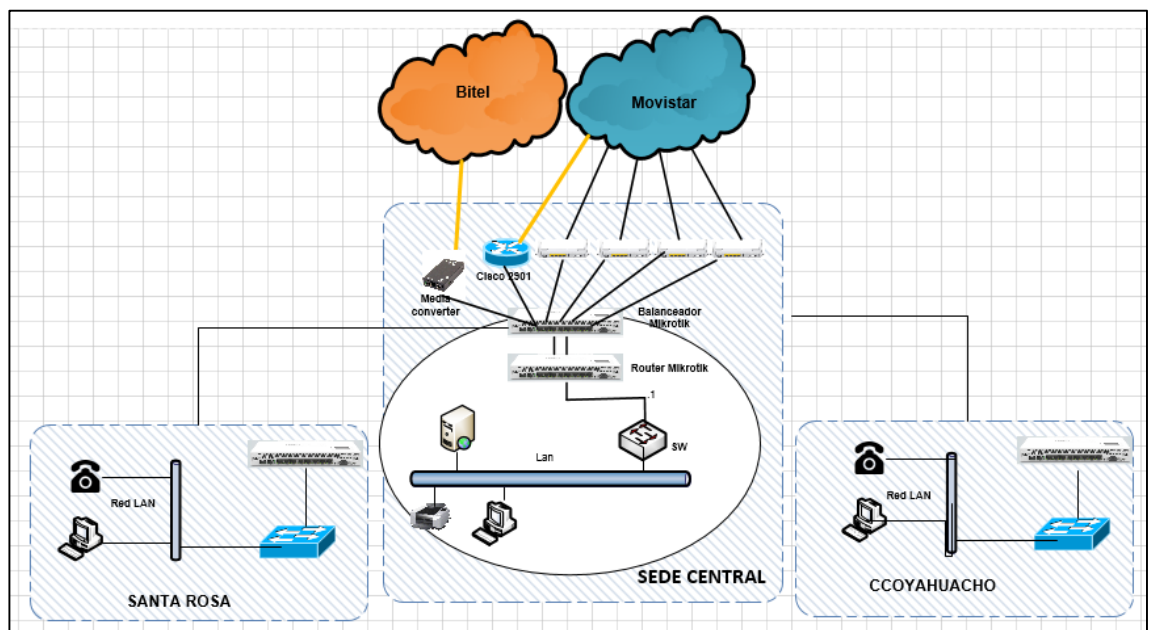


Gráfico 03: Diagrama de red actual - UNAJMA
Fuente: Elaboración propia

En la actualidad surge la necesidad de estar en constante comunicación, gracias al Internet podemos recibir una respuesta inmediata en cuestión de segundos sin importar que los usuarios de la comunicación se encuentren separados geográficamente. Interconectar las sedes de la Universidad Nacional José María Arguedas utilizando un medio físico de fibra óptica tiende a ser muy costoso y sugiere no adecuarse a la geografía de la localidad, considerando que adicionalmente la distancia de ubicación de los locales de la Universidad Nacional José María Arguedas se encuentra muy alejadas.

Por lo tanto, es necesario que se evalúe el performance de la comunicación de voz, video y datos entre las sedes de la Universidad Nacional José María Arguedas mediante una red privada virtual.

1.5 Viabilidad

La viabilidad del presente proyecto es determinada por los siguientes aspectos.

1.6 Viabilidad económica

Para la implementación de una Red Privada Virtual en la UNAJMA se utilizará la infraestructura de red actual, resultando está más económica a comparación de un despliegue de red físico. Inclusive se reducirá los costos de implementación que puedan ser generados en contratar un ISP (proveedor de servicios de internet).

La gestión y equipos necesarios la para la habilitación de los recursos y gastos económicos del presente proyecto, serán asumidos directamente por el investigador, del mismo modo con la adquisición de los componentes tecnológicos a nivel de hardware y software necesarios para la implementación y pruebas según corresponda.

En los siguientes cuadros se detalla el presupuesto y los componentes necesarios para la implementación de la solución propuesta, considerando los valores que se muestran como montos referenciales.

1.6.6 Presupuesto económico para el análisis e implementación

FASE DE ANALISIS	Diagnóstico de la red. Local Central y locales remotos.	S/.500.00
	Análisis de restricciones físicas y requerimientos de conectividad.	S/.500.00
	Definición del alcance y dimensionamiento a nivel de hardware y software.	S/.2800.00
FASE DE IMPLEMENTACION	Direccionamiento IP de los Locales	S/.200.00
	Preparación del local central y remoto para la instalación de equipos.	S/.500.00
	Configuración de los Dispositivos de conexión (Router, Central Yeastar, Firewall Fortigate, teléfonos IP, etc)	S/.250.00
	Configuración de los Equipos necesarios en cada local.	S/.500.00
FASE FINAL	Capacitación del funcionamiento a la OSI (UNAJMA)	S/.450.00
	Pruebas y validaciones con el usuario final (OSI).	S/.500.00

1.7 Viabilidad técnica

Para realizar el presente proyecto será necesario la habilitación de componentes, equipos de comunicaciones y herramientas de software, estos serán simulados mediante máquinas virtuales de manera que se pueda demostrar el funcionamiento y operatividad de la red privada virtual mediante las políticas de seguridad configuradas.

Se detalla los componentes necesarios para la implementación:

SOFTWARE	
Descripción	Unidades
Herramienta de monitoreo CACTI	1
VMWARE	1
CENTOS	1

HARDWARE	
Descripción	Unidades
Equipo CPU – SERVIDOR	3
FORTIGATE UTM	2
CENTRAL YEASTAR	1
SWITCH	4
TELEFONOS IP	3

1.8 Viabilidad Operativa

El desarrollo del proyecto es viable operativamente, porque es evidente que en la actualidad no existe una comunicación de los servicios y aplicaciones a nivel de red entre los locales de la Universidad Nacional José María Arguedas, y existe una baja calidad en la comunicación de voz, video y datos, esto trae como consecuencia el deficiente servicio de internet para cada uno de sus locales; adicionalmente se cuenta con la aprobación y disposición de la parte administrativa y OSI para la ejecución del proyecto.

Cabe señalar que posterior a la implementación de la solución, se realizara la validación de lo implementado, tomando como usuario final a la oficina de sistemas de información (OSI), de la UNAJMA. Es decir, se elevará un documento tipo check_list para que sea esta quien valide las pruebas de lo implementado y posterior a ello se determine el performance y la baja calidad de la comunicación de voz, video y datos de la Universidad.

1.9 Limitación del estudio

La orientación del presente proyecto es exclusivamente para la Universidad Nacional José María Arguedas, ya que es evidente que en la actualidad los locales no se encuentran interconectados con medios óptimos para su real aprovechamiento y operatividad de red, y mantienen una baja calidad en la comunicación a nivel de voz, video y datos.

CAPÍTULO 2: MARCO TEÓRICO

2.1. Marco teórico

2.1.1. Antecedentes

Díaz (2010) en su proyecto de Diseño e Implementación de una Red Privada Virtual para la Empresa Eléctrica Quito S.A, refiere que las políticas de modernización han llevado a mejorar el equipamiento de seguridad perimetral de la red corporativa, y que se ha añadido un nuevo servicio que es la VPN, lo que abrirá sin duda otras opciones de conectividad para el acceso a los servicios de la LAN Interna. También menciona que un equipo UTM Fortigate permite a más de la funcionalidad de firewall convencional, la posibilidad de controlar amenazas por medio de su IPS incorporado, el filtrado de contenido, antivirus y antispam y que mejoran la seguridad perimetral de la red corporativa.

Menéndez (2012). En su tesis Estudio del Desempeño e Implementación de una Solución MPLS-VPN sobre múltiples sistemas Autónomos. Define el concepto de una red privada virtual como una estructura de red que emula una red privada sobre infraestructura pública existente. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios. Además, añade que el equivalente lógico a esta red VPN sería un enlace privado punto a punto (peer-to-peer), que es sumamente costoso si se trata de extender la red a grandes distancias, debido al requerimiento de cableado y equipos en la localidad a la cual se quiera llegar.

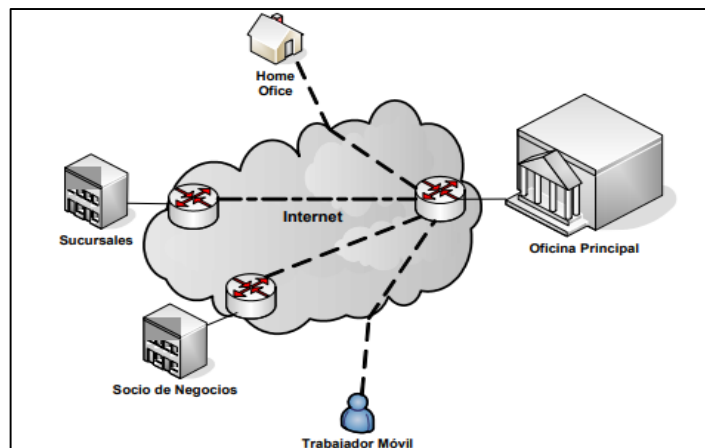


Gráfico 04: Diagrama de una VPN en una organización
Fuente: Trujillo (2006)

Álvarez et al. (2014) Concluye que en definitiva, las redes privadas virtuales resultaron un tema bastante sencillo de abordar en primera instancia, pues la información es relativamente abundante y fácil de entender, más lo complejo vino al ir entendiendo y profundizando en el tema. Estas redes artificiales nacieron para poder abaratar costos a nivel empresarial, reemplazando las conexiones dedicadas punto a punto por cables físicos al utilizar la Internet como su estructura y camino esencial. ¿Cómo poder controlar todo lo que se trafica? En la red son solo algunos los participantes, no cualquier usuario en la Internet puede aparecer en ésta, y así nacen una serie de protocolos que ayudan a las bases de la VPN, aportando confidencialidad, integridad y autenticación. Siendo IPSec el estándar “de-facto” para las VPN, nuestro foco se mantuvo en comprender sus componentes y cómo actúa el set de protocolos y cómo los datos son transmitidos entre emisor y receptor. Los tipos de conexiones, implementaciones y de redes privadas virtuales en sí son las que ayudan a resolver distintos escenarios y necesidades de conexión tanto para clientes finales como grandes empresas, siendo esto lo que nos llevó a nuestra parte práctica. Configurar un cliente y servidor VPN a nivel Internet es complejo, son muchas variables de seguridad en el equipo los que hay que manejar y comprender para que otros usuarios puedan participar de nuestra red, mas con ayuda de Hamachi, que es un VPN personal con directorio y servidor centralizado, estos problemas son fácilmente solucionables para un usuario estándar. Siendo que las configuraciones de VPN actuales disponibles en

routers, firewalls, y en los mismos sistemas operativos parecen simples, queda el reto de hacerlas disponibles para usuarios finales, así sería más eficiente y sencillo el uso para cualquiera con nociones de redes de computadores, pues la multiplicidad de protocolos y opciones parecen aturdir el proceso. Pero, es ésta misma la que facilita la disponibilidad para un amplio espectro de dispositivos y recibe la comunicación.

2.2. Marco Conceptual

2.2.1. Cacti

Cacti es un paquete libre y de la open-source de software diseñada a utilizar el SNMP para recopilar estadística de los dispositivos capaces del SNMP, incluyendo los dispositivos de Cisco y los interruptores, así como los servidores y los sitios de trabajo. CACTI constituye un completo almacenamiento de toda la información necesaria para crear los gráficos y los agrupan en una base de datos de MySQL. Cacti tiene capacidades incorporadas del SNMP. Es capaz de la interrogación de todos los dispositivos SNMP en la red, y la adición de la información seleccionada ingresa a los gráficos. En su forma más simple, los cactos le darán la capacidad de agregar un gráfico para los aspectos más comunes del usuario que supervisa (espacio de disco, promedio de la carga, uso de la memoria, etc.) y la supervisión de la red (los octetos dentro y fuera de un interfaz).

Es una completa solución para el monitoreo de redes. Utiliza RRdtool (herramienta de la base de datos, diseñada para manejar datos en series de tiempo como: ancho de banda, temperatura, carga de la CPU, etc.) para almacenar la información de los dispositivos y aprovechar sus funcionalidades de graficación. Proporciona un esquema rápido de obtención de datos remotos, múltiples métodos de obtención de datos (SNMP, scripts), un manejo avanzado de templates, y características de administración de usuarios. Además ofrece un servicio de alarmas mediante el manejo de umbrales. Todo ello en una sola consola de administración. (Díaz, 2006)

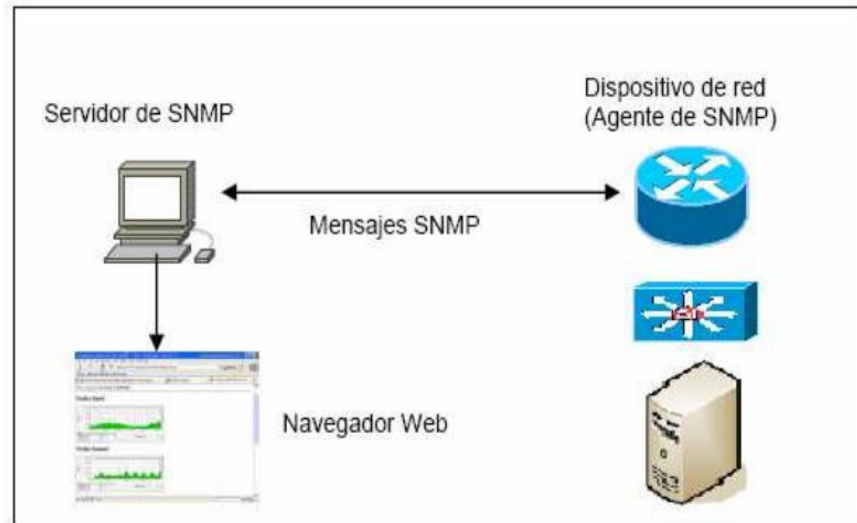


Gráfico 05: Funcionamiento de CACTI
Fuente: (Díaz, 2006)

2.2.1.1. Monitoreo con CACTI

Cacti es un sistema de monitorización con el que podemos tener controlados casi en tiempo real los dispositivos que soportan los servicios que presta nuestra red (routers, conmutadores o servidores, tráfico de interfaces, cargas, CPU, temperaturas, etc.). Es un potente software que nos permite controlar en todo momento el estado de nuestra red. Este sistema de monitorización contiene un recolector de datos excelente, un sistema avanzado de creación de plantillas y gráficos y una completa interfaz de gestión de usuarios. La aplicación está construida en php, y utiliza MySQL para el almacenamiento de información sobre los gráficos y datos recogidos. El protocolo utilizado para la comunicación con los distintos equipos es SNMP, el cual facilita el intercambio de información de administración entre dispositivos de red y permite a los administradores supervisar el uso de la red, buscar y resolver sus problemas, y planificar su crecimiento. MRTG.; siendo una de las partes más útiles de la herramienta Cacti es la monitorización a través de gráficas. (Peinado, 2012).

2.2.1.2. Aplicación de CACTI

La elección del enfoque de monitoreo a emplear debe siempre partir del objetivo que se persigue con el mismo (medir el rendimiento o caracterizar y/o contabilizar el uso de la red), no olvidando que el enfoque activo agrega tráfico a la red y en dependencia del ancho de banda que se dispone, pudiera esto convertirse en una desventaja. El monitoreo pasivo puede realizarse a través de distintas técnicas, las cuales pueden acompañarse de la definición de métricas o alarmas garantizando así el buen funcionamiento de los dispositivos de red. Es importante definir el alcance de los dispositivos de monitoreo, así como el espectro a analizar en cada uno de ellos logrando de esta forma una estrategia de monitoreo eficiente. Es necesario una correcta selección de las herramientas y dispositivos a emplear dentro de la red, en función de optimizar los recursos y la propia infraestructura. (Junco et al, 2018)

2.2.2. Performance de la red

Cruz (2013) En el resumen de su proyecto "Aplicación para analizar el rendimiento de red", considera que el rendimiento se evalúa identificando los equipos que generan el tráfico presente en la red y clasificando este según los protocolos de nivel de enlace, red, transporte o aplicación al que corresponde.

2.2.3. Comparación de Equipos de Red Firewall UTM

Se detalla la comparación de los siguientes equipos, realizada por la NSSLabs (2013). FW-1301, WatchGuard XTM 1050. Evaluación en base a seguridad, performance, administración, costos.

Product	Protection & Management	Value	Overall
Barracuda F800	Neutral	Recommended	Neutral
Check Point 12600	Recommended	Recommended	Recommended
Cisco Systems	Caution	Caution	Caution
Cyberoam CR2500iNG	Caution	Neutral	Neutral
Dell SonicWALL NSA 4500	Recommended	Neutral	Neutral
Fortinet FortiGate-800c	Recommended	Recommended	Recommended
Juniper SRX550	Recommended	Recommended	Recommended
NETASQ NG1000-A	Caution	Caution	Caution
NETGEAR ProSecure UTM95	Caution	Caution	Caution
Palo Alto Networks PA-5020	Recommended	Neutral	Neutral
Sophos UTM 425	Caution	Caution	Caution
Stonesoft FW-1301	Recommended	Recommended	Recommended
WatchGuard XTM 1050	Recommended	Neutral	Neutral

Gráfico 06: Comparativa de Equipo de Seguridad

Fuente: Artes et al (2013)

2.2.4. Fortinet

La misión de Fortinet es ofrecer la red más innovadora y de mayor rendimiento estructura de seguridad para asegurar y simplificar su infraestructura de TI. Es un líder mundial de proveedor de dispositivos de seguridad de red para operadores, centros de datos, empresas y oficinas distribuidas.

2.2.4.1 Fortigate UTM

Fortigate es un Firewall basado en hardware desarrollado por Fortinet. El sistema de Fortigate es el único sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar al rendimiento de la red, incluso para aplicaciones en tiempo real como la navegación Web. Las soluciones de FortiGate también incluyen; firewall, filtrado de contenido, VPN, antivirus, antispam, detección y prevención de intrusos, gestor de tráfico y balanceo de carga.

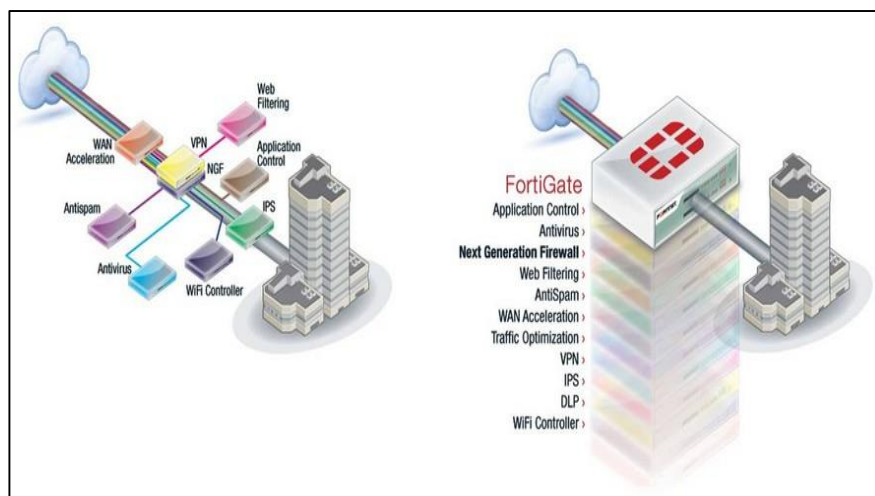


Gráfico 07: Integración de soluciones en una sola plataforma Fortigate
Fuente: Sitio oficial Fortinet

2.2.5. Redes Privadas Virtuales

Virtual Private Network (VPN) es un grupo de dos o más sistemas de ordenadores, generalmente conectados a una red corporativa privada, que se comunican "con seguridad" sobre una red pública. Es decir, que para transmitir información a través de una red pública (insegura), en la VPN se aplican métodos de seguridad para garantizar la privacidad de los datos que se intercambian entre ambas, y protocolos de túneles.

A las Redes Privadas Virtuales, se les considera "privadas" porque se establecen exclusivamente entre el emisor y el receptor de la información, y "virtuales", porque no se necesita un cable o cualquier otro medio físico directo entre los comunicantes. Las VPN extienden la red corporativa de una empresa a las oficinas distantes, por ejemplo. En lugar de alquilar líneas dedicadas con un costo muy elevado, utilizan los servicios mundiales de IP, incluyendo la Internet. Usando una VPN, se crea una conexión privada segura a través de una red pública como Internet. Los usuarios remotos pueden hacer una llamada local a Internet, y no usar llamadas de larga distancia. (Trujillo, 2006).

2.2.6. Aplicaciones de las Redes Privadas Virtuales

Hernández et al (2006). Cuando la informática evoluciona, se comprueba que no es suficiente con procesar la información, sino que además, es preciso compartir esta información entre distintos equipos, así como los recursos que pueden ser muy costosos también se pueden compartir. Nace la Red de Área Local (LAN - Local Area Network). ¿Qué ocurre en este caso cuando tenemos que transmitir información confidencial de un equipo a otro?, la solución pasa por interconectar entre si aquellos equipos que comparten la información confidencial, separando físicamente la red confidencial de la red general. Esto presenta varios problemas, el primero es la duplicidad de recursos de red que se necesitan, ya que tendremos que montar y mantener dos redes. La segunda es que aun así la confidencialidad no se puede considerar segura, puesto que la seguridad viene impuesta por la separación física de las dos redes, pero nada impide que en una determinada parte de la instalación alguien se pueda conectar a dicha red y leer los datos que circulan. La solución pasa por usar la misma red general para transmitir la información confidencial junto a la información abierta. Por consiguiente, aquí nace el primer escenario de aplicación de las Redes Privadas Virtuales, como separación en una Intranet de aquellos departamentos, personas o equipos, que no deban tener acceso a la información confidencial de los que sí la puedan tener. El siguiente paso de la Informática, se da de la mano de holdings empresariales, que tienden a extender sus negocios en varios edificios y que necesitan interconectar entre sí todas sus oficinas. En este caso las soluciones de interconexión pasaban por utilizar líneas punto a punto, X25, Frame Relay, etc. conocidas con el nombre de Redes de Área Extensa (WAN - Wide Área Network). En este caso la información se puede considerar hasta cierto punto segura, ya que los conocimientos necesarios para poder acceder a las líneas, no se encuentra al alcance de cualquier persona, además de los equipos necesario para ello.

2.2.7. Implementación de las Redes Privadas Virtuales

Fernández et al (2006) Sugiere que. “Las redes privadas virtuales, deben de ser transparentes a los usuarios o aplicaciones que las utilizan”.

Albeiro (2010) Definir un entorno común para la mediana empresa resultaría desgastante, teniendo en cuenta la cantidad de actividades comerciales existentes, pero el desarrollo de su actividad siempre busca la expansión y el posicionamiento de su marca dentro de un área geográfica, sea esta una ciudad, un departamento, el país y más. Este crecimiento, en la mayoría de las oportunidades se encuentra ligado a la oportunidad, la legislación y los ciclos económicos. En ese punto es cuando la organización inicia el proceso para determinar qué herramientas va a utilizar y determina los costos operativos de esas soluciones. Generalmente, se inicia con un acceso a Internet para efectos de comunicación, y en consecuencia, un firewall que asegure la integridad de la red interna frente a ataques externos, administrando de paso este recurso. Seguido y con base en el tipo de expansión que la mediana empresa busca, se presentan alternativas de comunicación en las cuales se arrienda un servicio (canales dedicados) o se implementa una solución de redes privadas virtuales (VPN). La definición de dicho medio de comunicación se basa en el costo, la eficiencia, la calidad de servicio que estas redes aporten, no sin antes advertir las particularidades propias de ubicación geográfica de las agencias.

2.2.8. Requerimientos básicos para una VPN

Trujillo (2006). Sugiere que una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puede obviarse algunos.

Autenticación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.

Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.

Encriptación de datos, los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.

Administración de claves, debe mantener un mantenimiento de claves de encriptación para los clientes y los servidores.

Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando la red pública, por ejemplo, IPX, IP, etc.

2.2.9. Arquitecturas de VPN

2.2.9.1 VPN Sitio a cliente

Con las VPN de sitio a cliente, los trabajadores móviles pueden acceder de forma remota a los recursos de la información corporativa, cada uno administrado con el perfil de acceso y limitación que corresponda.

2.2.9.2 VPN Sitio a Sitio

Colomes (2010) En su artículo "Interconectando sucursales mediante una VPN IPsec Site-to-Site" refiere que el caso de interconexiones de sucursales es bastante recurrente y se debe emplear una solución que permita tener a todos los empleados sincronizados en la red remota y además que la conexión cuando pase por Internet desde A hacia B se haga mediante un túnel seguro (cifrado) para prevenir problemas de interceptación de las transacciones. Algunas cosas que hay que saber antes de configurar son, por ejemplo, que IPsec es un estándar de la industria, por lo que no solamente funciona bien en routers Cisco, sino que también en Huawei, Juniper, Routers Linux, Windows, entre varios. Uno de los componentes principales de IPsec es IKE (Internet Key Exchange) el cual tiene como objetivo intercambiar información entre los peers involucrados. La información que intercambia Router_A con Router_B va desde las claves pre compartidas (Preshared Key) hasta el tipo de algoritmos de hash y cifrado que se utilizarán (AES, DES, 3DES, MD5, SHA, etc.)

2.2.10. El Protocolo IPSec

Trujillo (2006). Refiere que el protocolo IPSec en realidad es un conjunto de estándares para integrar en IP, funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3. El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES que se espera sea el más utilizado en un futuro próximo.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

2.2.11. Análisis del rendimiento de la red

Urdaneta (2005), realizó una investigación titulada Análisis de Tráfico en una Red LAN aplicando la Tecnología de Redes Neuronales, el propósito de esta investigación fue evaluar la aplicabilidad de la tecnología de redes neuronales para el análisis de tráfico en la red de área local del colegio universitario.

Rincón (2003), realizó una investigación titulada Modelo Matemático para la Estimación del Performance de una Red Ethernet, el propósito de esta investigación fue formular un modelo matemático que permita la estimación del rendimiento de una red Ethernet. La investigación fue de campo de carácter explicativo, concluyó que el comportamiento de la red Ethernet de la licenciatura en computación de la Universidad del Zulia, permitió definir las variables fundamentales del modelo matemático a formular. Planteó algunas recomendaciones como el análisis de otros parámetros para la medición del rendimiento de redes Ethernet, como retardo promedio y throughput, entre otros.

2.2.12. Latencia

Valdivia (2006). Refiere que la latencia es el retardo que se produce entre el tiempo en que una trama comienza a dejar el dispositivo origen y el tiempo en que la primera parte de la trama llega a su destino. Existe una gran variedad de condiciones que pueden causar retardos mientras la trama viaja desde su origen a su destino. Retardos de los medios causados por la velocidad limitada a la que las señales pueden viajar por los medios físicos. Retardos de circuito causado por los sistemas electrónicos que procesan la señal a lo largo de la ruta. Retardos de software causados por las decisiones que el software debe de tomar para implementar la comunicación y los protocolos. Retardos causados por el contenido de la trama y en que parte de la trama se pueden tomar las decisiones de conmutación. Por ejemplo un dispositivo no puede tomar las decisiones a su destino hasta que la dirección MAC destino haya sido leída.

2.2.13. Protocolo ICMP

Ortiz (2003), Refiere que el Servicio ICMP (Internet Control Message Protocol), se establece para el intercambio de información sobre las dificultades de ruteo con paquetes IP o intercambios simples como son las peticiones de eco y respuesta de eco. ICMP es utilizado principalmente para enviar información, acerca del éxito o falla de los paquetes de información enviados a través de la red.

Cuando un paquete de información no llega a su destino, los ruteadores se encargan de transmitir un mensaje ICMP, incluyendo el tipo de error que se generó en la red.

Por ejemplo, “no se puede alcanzar la red de destino”, “host no existente”, o “puerto no se puede alcanzar”. Cuando se genera la petición de eco se inicializa un contador, que mide el tiempo de respuesta de dicha petición. Sabemos que cualquier paquete en tránsito de red, tiene un tiempo de vida establecido. Si la respuesta excede este tiempo de vida, el paquete es descartado por la red y ésta envía un mensaje ICMP de error.

CAPITULO 3: MATERIALES Y MÉTODOS

Para el desarrollo de este proyecto se utiliza la metodología PDDIOO.

3.1 Metodología PPDIOO

La metodología PPDIOO posee su origen bajo los lineamientos propuestos en el ciclo de vida PPDIOO que usa Cisco para administración de red. El seguimiento de este ciclo de vida propuesto ayuda a cumplir objetivos trazados como son la disminución del costo total de administración de la red y aumento de disponibilidad de la red a su vez mejora en agilidad para implementación de cambios en la estructura de la red. El ciclo de vida así puede ser útil para implementación de nuevas redes así como para actualizaciones en redes existentes. Los elementos que conforman el ciclo de vida forman un círculo sin fin puesto que por ejemplo el paso de optimización conlleva a realizar actividades como identificar cambios, validar en la infraestructura existente; misma que conllevarían a iniciar desde el paso de preparación. (Erazo, 2016).



Gráfico 8: Fases de la Metodología PDDIOO
Fuente: Elaboración propia

3.2 Fases para la administración de la red - PPDIOO

3.2.1 Preparación

Se ha realizado la solicitud a la oficina de Sistemas de Información (OSI), para la habilitación de accesos a la información del dimensionamiento de la red y comunicaciones de la UNAJMA, adicionalmente se ha solicitado al Presidente Vice académico para que mediante la (OSI), se facilite los permisos de accesos a los ambientes de la Universidad donde se encuentran instalados los equipos de redes y comunicaciones.

Se ha realizado el levantamiento de la información del estado situacional actual, a nivel de infraestructura de red y comunicaciones que mantiene la Universidad Nacional José María Arguedas.

Esta información comprende el tipo de servicio de internet contratado, proveedor de internet (ISP), nivel de servicio y los equipos que son utilizados para el despliegue de la red desde el local central hacia los locales remotos.

En base a esta información, se ha consolidado las deficiencias y carencias con las que cuenta la Universidad Nacional José María Arguedas asociadas a la baja calidad en la comunicación de voz, video y datos entre los locales. Todo esto manteniendo a la Oficina de Sistema de Información (OSI) como usuario final evaluador para la solución propuesta.

Se ha identificado los principales problemas que tiene actualmente la Universidad respecto al servicio de internet y la interconexión del servicio de comunicaciones de red.

Identificación de reportes y solicitudes.

Se ha procedido a identificar los principales problemas que tiene la Universidad actualmente con el servicio de internet y la interconexión del servicio de comunicaciones, siendo los siguientes.

- **Sin acceso a Internet**

La oficina se sistema de información (OSI), recibe diariamente incidencias de reporte de pérdida de conexión a internet por parte de los usuarios de la Universidad.

- **Lentitud en el acceso a Internet**

La oficina se sistema de información (OSI), recibe diariamente incidencias de reporte de lentitud de conexión a internet por parte de los usuarios de la Universidad.

- **Intermitencia en el acceso a Internet**

La oficina se sistema de información (OSI), recibe diariamente incidencias de reporte de conexión y desconexión a internet por parte de los usuarios de la Universidad.

La red privada virtual implementada interconectara los servicios y equipos a nivel de red y comunicaciones mejorando la calidad del servicio de Internet y comunicaciones para toda la Universidad.

Se muestra de forma tentativa, el presupuesto y los componentes necesarios para la implementación de la solución propuesta, considerando los montos como referenciales.

FASE DE ANALISIS	Diagnóstico de la red. Local Central y locales remotos.	S/.500.00
	Análisis de restricciones físicas y requerimientos de conectividad.	S/.500.00
	Definición del alcance y dimensionamiento a nivel de hardware y software.	S/.2800.00
FASE DE IMPLEMENTACION	Direccionamiento IP de los Locales	S/.200.00
	Preparación del local central y remoto para la instalación de equipos.	S/.500.00

	Configuración de los Dispositivos de conexión (Router, Central Yeastar, Firewall Fortigate, teléfonos IP, etc.)	S/250.00
	Configuración de los Equipos necesarios en cada local.	S/500.00
FASE FINAL	Capacitación del funcionamiento a la OSI (UNAJMA)	S/450.00
	Pruebas y validaciones con el usuario final (OSI).	S/500.00

3.2.2 Planeación

El dimensionamiento y estructura de la red y las comunicaciones de la Universidad se detallan en el siguiente gráfico.

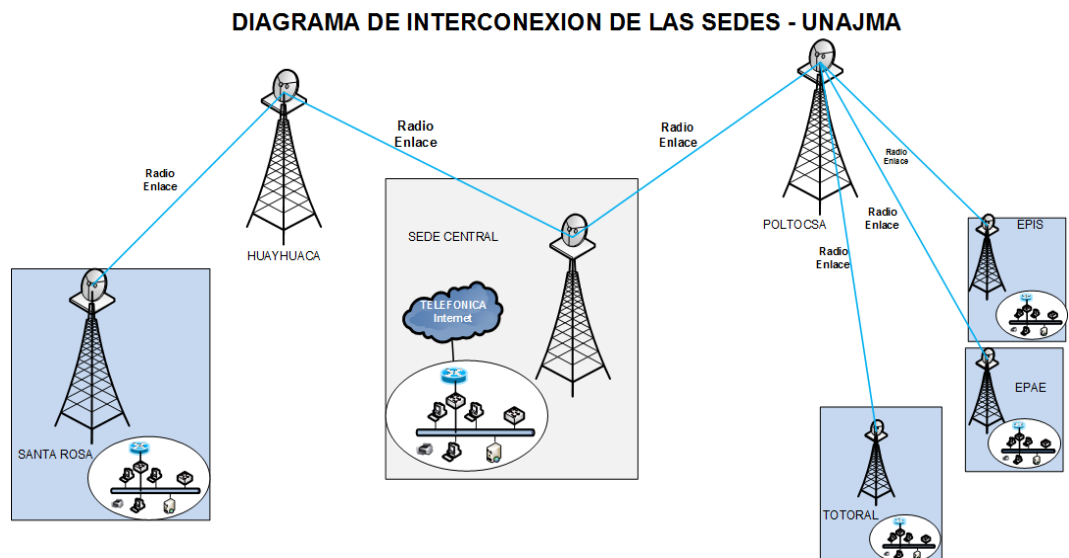


Gráfico 9: Diagrama de interconexión de los locales de la UNAJMA.
Fuente: Elaboración Propia

- **Análisis del servicio de Internet actual y consumo del Ancho de Banda en la UNAJMA**

Para el monitoreo de la red y reporte de consumo de ancho de banda se recomienda utilizar una herramienta basada en software libre, el cual puede ser instalado en una máquina virtual, con la función de monitorear la red,

Tabla 2: Relación de servicio de Internet y ancho de banda contratado.

Servicio Actual de Internet Contratado - UNAJMA			
Proveedor	Tipo	BW	Garantía
Movistar	Int + Telf	20 Mb	40%
Movistar	Int + Telf	20 Mb	40%
Movistar	Int + Telf	15 Mb	40%
Movistar	Int + Telf	15 Mb	20%
Movistar	Int + Telf	08 Mb	20%
Movistar	Int + Telf	20 Mb	100%
Bitel	Fibra Óptica	05 Mb	100%

Fuente: Elaboración propia

3.2.3 Diseño

En esta fase se logra determinar un modelo de red lógico que permite una segmentación del ancho de banda actualmente contratado, se determina el BW máximo por facultad, inclusive se limita el BW para la navegación de cada usuario.

Se detalla los componentes necesarios para la implementación:

SOFTWARE	
Descripción	Unidades
Herramienta de monitoreo CACTI	1
VMWARE	1
CENTOS	1

HARDWARE	
Descripción	Unidades
SERVIDOR	4
FORTIGATE UTM	2
CENTRAL YEASTAR	1
SWITCH	4
TELEFONOS IP	3

3.3 Técnicas e instrumentos de recolección de datos

En esta investigación se utilizó la técnica de recolección de información, se realizó una entrevista al personal que labora en la Oficina de Sistemas de Información, de la Facultad de Ingeniería de Sistemas de la Universidad en el mes de octubre del año 2018, en donde se consolidó la información del tipo de servicio de Internet que tiene contratado la Universidad, los equipos instalados por los proveedores de Internet, así como el modelo de equipos propios de la Universidad utilizados para el despliegue de la comunicación de red a los usuarios.

La universidad cuenta con un promedio de 1700 usuarios que disponen del servicio de Internet, sea por medio físico Ethernet o medio inalámbrico WIFI, tiene 2 proveedores de internet (Movistar y Bitel), cada uno de estos tienen instalado en el cuarto de comunicaciones de la Universidad un equipo router y un Media converter para la línea dedicadas de fibra óptica.

Estos equipos router instalados por los proveedores sirven para el monitoreo y la validación de la operatividad del servicio brindado.

Por parte de la Universidad se cuenta con un equipo Mikrotik Cloud Core utilizado como balanceador de los servicios de Internet por ADSL y Fibra Óptica, y un equipo Mikrotik utilizado para la administración de la red LAN y la segmentación del ancho de banda.

3.3.1 Método de la medición

Se utilizó la base de datos de los clientes que cuenta el proveedor de Internet Optical Network, asociado al ancho de banda, circuito y sede de cada empresa. De esta forma se recomienda el promedio de ancho de banda a contratar para la Universidad Nacional José María Arguedas.

3.4 Forma de determinar el ancho de banda a contratar.

Se procedió a recolectar la información del ancho de banda contratado y la cantidad de matriculados de un grupo de Universidades del Perú, posteriormente recomendar el ancho de banda adecuado a contratar por la Universidad Nacional José María Arguedas.

3.4.1 Entidad y ancho de banda de Internet contratado.

COD. CIRCUIT	COD. CLIENTE	CIRCUITO	CLIENTE	Local	ANCHO BANDA	TIPO SERVICIO
1104	677	Gonzales 285 Int	UNIVERSIDAD NAC. FEDERICO VILLARREAL -UNFV	Local Central	300 Mbps	Internet
3496	1645	Andes - Int- Administracion	UNIVERSIDAD ANTONIO RUIZ DE MONTOYA	Local Central	170 Mbps	Internet
3497	1645	Andes - Int - Estudiantes	UNIVERSIDAD ANTONIO RUIZ DE MONTOYA	Local Remoto	10 Mbps	Internet
4445	281	Javier Prado Oeste - Int	UNIVERSIDAD NACIONAL DE INGENIERIA UNI	Local Remoto	8 Mbps	Internet
6210	1383	Gonzales F.O.	UNIVERSIDAD CATOLICA SEDES SAPIENTIAE	Local Central	40 Mbps	Internet
6321	1442	Panamericana Sur - INT	UNIVERSIDAD AUTONOMA DEL PERU S.A.C.	Local Central	400 Mbps	Internet
7264	625	San Felipe - INT 1	UNIVERSIDAD ALAS PERUANAS S.A.	Local Central	150 Mbps	Internet
9665	2704	UNIVERSITARIA - INT SECUNDARIO	ASOCIACION CIVIL UNIVERSIDAD DE CIENCIAS Y HUMANIDADES UCH	Local Remoto	25 Mbps	Internet
10411	2704	UNIVERSITARIA 5175 - INT - 25 Mbps	ASOCIACION CIVIL UNIVERSIDAD DE CIENCIAS Y HUMANIDADES UCH	Local Remoto	25 Mbps	Internet
11893	3697	MARTIR OLAYA 162 1 - INT - 100 Mbps - Primario	UNIVERSIDAD DE PIURA	Local Central	100 Mbps	Internet
13692	2002	28 DE JULIO 1056 - INT - 400 Mbps	UNIVERSIDAD PRIVADA TELESUP S.A.C.	Local Central	400 Mbps	Internet
13938	3697	MARTIR OLAYA 162 1 - INT - 100 Mbps - Primario	UNIVERSIDAD DE PIURA	Local Central	100 Mbps	Internet
16301	4477	INDUSTRIAL 3701 - INT - 60 Mbps	UNIVERSIDAD SAN ANDRES S.A.C. - USAN S.A.C.	Local Central	60 Mbps	Internet

Tabla 3: Relación entre la entidad y el ancho de banda contratado
Fuente: Base de Datos- Optical Networks ISP - 2018

3.4.2 Entidad y cantidad de matriculados

DEPARTAMENTO	DESCRIPCIÓN	2013	2014	2015
AMAZONAS	UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS	6,133	3925	3940
ANCASH	UNIVERSIDAD NACIONAL DEL SANTA	3,209	3469	3578
ANCASH	UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO	13,056	6272	6459
ANCASH	UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE	52,881	44981	46893
ANCASH	UNIVERSIDAD SAN PEDRO	23,207	22593	21176
APURIMAC	UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS	1,403	1491	1430
APURIMAC	UNIVERSIDAD TECNOLÓGICA DE LOS ANDES	17,503	5088	4596
AREQUIPA	UNIVERSIDAD NACIONAL DE SAN AGUSTÍN	27,647	26322	26216
AREQUIPA	UNIVERSIDAD AUTONOMA SAN FRANCISCO	1,018	759	689
AREQUIPA	UNIVERSIDAD CATÓLICA DE SANTA MARÍA	13,391	14198	13673
AREQUIPA	UNIVERSIDAD CATÓLICA SAN PABLO	6,167	6648	7359
AREQUIPA	UNIVERSIDAD CIENCIAS DE LA SALUD	76	223	227
AREQUIPA	UNIVERSIDAD LA SALLE	628	675	934
AREQUIPA	UNIVERSIDAD PRIVADA AUTÓNOMA DEL SUR	146	257	369
AYACUCHO	UNIVERSIDAD DE AYACUCHO FEDERICO FROEBEL	181	308	349
CAJAMARCA	UNIVERSIDAD NACIONAL DE CAJAMARCA	15,022	8119	9409
CAJAMARCA	UNIVERSIDAD NACIONAL DE JAÉN	400	1107	1462
CAJAMARCA	UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO	4,076	3621	4464
CALLAO	UNIVERSIDAD NACIONAL DEL CALLAO	13,165	15256	15805
CUSCO	UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO	17,683	20610	20710
CUSCO	UNIVERSIDAD GLOBAL DEL CUSCO	214	310	330
CUSCO	UNIVERSIDAD ANDINA DEL CUSCO	16,097	15407	16205
HUANCAVELICA	UNIVERSIDAD NACIONAL DE HUANCAVELICA	5,527	5434	4909
HUANUCO	UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA	3,069	3206	3138
HUANUCO	UNIVERSIDAD DE HUANUCO	9,917	10365	9622
JUNIN	UNIVERSIDAD NACIONAL DEL CENTRO DEL PERÚ	10,615	13658	12983
JUNIN	UNIVERSIDAD CONTINENTAL	10,429	18488	18370
JUNIN	UNIVERSIDAD PERUANA DEL CENTRO	61	704	943
JUNIN	UNIVERSIDAD PERUANA LOS ANDES	29,876	35403	37613
JUNIN	UNIVERSIDAD PRIVADA DE HUANCAYO FRANKLIN ROOSEVELT	1,101	3200	3038
LA LIBERTAD	UNIVERSIDAD NACIONAL DE TRUJILLO	12,932	13527	13507
LA LIBERTAD	UNIVERSIDAD CATÓLICA DE TRUJILLO BENEDICTO XVI	571	1662	1960

Tabla 4: Relación de entidad y cantidad de matriculados por periodo
Fuente: (SUNEDU) – Oficina de Planeamiento y Presupuesto.

3.5 Forma de recomendar el equipo y modelo a utilizar.

Se procedió a recolectar la información de los equipos de seguridad Firewall UTM que tienen las instituciones del estado y empresas en Lima Metropolitana, posteriormente recomendar el modelo y equipo adecuado a contratar y utilizar por la Universidad Nacional José María Arguedas.

Cliente	Marca	Modelo	Estado2
Unidad Ejecutora 004 - Fondo De Cooperacion Para El Desarrollo Social	Fortinet	Fortigate 100D	Productivo
Municipalidad Distrital De San Martin De Porres	Fortinet	Fortigate 100D	Productivo
Viaconsumo S.A.C	Fortinet	Fortigate 100D	Productivo
Municipalidad Distrital De San Martin De Porres	Fortinet	Fortigate 100D	Productivo
Motores Diésel Andinos S.A	Fortinet	Fortigate 100D	Productivo
Viaconsumo S.A.C	Fortinet	Fortigate 100D	Productivo
Class Complements Sac	Fortinet	Fortigate 100D	Productivo
Grupo Verona S.A.C.	Fortinet	Fortigate 100D	Productivo
Motores Diesel Andinos S.A	Fortinet	Fortigate 100D	Productivo
Municipalidad Distrital De San Martin De Porres	Fortinet	Fortigate 100D	Productivo
Energigas S.A.C.	Fortinet	Fortigate 100D	Productivo
Industrial Controls S.A.C.	Fortinet	Fortigate 100E	Productivo
Hospital Nac Docente Madre Niã?Á?O San Bartolome	Fortinet	Fortigate 200B	Productivo
Mayo Publicidad S.A	Fortinet	Fortigate 200D	Productivo
Instituto Nacional De Oftalmologia	Fortinet	Fortigate 200D	Productivo
Kaercher Peru S.A.	Fortinet	Fortigate 200E	Productivo
Cep Parroq Santisimo Nombre De Jesus	Fortinet	Fortigate 300C	Productivo
Unidad Ejecutora 004 - Fondo De Cooperacion Para El Desarrollo Social	Fortinet	Fortigate 300C	Productivo
Unidad Ejecutora 004 - Fondo De Cooperacion Para El Desarrollo Social	Fortinet	Fortigate 300C	Productivo
Esc Nac Sup Folklore Jose Maria Arguedas	Fortinet	Fortigate 500D	Productivo
Municipalidad Distrital De San Martin De Porres	Fortinet	Fortigate 500D	Productivo
Maquinarias S.A.	Fortinet	Fortigate 500D	Productivo
Organismo Supervisor De La Inversion En Energia Y Minería	Fortinet	Fortigate 500D	Productivo
Hospital Nac Docente Madre Niã?Á?O San Bartolome	Fortinet	Fortigate 500D	Productivo
Municipalidad Distrital De San Martin De Porres	Fortinet	Fortigate 500D	Productivo

Tabla 5: Instituciones y empresa con equipos Fortigate en el Peru
Fuente: Base de Datos- Optical Networks ISP - 2018

CAPITULO 4: RESULTADOS Y DISCUSIÓN

4.1 Presentación general de resultados

Se detalla la información de las pruebas de comunicación de red realizadas a nivel de LAN y WAN en la Universidad Nacional José María Arguedas.

4.1.1 Pruebas del servicio a nivel LAN

Se instaló una central telefónica Yeastar S20 VoIP PBX y un teléfono IP Yeastar T21 en el ambiente donde se encuentran los equipos de comunicaciones del local central de la UNAJMA.

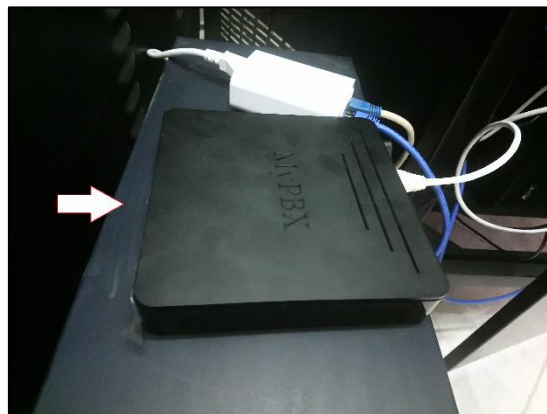


Gráfico 10: Ubicación de Central Yeastar instalada.
Fuente: Elaboración Propia

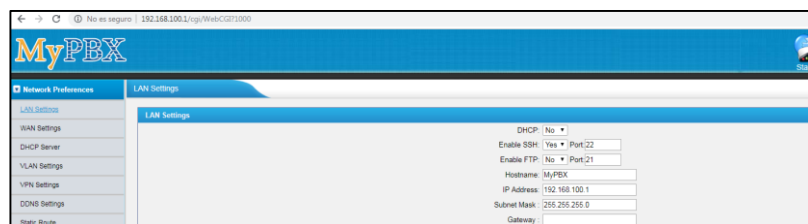
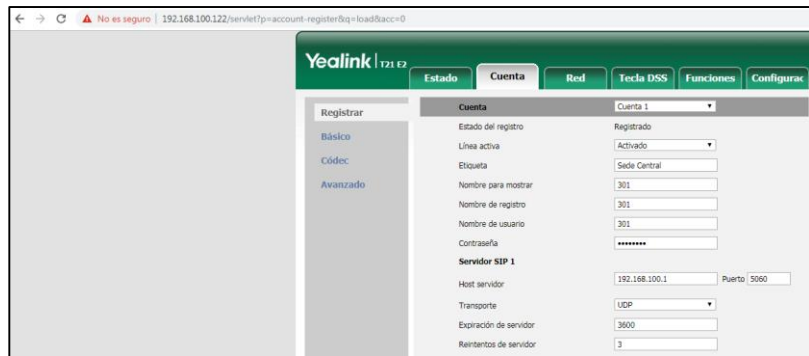
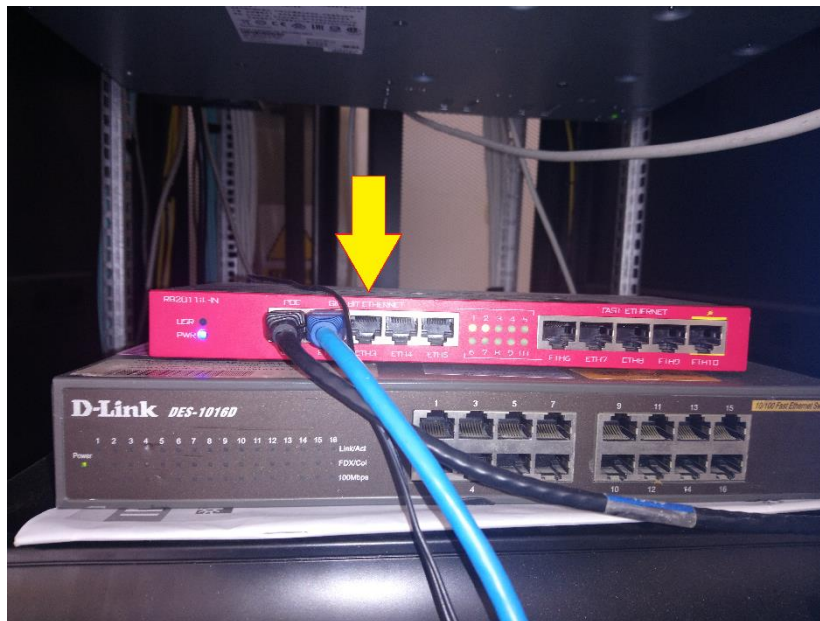


Gráfico 11: Configuración de la Central Yeastar.
Fuente: Elaboración Propia



*Gráfico 12: Configuración del Telefono IP Yeastar.
Fuente: Elaboración Propia*

Se instaló un teléfono IP Yeastar T21 en el ambiente donde se encuentran los equipos de comunicaciones del local de Sistemas de la UNAJMA, y se utilizó el puerto 3 disponible del equipo Mikrotik RB2011 y se configuro el segmento 192.168.101.0/24 para la nueva red de telefonía.



*Gráfico 13: Puertos disponibles en router Mikrotik - Sistemas
Fuente: Elaboración Propia*



Gráfico 14: Puerto utilizado para conexión de Teléfono IP
Fuente: Elaboración Propia

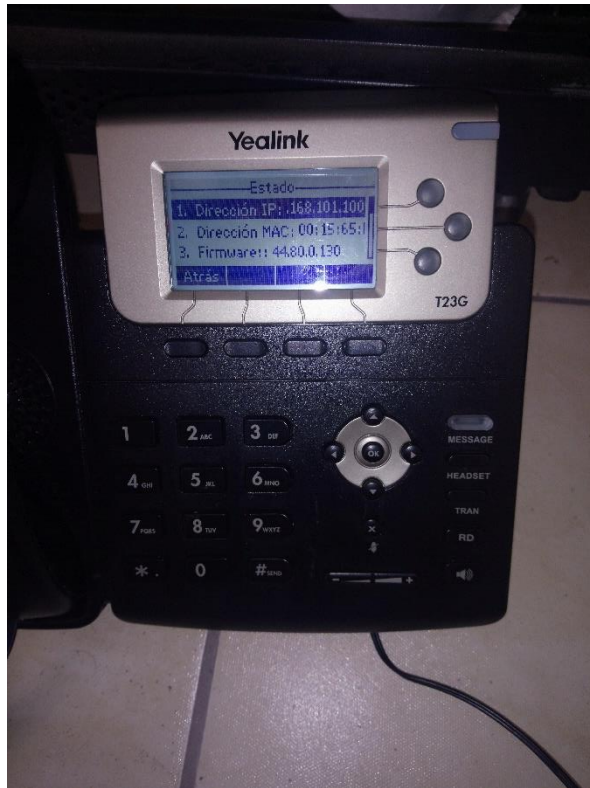


Gráfico 15: Teléfono IP instalado y configurado.
Fuente: Elaboración Propia

The screenshot shows the MyPBX web interface with the 'Routing Table' section highlighted. The table contains the following data:

Destination	Subnet Mask	Gateway	Metric
0.0.0.0	0.0.0.0	192.168.100.254	0
20.20.20.0	255.255.255.0	0.0.0.0	0
192.168.100.0	255.255.255.0	0.0.0.0	0
224.0.0.0	224.0.0.0	0.0.0.0	0

Gráfico 16: Configuración de enrutamiento en central telefónica.
Fuente: Elaboración Propia

The screenshot shows the MyPBX web interface with the 'Extension Status' section highlighted. The table contains the following data:

Extension	Status
300(SIP)	Registered
301(SIP)	Registered

Gráfico 17: Anexos registrados en PBX central telefónica.
Fuente: Elaboración Propia

```

192.168.100.1 - PuTTY
== Manager 'admin' logged on from 127.0.0.1
== Manager 'admin' logged off from 127.0.0.1

MyPBX*CLI> exit
Executing last minute cleanups
root@MyPBX:~# ping 192.168.101.100
PING 192.168.101.100 (192.168.101.100): 56 data bytes
64 bytes from 192.168.101.100: seq=0 ttl=62 time=4.556 ms
64 bytes from 192.168.101.100: seq=1 ttl=62 time=5.013 ms
64 bytes from 192.168.101.100: seq=2 ttl=62 time=5.948 ms
64 bytes from 192.168.101.100: seq=3 ttl=62 time=3.920 ms
64 bytes from 192.168.101.100: seq=4 ttl=62 time=10.305 ms
64 bytes from 192.168.101.100: seq=5 ttl=62 time=4.770 ms
64 bytes from 192.168.101.100: seq=6 ttl=62 time=4.791 ms
64 bytes from 192.168.101.100: seq=7 ttl=62 time=4.246 ms
64 bytes from 192.168.101.100: seq=8 ttl=62 time=7.755 ms
64 bytes from 192.168.101.100: seq=9 ttl=62 time=7.963 ms
64 bytes from 192.168.101.100: seq=10 ttl=62 time=3.942 ms
64 bytes from 192.168.101.100: seq=11 ttl=62 time=3.833 ms
64 bytes from 192.168.101.100: seq=12 ttl=62 time=5.957 ms
64 bytes from 192.168.101.100: seq=13 ttl=62 time=8.239 ms
64 bytes from 192.168.101.100: seq=14 ttl=62 time=4.408 ms
64 bytes from 192.168.101.100: seq=15 ttl=62 time=4.258 ms
64 bytes from 192.168.101.100: seq=16 ttl=62 time=3.960 ms
64 bytes from 192.168.101.100: seq=17 ttl=62 time=4.175 ms
^C
--- 192.168.101.100 ping statistics ---
18 packets transmitted, 18 packets received, 0% packet loss
round-trip min/avg/max = 3.833/5.446/10.305 ms

```

Gráfico 18: Pruebas ICMP hacia teléfono IP instalado en local remoto.
Fuente: Elaboración Propia

4.1.2 Resultados obtenidos de las pruebas a nivel LAN

```
root@MyPBX:~# ping 192.168.100.122
PING 192.168.100.122 (192.168.100.122): 56 data bytes
64 bytes from 192.168.100.122: seq=0 ttl=64 time=0.832 ms
64 bytes from 192.168.100.122: seq=1 ttl=64 time=0.599 ms
64 bytes from 192.168.100.122: seq=2 ttl=64 time=0.708 ms
64 bytes from 192.168.100.122: seq=3 ttl=64 time=0.549 ms
64 bytes from 192.168.100.122: seq=4 ttl=64 time=0.638 ms
64 bytes from 192.168.100.122: seq=5 ttl=64 time=0.590 ms
64 bytes from 192.168.100.122: seq=6 ttl=64 time=0.557 ms
64 bytes from 192.168.100.122: seq=7 ttl=64 time=0.602 ms
64 bytes from 192.168.100.122: seq=8 ttl=64 time=0.647 ms
64 bytes from 192.168.100.122: seq=9 ttl=64 time=0.518 ms
64 bytes from 192.168.100.122: seq=10 ttl=64 time=0.609 ms
64 bytes from 192.168.100.122: seq=11 ttl=64 time=0.648 ms
64 bytes from 192.168.100.122: seq=12 ttl=64 time=4.755 ms
^C
--- 192.168.100.122 ping statistics ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 0.518/0.942/4.755 ms
root@MyPBX:~#
```

Gráfico 19: Pruebas ICMP hacia teléfono IP instalado en local central

Fuente: Elaboración Propia

```
C:\Windows\system32\cmd.exe - ping 10.0.1.112 -t
Respuesta desde 10.0.1.112: bytes=32 tiempo=3ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=483ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1004ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=14ms TTL=64
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 10.0.1.112: bytes=32 tiempo=8ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=28ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=9ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1322ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=261ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=201ms TTL=64
Tiempo de espera agotado para esta solicitud.
Respuesta desde 10.0.1.112: bytes=32 tiempo=2209ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 10.0.1.112: bytes=32 tiempo=287ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=6ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=3301ms TTL=64
Tiempo de espera agotado para esta solicitud.
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=5ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=5ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=5ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=1ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=5ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=8ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=33ms TTL=64
Respuesta desde 10.0.1.112: bytes=32 tiempo=4ms TTL=64
```

Gráfico 20: Pruebas ICMP hacia gateway de router en local central

Fuente: Elaboración Propia

```

root@MyPBX:~# ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1): 56 data bytes
64 bytes from 192.168.101.1: seq=0 ttl=63 time=7.853 ms
64 bytes from 192.168.101.1: seq=1 ttl=63 time=4.573 ms
64 bytes from 192.168.101.1: seq=2 ttl=63 time=6.008 ms
64 bytes from 192.168.101.1: seq=3 ttl=63 time=4.533 ms
64 bytes from 192.168.101.1: seq=4 ttl=63 time=3.783 ms
64 bytes from 192.168.101.1: seq=5 ttl=63 time=13.281 ms
64 bytes from 192.168.101.1: seq=6 ttl=63 time=3.850 ms
64 bytes from 192.168.101.1: seq=7 ttl=63 time=4.015 ms
64 bytes from 192.168.101.1: seq=8 ttl=63 time=4.632 ms
64 bytes from 192.168.101.1: seq=9 ttl=63 time=4.268 ms
64 bytes from 192.168.101.1: seq=10 ttl=63 time=4.322 ms
64 bytes from 192.168.101.1: seq=11 ttl=63 time=6.716 ms
64 bytes from 192.168.101.1: seq=12 ttl=63 time=6.130 ms
64 bytes from 192.168.101.1: seq=13 ttl=63 time=6.326 ms
64 bytes from 192.168.101.1: seq=14 ttl=63 time=5.219 ms
64 bytes from 192.168.101.1: seq=15 ttl=63 time=7.425 ms
64 bytes from 192.168.101.1: seq=16 ttl=63 time=4.416 ms
64 bytes from 192.168.101.1: seq=17 ttl=63 time=5.461 ms
^C
--- 192.168.101.1 ping statistics ---
18 packets transmitted, 18 packets received, 0% packet loss
round-trip min/avg/max = 3.783/5.711/13.281 ms
root@MyPBX:~#

```

Gráfico 21: Pruebas ICMP hacia Gateway de router en local remoto
Fuente: Elaboración Propia

```

sent=60 received=60 packet-loss=0% min-rtt=3ms avg-rtt=5ms max-rtt=15ms

```

SEQ	HOST	SIZE	TTL	TIME	STATUS
60	10.0.1.112	56	64	5ms	
61	10.0.1.112	56	64	4ms	
62	10.0.1.112	56	64	4ms	
63	10.0.1.112	56	64	4ms	
64	10.0.1.112	56	64	3ms	
65	10.0.1.112	56	64	4ms	
66	10.0.1.112	56	64	4ms	
67	10.0.1.112	56	64	4ms	
68	10.0.1.112	56	64	9ms	
69	10.0.1.112	56	64	5ms	
70	10.0.1.112	56	64	3ms	
71	10.0.1.112	56	64	4ms	
72	10.0.1.112	56	64	4ms	
73	10.0.1.112	56	64	6ms	
74	10.0.1.112	56	64	7ms	
75	10.0.1.112	56	64	7ms	
76	10.0.1.112	56	64	7ms	
77	10.0.1.112	56	64	4ms	
78	10.0.1.112	56	64	6ms	
79	10.0.1.112	56	64	4ms	

```

sent=80 received=80 packet-loss=0% min-rtt=3ms avg-rtt=5ms max-rtt=15ms

```

Gráfico 22: Pruebas ICMP hacia IP WAN de router en local remoto
Fuente: Elaboración Propia

4.1.3 Conclusiones de las pruebas a nivel LAN

Luego de proceder a realizar las pruebas y verificaciones de los tiempos de respuesta hacia cada uno de los equipos y validar que estos valores se encuentran en el rango de los parámetros correctos, se procedió a realizar pruebas de llamadas con los anexos telefónicos instalados en los locales (central y remoto).

Se verificó que las llamadas se efectúan de manera correcta, sin interferencias ni entrecortes de voz, de esta manera se evidencia que los valores de latencia y tiempos de respuesta entre los equipos se encuentran dentro de los parámetros aceptables para para la comunicación de voz.

Del mismo modo se valida que los valores de tiempo de respuesta se encuentran dentro del rango aceptado para la para la comunicación video y datos.

Se verifico que se tiene perdida de paquetes al router Mikrotik instalado en el local de la Facultad de Sistemas, y por consecuencia de esto se pierde la comunicación con la sede central. (Perdida de paquetes 7 de cada 100).

Se verificó el tiempo de respuesta hacia el router de la Facultad de Sistemas. Cuando es continua no se tiene perdida de paquetes, las llamadas se efectúan de manera correcta, sin interferencias ni entrecortes de voz.

Se tomó como referencia realizar las pruebas de voz, por ser este un tipo de tráfico más sensible a la intermitencia y cambios de red.

4.1.4 Pruebas del servicio a nivel WAN

Se procedió a realizar las pruebas de latencia y tiempos de respuesta hacia Internet desde el balanceador Mikrotik obteniéndose los siguientes resultados.



Gráfico 23: Test de Velocidad del servicio dedicado Movistar

Fuente: Elaboración Propia

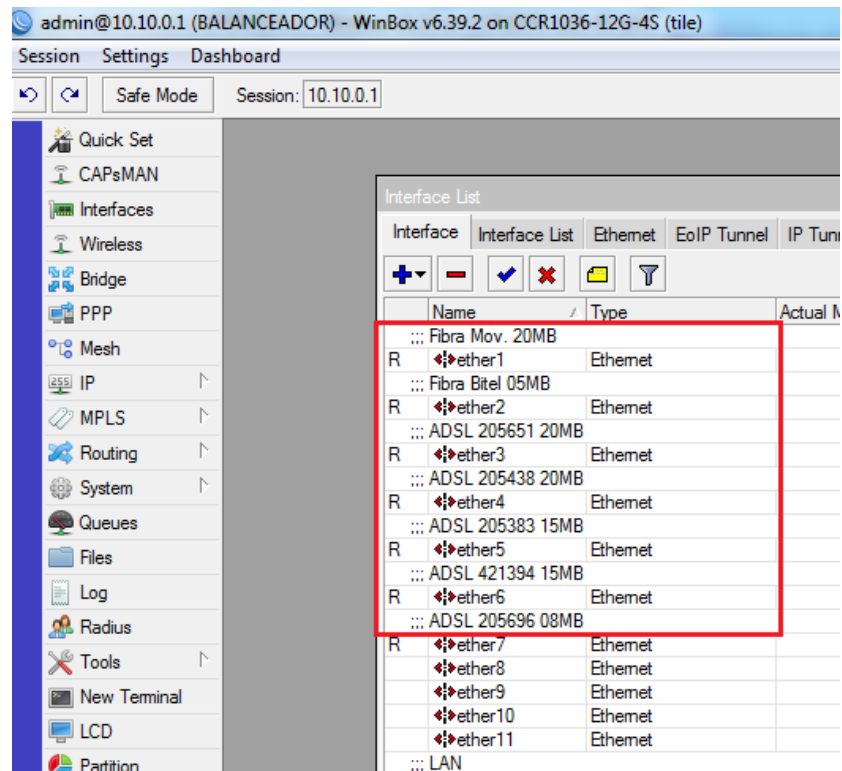


Gráfico 24: Puertos en router y los servicios de Internet contratados
Fuente: Elaboración Propia

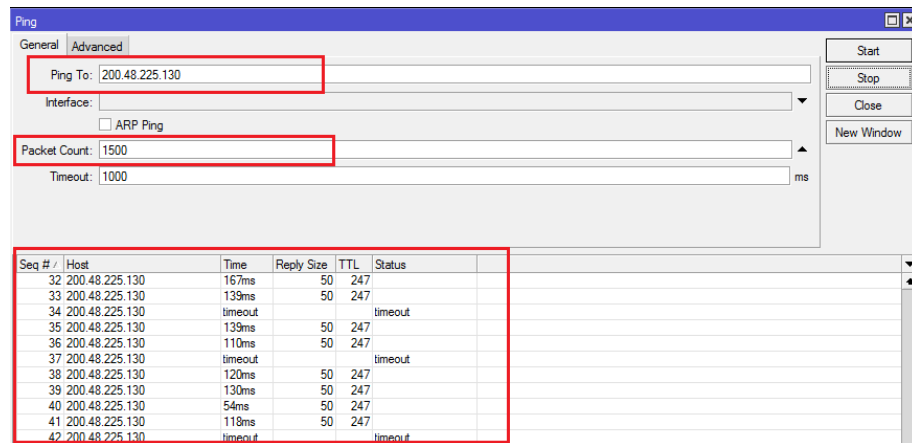


Gráfico 25: Pruebas de ICMP hacia los DNS de Telefónica
Fuente: Elaboración Propia

Seq # /	Host	Time	Reply Size	TTL	Status
32	200.48.225.130	167ms	50	247	
33	200.48.225.130	139ms	50	247	
34	200.48.225.130	timeout			timeout
35	200.48.225.130	139ms	50	247	
36	200.48.225.130	110ms	50	247	
37	200.48.225.130	timeout			timeout
38	200.48.225.130	120ms	50	247	
39	200.48.225.130	130ms	50	247	
40	200.48.225.130	54ms	50	247	
41	200.48.225.130	118ms	50	247	
42	200.48.225.130	timeout			timeout
43	200.48.225.130	158ms	50	247	
44	200.48.225.130	37ms	50	247	
45	200.48.225.130	105ms	50	247	
46	200.48.225.130	timeout			timeout
47	200.48.225.130	138ms	50	247	
48	200.48.225.130	133ms	50	247	
49	200.48.225.130	timeout			timeout
50	200.48.225.130	36ms	50	247	
51	200.48.225.130	82ms	50	247	
52	200.48.225.130	147ms	50	247	
53	200.48.225.130	149ms	50	247	
54	200.48.225.130	120ms	50	247	
55	200.48.225.130	138ms	50	247	
56	200.48.225.130	127ms	50	247	
57	200.48.225.130	138ms	50	247	
58	200.48.225.130	147ms	50	247	
59	200.48.225.130	137ms	50	247	
60	200.48.225.130	144ms	50	247	
61	200.48.225.130	60ms	50	247	
62	200.48.225.130	161ms	50	247	
63	200.48.225.130	132ms	50	247	

64 items | 51 of 64 packets received | 20% packet loss | Min: 36 ms | Avg: 122 ms | Max: 177 ms

Gráfico 26: Valores de tiempo de respuesta hacia los DNS de Telefónica
Fuente: Elaboración Propia

Ping (Running)

General | Advanced

Ping To: 8.8.8.8

Interface:

ARP Ping

Packet Count: 1500

Timeout: 1000 ms

Seq # /	Host	Time	Reply Size	TTL	Status
17	8.8.8.8	202ms	50	122	
18	8.8.8.8	204ms	50	122	
19	8.8.8.8	163ms	50	122	
20	8.8.8.8	100ms	50	122	
21	8.8.8.8	101ms	50	122	
22	8.8.8.8	101ms	50	122	
23	8.8.8.8	101ms	50	122	
24	8.8.8.8	101ms	50	122	
25	8.8.8.8	101ms	50	122	
26	8.8.8.8	101ms	50	122	
27	8.8.8.8	108ms	50	122	
28	8.8.8.8	101ms	50	122	
29	8.8.8.8	101ms	50	122	
30	8.8.8.8	102ms	50	122	
31	8.8.8.8	101ms	50	122	
32	8.8.8.8	233ms	50	122	
33	8.8.8.8	225ms	50	122	
34	8.8.8.8	timeout			timeout
35	8.8.8.8	timeout			timeout
36	8.8.8.8	timeout			timeout
37	8.8.8.8	timeout			timeout
38	8.8.8.8	218ms	50	122	
39	8.8.8.8	201ms	50	122	
40	8.8.8.8	215ms	50	122	
41	8.8.8.8	101ms	50	122	

42 items | 38 of 42 packets received | 9% packet loss | Min: 100 ms | Avg: 164 ms | Max: 241 ms

Gráfico 27: Pruebas ICMP hacia los DNS de Google
Fuente: Elaboración Propia

```

Simbolo del sistema
Traza a la dirección google-public-dns-a.google.com [8.8.8.8]
sobre un máximo de 30 saltos:
 1 <1 ms <1 ms <1 ms 192.168.44.1
 2 * * * Tiempo de espera agotado para esta solicitud.
 3 21 ms 21 ms 21 ms 192.168.33.13
 4 20 ms 21 ms 21 ms 10.112.197.65
 5 31 ms 35 ms 25 ms 10.112.0.177
 6 35 ms 39 ms 30 ms 10.112.128.222
 7 68 ms 65 ms 61 ms 5.53.1.213
 8 102 ms 101 ms 102 ms 94.142.99.109
 9 102 ms 102 ms 101 ms google-ae15-8-grtr4br4.net.telefonicaglobalsolu
tions.com [215.184.112.171]
10 101 ms 102 ms 102 ms 108.170.249.17
11 102 ms 102 ms 102 ms 108.170.228.27
12 101 ms 102 ms 102 ms google-public-dns-a.google.com [8.8.8.8]

Traza completa.
C:\Users\SADM-OSI-N-02>13
"13" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
C:\Users\SADM-OSI-N-02>_

```

Gráfico 28: Pruebas de tracer hacia los DNS de google
Fuente: Elaboración Propia

Fwd: POOL DE IPS CD 170957 EMPRESA UNIV NACIONAL JOSE MARIA ARGUEDAS Recibidos x

Oficina de Sistemas de Informacion
para mí ▾

🌐 inglés ▾ > español ▾ [Traducir mensaje](#)

----- Forwarded message -----
 From: Service Desk Empresarial <sdempresas@cc.atentoperu.pe>
 Date: sáb., 10 nov. 2018 a las 13:21
 Subject: POOL DE IPS CD 170957 EMPRESA UNIV NACIONAL JOSE MARIA ARGUEDAS
 To: osi@unajma.edu.pe <osi@unajma.edu.pe>

Estimado cliente,

Se envía la información solicitada del enlace

Address: 181.65.139.241
 Netmask: 255.255.255.248 = 29
 Network: [181.65.139.240/29](#)
 HostMin: 181.65.139.242
 HostMax: 181.65.139.246
 Broadcast: 181.65.139.247
 Hosts/Net: 6

Gráfico 29: Datos de pool de IP publica contratado con Movistar
Fuente: Elaboración Propia

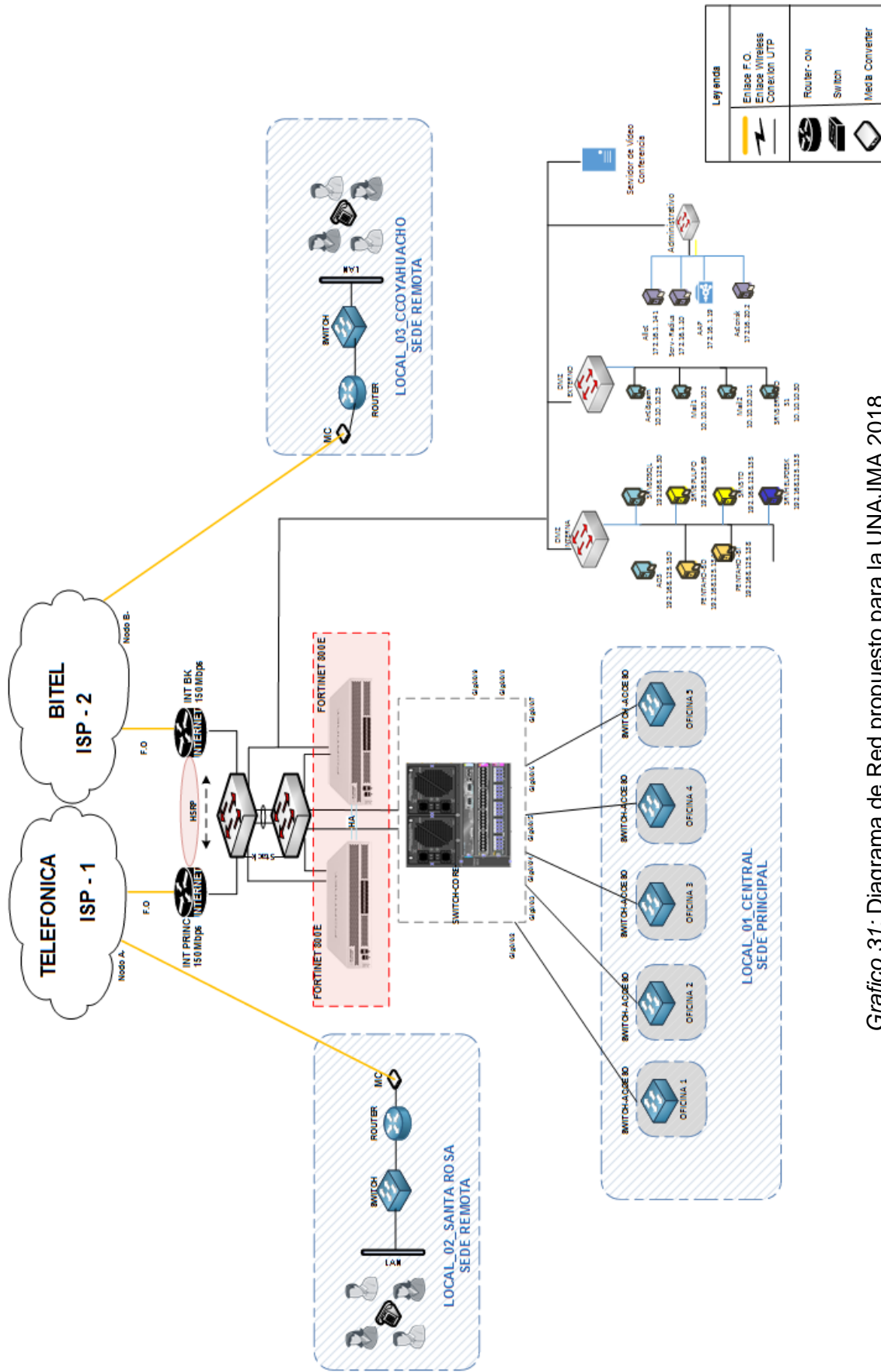
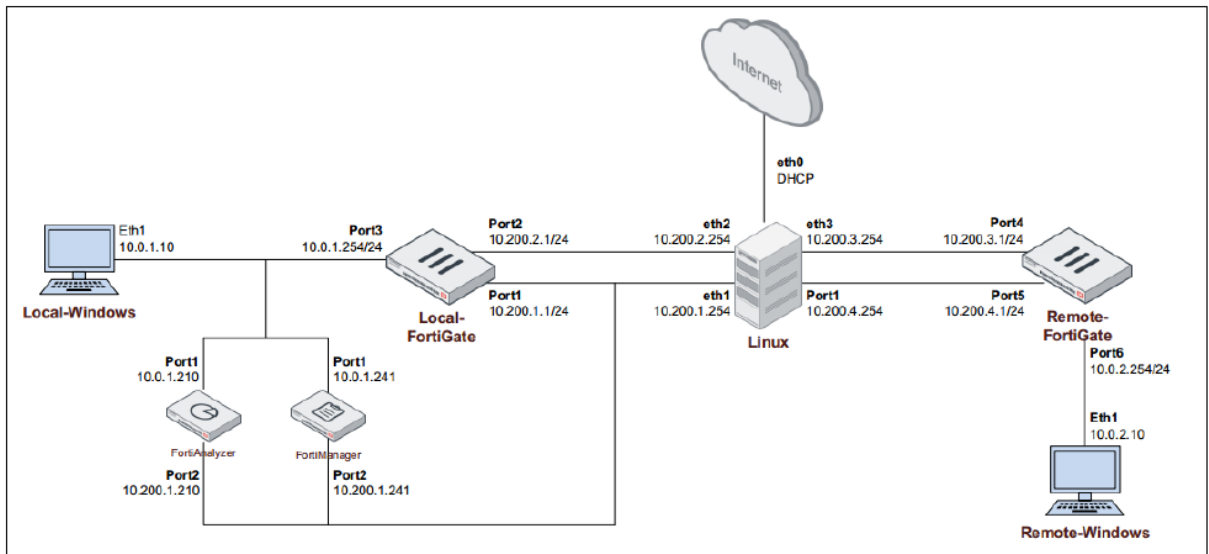


Grafico 31: Diagrama de Red propuesto para la UNAUMA 2018

Fuente: Elaboración Propia

4.1.6 Diagrama para las pruebas de funcionamiento

Se muestra el diagrama utilizado y necesario para la implementación y pruebas de funcionamiento de las políticas de seguridad UTM utilizando equipos Fortigate.



TOPOLOGIA DE RED

Gráfico 32: Topología diseñada para pruebas de funcionamiento
Fuente: Elaboración Propia

4.1.7 Máquinas virtuales utilizadas

Local - Windows	01
Remote Windows	01
Local- Fortigate	01
Remoto - Fortigate	01
Linux	01
Fortianalyzer	01
Fortimanager	01

Por la complejidad de una red simulada y el alcance de interfaces que se maneja mediante esta, se utilizó el modo de LAN Segments para lograr la comunicación de las máquinas virtuales implementadas.

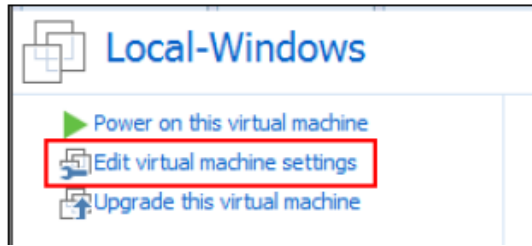


Gráfico 33: Fase 1 - Editar la configuración de las máquinas virtuales
Fuente: Elaboración Propia

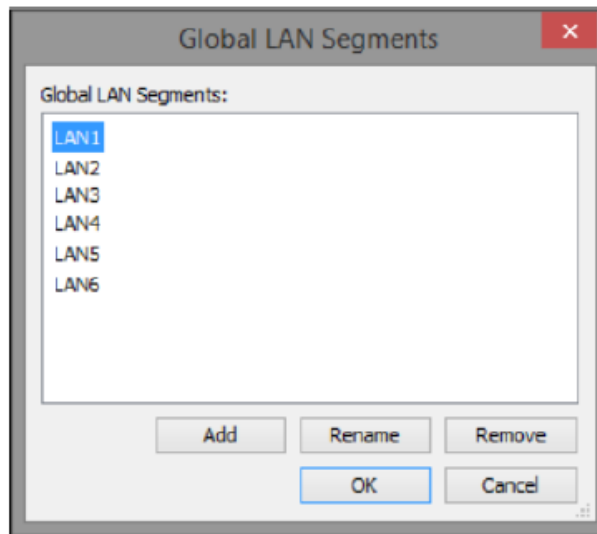


Gráfico 34: Fase 2 - Editar la configuración global y Lan Segments
Fuente: Elaboración Propia

En esta fase se debe de tener bastante consideración de manera que la conexión de las interfaces de cada máquina virtual sea como corresponde, logrando la comunicación de estas.

LOCAL-FORTIGATE & REMOTE-FORTIGATE	
Network Adapter	Lan Segment
1	LAN1
2	LAN2
3	LAN3
4	LAN4
5	LAN5
6	LAN6

LOCAL-WINDOWS	
Network Adapter	Lan Segment
1	LAN3
2	HOST-ONLY

REMOTE-WINDOWS	
Network Adapter	Lan Segment
1	LAN6
2	HOST-ONLY

LINUX	
Network Adapter	Lan Segment
1	NAT
2	LAN1
3	LAN2
4	LAN4
5	LAN5

FORTIMANAGER	
Network Adapter	Lan Segment
2	LAN3
3	LAN1

Gráfico 35: Fase 3 - Parámetros que contendrá cada VM
Fuente: Elaboración Propia

4.1.8 Modo de configuración de los segmentos de red

```
eth0 = LAN0 = Management network
eth1 = LAN1 = 10.200.1.254/24
eth2 = LAN2 = 10.200.2.254/24
eth3 = LAN4 = 10.200.3.254/24
eth4 = LAN5 = 10.200.4.254/24
```

4.1.9 Configuración de la VM con el Fortigate remoto

```
config system interface
edit port1
    set ip 10.200.1.1 255.255.255.0
    set allowaccess http
next
edit port3
    set ip 10.0.1.254 255.255.255.0
    set allowaccess http
next
end
config router static
edit 1
    set gateway 10.200.1.254
    set device port1
next
end
config system interface
edit port4
    set ip 10.200.3.1 255.255.255.0
    set allowaccess ping https ssh http fgfm
next
end
config router static
edit 1
    set device port4
    set gateway 10.200.3.254
next
end
config firewall policy
edit 1
    set srcintf port3
    set dstintf port1
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
    set nat enable
next
end
```

4.1.10 Configuración de la VM en el Windows remoto

Configuración de la red (LAN6)

Dirección IP: 10.0.2.10

Mascara: 255.255.255.0

Default Gateway: 10.0.2.254

DNS: 10.0.2.254

4.1.11 Configuración de la VM en el FortiAnalyzer

```
config system interface
  edit port1
    set ip 10.0.1.210 255.255.255.0
    set allowaccess http https ssh ping telnet
  next
end
```

4.2 Enrutamiento

4.2.1 Configuración del enrutamiento en un equipo Fortigate

El proceso para crear un enrutamiento es más sencillo, ya que Fortigate nos proporciona una interfaz gráfica, cabe señalar que es necesario tener consideración es y definir el puerto correcto asociado a LAN y WAN.

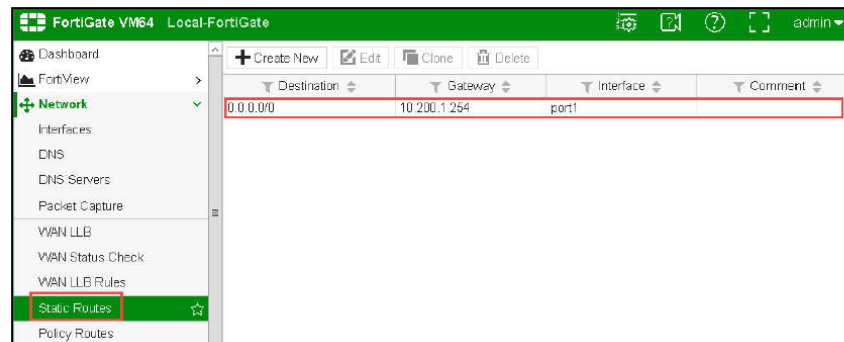


Gráfico 36: Modo de crear un enrutamiento estático
Fuente: Elaboración Propia

4.2.2 Verificación de los parámetros de las rutas

La ruta por defecto de salida a internet mantendrá los siguientes parámetros, estos pueden ser modificados de acuerdo al dimensionamiento de la red, se puede modificar los valores de la distancia administrativa y la prioridad según se requiera.

The screenshot shows the 'Edit Static Route' configuration interface. The 'Destination' field is set to 'Subnet' with the value '0.0.0.0/0.0.0.0'. The 'Device' is 'port1' and the 'Gateway' is '10.200.1.254'. The 'Administrative Distance' is '10'. The 'Status' is 'Enabled'. The 'Priority' is '0'. The 'Advanced Options' section is expanded, showing the 'Priority' field set to '0'.

Gráfico 37: Parámetros de una ruta estática en el equipo FG
Fuente: Elaboración Propia

Se realizó las pruebas y verificaciones añadiendo una ruta secundaria por defecto, de manera que al cambiar la prioridad por un valor distinto se pueda verificar el comportamiento de la tabla de enrutamiento del equipo Fortigate.

Field	Value
Destination	Subnet 0.0.0.0/0.0.0.0
Device	port2
Gateway	10.200.2.254
Administrative Distance	20

4.2.3 Verificaciones y monitoreo del enrutamiento por CLI

A partir de añadir una segunda ruta por defecto, se puede verificar que el equipo considerara valida la ruta que tenga una distancia administrativa menor, pero adicional a esto se puede cambiar el valor de la prioridad si se tiene el caso que la distancia administrativa es igual.

```

Student # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
> - selected route, * - FIB route, p - stale info

S 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
C *> 10.0.1.0/24 is directly connected, port3
C *> 10.200.1.0/24 is directly connected, port1
C *> 10.200.2.0/24 is directly connected, port2

```

Gráfico 38: Muestra la tabla de enrutamiento con 2 rutas por defecto
Fuente: Elaboración Propia

4.3 Link Monitor

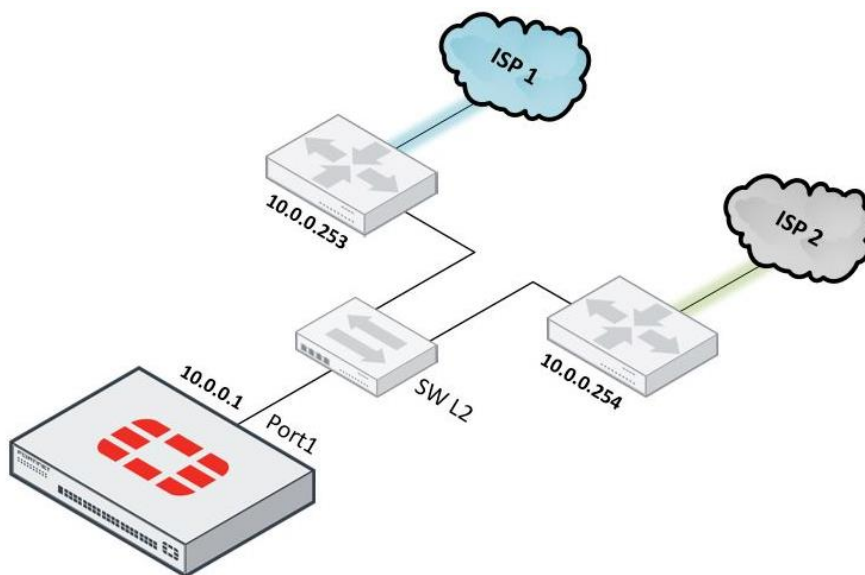


Gráfico 39: Diagrama de funcionamiento de Link monitor
Fuente: Elaboración Propia

4.3.1 Configuración de Link Monitor en el equipo Fortigate

```
config system link-monitor
  edit port1-monitor
    set srcintf port1
    set server 4.2.2.1
    set gateway-ip 10.200.1.254
    set protocol ping
    set update-static-route enable
  next
end
```

```
config system link-monitor
  edit port2-monitor
    set srcintf port2
    set server 4.2.2.2
    set gateway-ip 10.200.2.254
    set protocol ping
    set update-static-route enable
  next
end
```

4.3.2 Monitoreo y pruebas del Link Monitor

```
diagnose sniffer packet any 'tcp[13]&2==2 and port 80' 4
```

```

20.962428 port3 in 10.0.1.10.59783 -> 23.61.75.27.80: syn 1163444388
20.962442 port1 out 10.200.1.1.59783 -> 23.61.75.27.80: syn 1163444388
20.962911 port1 in 23.61.75.27.80 -> 10.200.1.1.59782: syn 2959681813 ack 43814508
20.962921 port3 out 23.61.75.27.80 -> 10.0.1.10.59782: syn 2959681813 ack 43814508
20.963149 port1 in 23.61.75.27.80 -> 10.200.1.1.59783: syn 2495936434 ack 1163444389
20.963160 port3 out 23.61.75.27.80 -> 10.0.1.10.59783: syn 2495936434 ack 1163444389
21.072851 port3 in 10.0.1.10.59784 -> 50.63.243.230.80: syn 1505097546
21.072886 port1 out 10.200.1.1.59784 -> 50.63.243.230.80: syn 1505097546
21.073829 port1 in 50.63.243.230.80 -> 10.200.1.1.59784: syn 4017335094 ack 1505097547
21.073852 port3 out 50.63.243.230.80 -> 10.0.1.10.59784: syn 4017335094 ack 1505097547

```

Gráfico 40: Muestra el tráfico saliente de acuerdo al destino disponible
Fuente: Elaboración Propia

4.4 Balanceo de carga

Edit Interface

Name: wan-load-balance

Type: WAN Links Interface

Interface State: ↑ Enable ↓ Disable

WAN LLB

+ Create New ✎ Edit 🗑 Delete

Seq.#	Interface	Status	Gateway
1	port1	✔	10.200.1.254
2	port2	✔	10.200.2.254

Load Balancing Algorithm

Volume Sessions Spillover Source-Destination IP Source IP

WAN Links Usage

Bandwidth Volume

Gráfico 41: Muestra el enrutamiento para el balanceo de carga
Fuente: Elaboración Propia

Field	Value
Destination	Subnet 0.0.0.0/0.0.0.0
Device	wan-load-balance
Administrative Distance	10

4.4.1 Creación de la política para el balanceo de carga

Field	Value
Name	Internet
Incoming Interface	port3
Outgoing Interface	wan-load-balance
Source	LOCAL_SUBNET
Destination Address	all
Schedule	always
Services	ALL

4.4.2 Pruebas y monitoreo del balanceo de carga configurado.

```
37.401649 port3 cut 172.217.3.66.80 -> 10.0.1.10.52154: syn 1491890656 ack 512882779
37.615797 port3 in 10.0.1.10.52155 -> 216.239.120.235.80: syn 1938323251
37.615824 port2 cut 10.200.2.1.52155 -> 216.239.120.235.80: syn 1938323251
37.616114 port3 in 10.0.1.10.52156 -> 172.217.3.66.80: syn 1172753644
37.616133 port1 cut 10.200.1.1.52156 -> 172.217.3.66.80: syn 1172753644
37.679340 port1 in 172.217.3.66.80 -> 10.200.1.1.52156: syn 4074209909 ack 1172753645
37.679397 port3 cut 172.217.3.66.80 -> 10.0.1.10.52156: syn 4074209909 ack 1172753645
37.740044 port2 in 216.239.120.235.80 -> 10.200.2.1.52155: syn 3762422914 ack 1938323252
37.740141 port3 cut 216.239.120.235.80 -> 10.0.1.10.52155: syn 3762422914 ack 1938323252
37.763175 port3 in 10.0.1.10.52157 -> 104.73.246.75.80: syn 26349641
37.763236 port2 cut 10.200.2.1.52157 -> 104.73.246.75.80: syn 26349641
```

Gráfico 42: Muestra el tráfico saliente de acuerdo al segmento de red
Fuente: Elaboración Propia

4.5 Alta disponibilidad (HA)

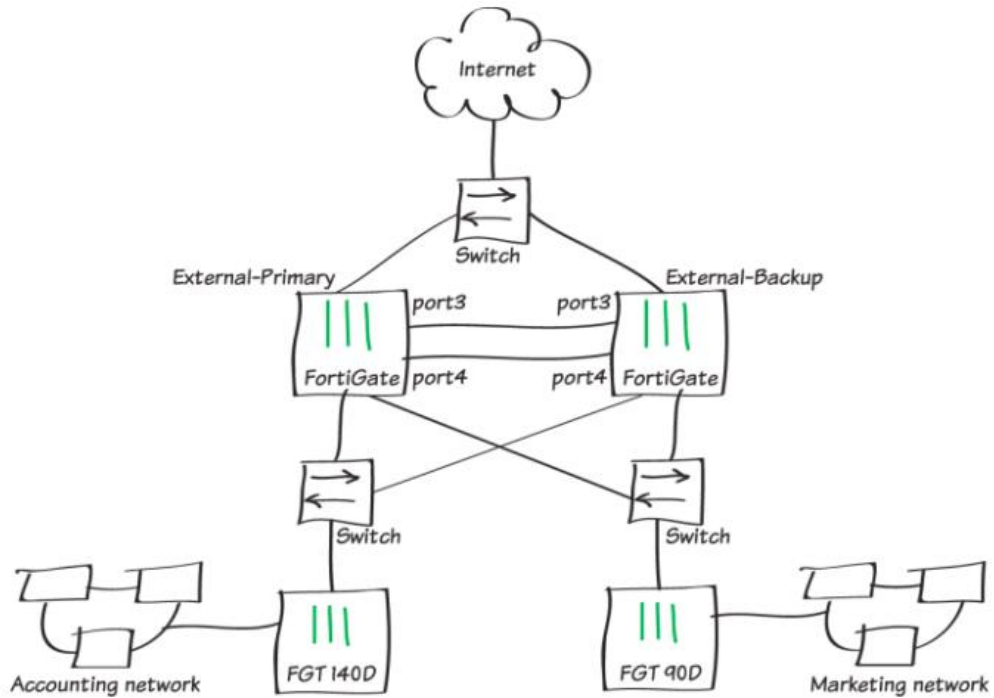


Gráfico 43: Muestra el funcionamiento de la alta disponibilidad
Fuente: Sitio Oficial Fortinet

Se diseñó mediante máquinas virtuales el modo de conexión para demostrar y validar el funcionamiento de la alta disponibilidad en equipos Fortigate.

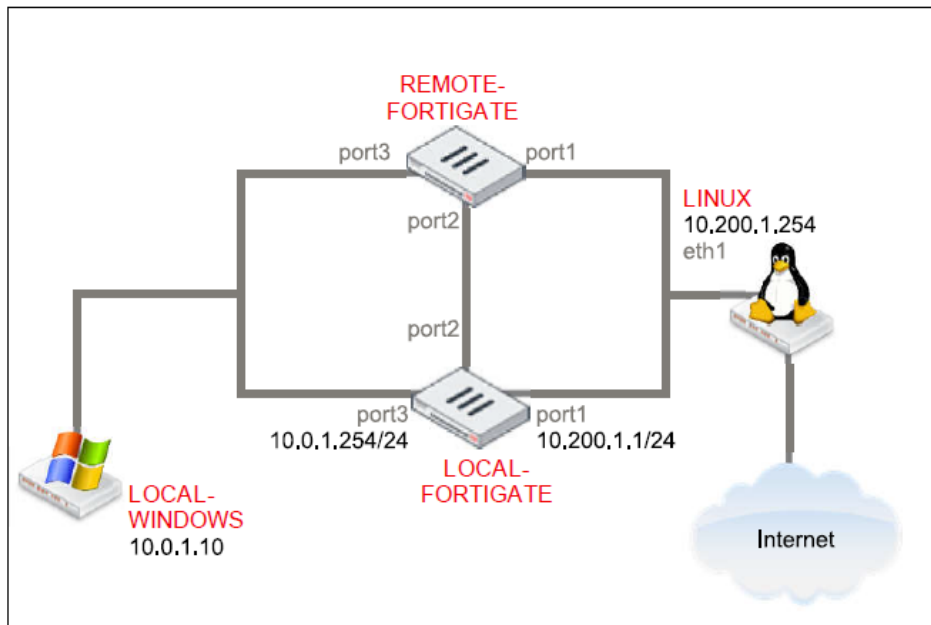


Gráfico 44: Diagrama para las pruebas de alta disponibilidad
Fuente: Elaboración Propia

Se estableció y configuro los equipos Fortigate en las máquinas virtuales, para poder validar el funcionamiento de la alta disponibilidad.

Field	Value
Mode	Active-Active
Device Priority	200
Group Name	Training
Password	Fortinet
Enable Session Pick-up	Check the box to enable it
Heartbeat Interface Enable	Check the box for port2 Uncheck the box for port4

High Availability

Mode: Active-Active

Device Priority: 200

Reserve Management Port for Cluster Member: port1

Cluster Settings

Group Name: Training

Password:

Enable Session Pick-up

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
port1	<input type="checkbox"/>	<input type="checkbox"/>	0
port2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
port3	<input type="checkbox"/>	<input type="checkbox"/>	0
port4	<input type="checkbox"/>	<input type="checkbox"/>	50
port5	<input type="checkbox"/>	<input type="checkbox"/>	0
port6	<input type="checkbox"/>	<input type="checkbox"/>	0
port7	<input type="checkbox"/>	<input type="checkbox"/>	0

Apply

Gráfico 45: Configuración del HA modo interfaz
Fuente: Elaboración Propia

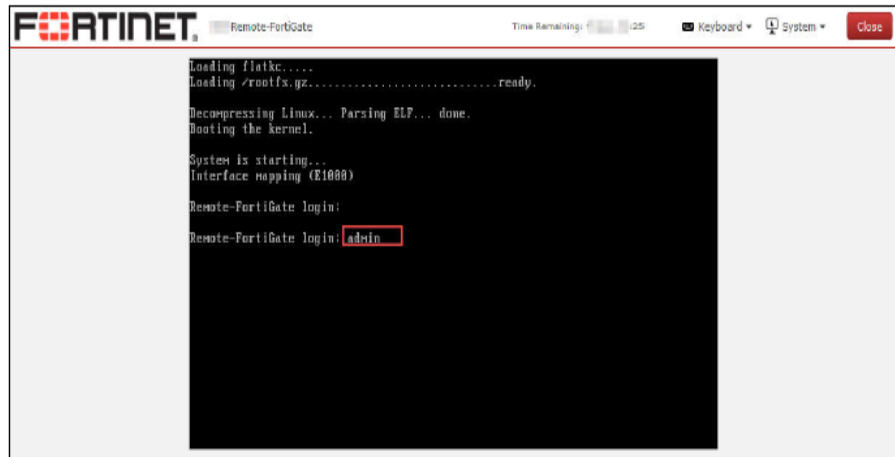


Gráfico 46: Acceso configuración HA en Fortigate remoto
Fuente: Elaboración Propia

Se proceder a configurar los parámetros de HA en el segundo equipo Fortigate

```
config system ha

    set group-name Training

    set mode a-a

    set password Fortinet

    set hbdev "port2" 0

    set session-pickup enable

    set override disable

    set priority 100

end
```



Gráfico 47: Muestra por interfaz el funcionamiento del HA por interfaz
Fuente: Elaboración Propia

4.6 Filtro Web

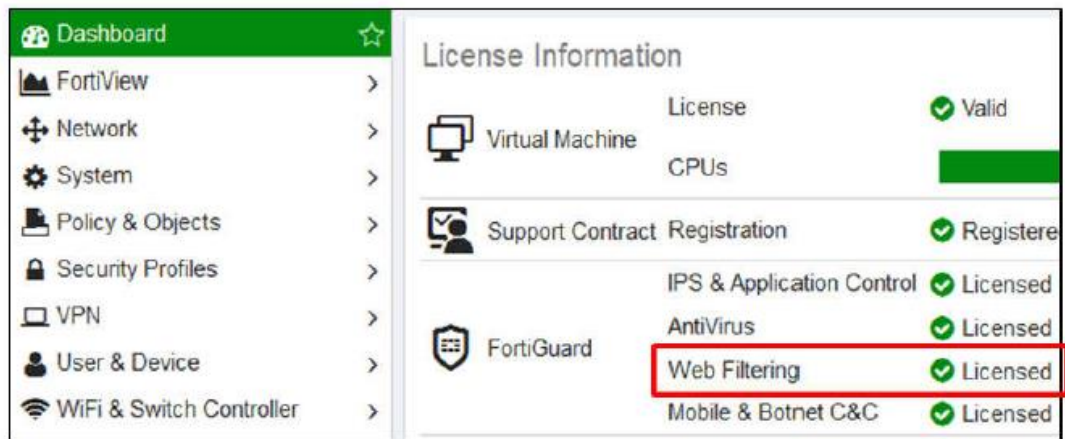


Gráfico 48: Muestra la licencia de Filtro Web
Fuente: Elaboración Propia



Gráfico 49: Muestra Filtro web por default
Fuente: Elaboración Propia



Gráfico 50: Muestra las categorías del Filtro Web
Fuente: Elaboración Propia

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
port3 - port1 (1 - 1)									
1	Internet_Access	all	all	always	ALL	ACCEPT		Enabled	Disabled

Gráfico 51: Muestra una regla que contiene el filtro web
Fuente: Elaboración Propia

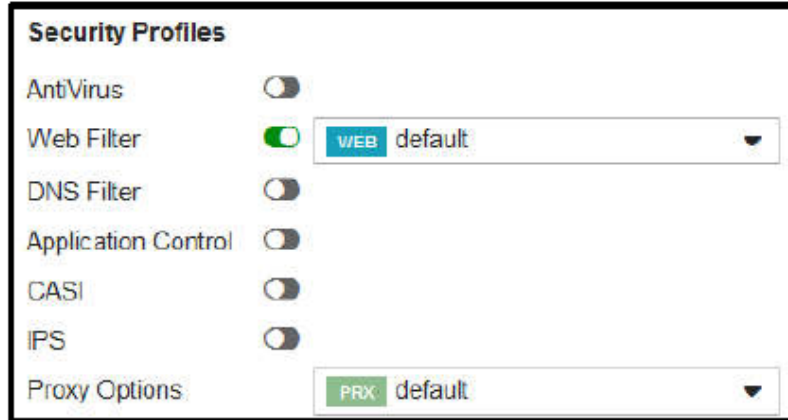


Gráfico 52: Muestra habilitado el Filtro web en la regla
Fuente: Elaboración Propia

Website	Category	Action
http://www.youtube.com/	Streaming Media category	Block
http://www.skype.com/	Internet Telephony	Warning
http://www.bing.com/	Search Engines and Portals	Allow

Gráfico 53: Muestra la acción al aplicar la regla
Fuente: Elaboración Propia



Gráfico 54: Muestra el mensaje de bloqueo con Filtro web
Fuente: Elaboración Propia



Gráfico 55: Muestra el mensaje de alerta y acceso por Filtro web
Fuente: Elaboración Propia



Gráfico 56: Muestra el modo de activar la autenticación de acceso
Fuente: Elaboración Propia



Gráfico 57: Muestra la alerta de acceso modo autenticación
Fuente: Elaboración Propia

The screenshot shows the 'Log & Report' section of the FortiGuard Web Filtering interface. It features a table of log entries and a 'Log Details' sidebar for the selected entry (row 17).

#	Date/Time	User	Source	Action	Destination
1	09:09:23		10.0.1.241	passthrough	208.91.112.68/
2	09:09:13		10.0.1.10	passthrough	www.bing.com/fd/ls/lsp.asp
3	09:09:00		10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=0
4	09:09:00		10.0.1.10	passthrough	www.bing.com/fd/ls/lsp.asp
5	09:09:00		10.0.1.10	passthrough	www.bing.com/Passport.as
6	09:09:00		10.0.1.10	passthrough	www.bing.com/
7	09:09:00		10.0.1.10	passthrough	a4.bing.com/fd/ls/l?IG=070
8	09:09:00		10.0.1.10	passthrough	login.live.com/
9	09:08:58		10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=0
10	09:08:58		10.0.1.10	passthrough	www.bing.com/HPImageAr
11	09:08:58		10.0.1.10	passthrough	www.bing.com/hp?ID=S
12	09:08:58		10.0.1.10	passthrough	www.bing.com/notifications
13	09:08:58		10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=0
14	09:08:58		10.0.1.10	passthrough	www.bing.com/fd/ls/lsp.asp
15	09:09:57		10.0.1.10	passthrough	www.bing.com/
16	09:08:03		10.0.1.10	blocked	www.bing.com/
17	09:07:31		10.0.1.10	blocked	www.bing.com/

The 'Log Details' sidebar for the selected entry (row 17) shows the following information:

- General:** Date: 05/02/2016, Time: 09:07:31, Session ID: 56, Virtual Domain: root
- Source:** IP: 10.0.1.10, Port: 54289, Interface: port3
- Destination:** IP: 204.79.197.200, Port: 80, Interface: port1, Hostname: www.bing.com, URL: www.bing.com/
- Application:** Protocol: 8

Gráfico 58: Muestra el modo de verificar accesos y trafico web
Fuente: Elaboración Propia

4.7 Control de aplicaciones



Gráfico 59: Muestra el perfil por defecto de control de aplicaciones
Fuente: Elaboración Propia

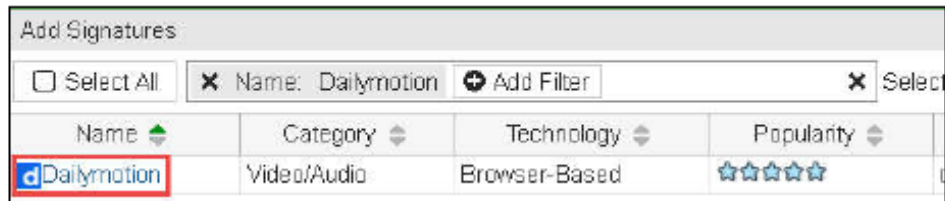


Gráfico 60: Muestra el modo de añadir una aplicación al perfil
Fuente: Elaboración Propia

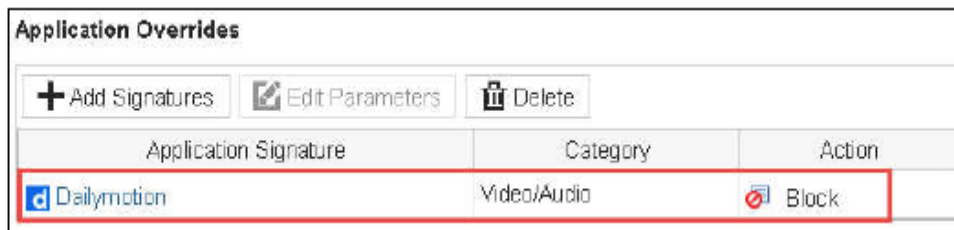


Gráfico 61: Muestra la acción que puede tomarse sobre la aplicación
Fuente: Elaboración Propia

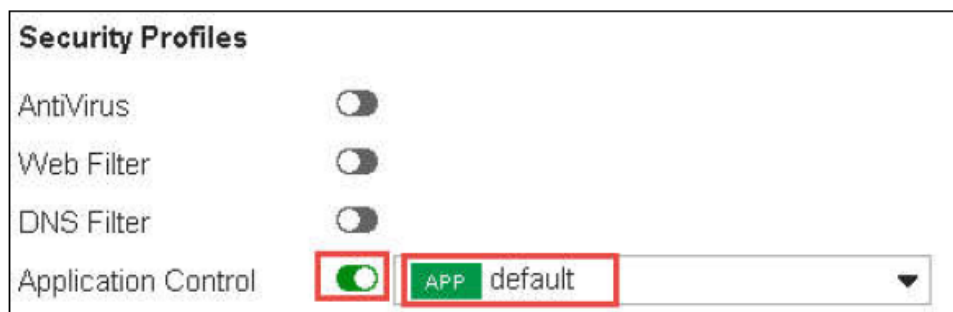


Gráfico 62: Muestra el modo aplicar el perfil a una regla
Fuente: Elaboración Propia

4.8 Traffic Shaping - Segmentación del ancho de banda

Con el Traffic shaping o segmentación del ancho de banda, se hace posible limitar el ancho de banda para grupos, usuarios y destinos específicos, inclusive determinar el límite máximo de consumo del BW.




Gráfico 63: Muestra el modo agregar el perfil a una regla
Fuente: Elaboración Propia

4.9 VPN y Acceso remoto a equipo Fortigate

La VPN nos posibilita realizar conexiones a nuestra red interna utilizando la infraestructura de internet, puede ser mediante una VPN tipo, sitio a sitio o sitio a cliente.

Field	Value
Listen on Interface(s)	port1
Listen on Port	10443
Restrict Access	Allow access from any host
Inactive For	3000 seconds
Server Certificate	Fortinet_Factory
Field	Value
Name	SSL VPN Access
Incoming Interface	SSL-VPN tunnel interface
Outgoing Interface	port3
Source	SSLVPN_TUNNEL_ADDR1 SSL_VPN_USERS
Destination Address	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

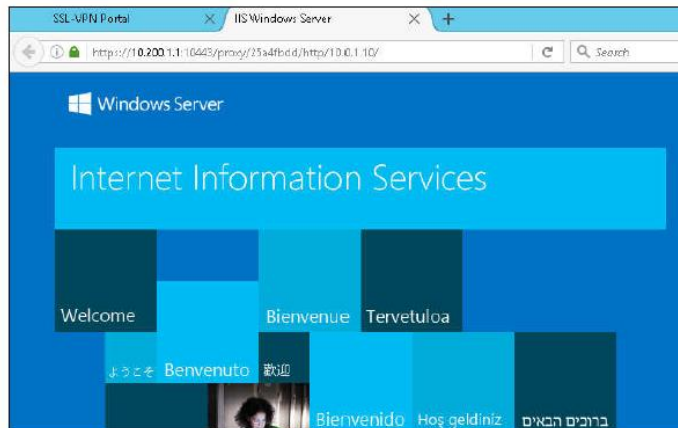


Gráfico 64: Muestra el modo de acceso por VPN portal
Fuente: Elaboración Propia



Gráfico 65: Muestra el modo de acceso por cliente
Fuente: Elaboración Propia



Gráfico 66: Muestra la sesión iniciada por la VPN
Fuente: Elaboración Propia

CONCLUSIONES

- Se realizó la identificación del estado actual a nivel de red y comunicaciones con que cuenta la Universidad Nacional José María Arguedas y se planteó un diagrama de red y el dimensionamiento de equipos de acuerdo a su alcance.
- Se realizó las pruebas de la comunicación de voz entre el local principal y el local de la Facultad de Sistemas, y se concluye que solamente cuando se garantice que no existe pérdida de paquetes constantemente ni una latencia alta, se puede utilizar el medio para la comunicación de voz, video y datos.
- De acuerdo a las pruebas realizadas y los resultados obtenidos. Se concluye que la baja calidad en la comunicación de voz, video y datos en la Universidad Nacional José María Arguedas, es a causa a un deficiente servicio de Internet contratado, el equipo Balanceador con el que cuenta y el modelo de router instalados en cada local.

RECOMENDACIONES

A continuación, se formulan algunas recomendaciones de acuerdo con las pruebas y resultados obtenidos.

PRIMERO: Se recomienda dar de baja los 06 servicios de Internet ADSL que tiene contratado la Universidad, ya que se evidencio que el ancho de banda ofrecido es variable y generará indisponibilidad de la red en la Universidad.

SEGUNDO: Se recomienda instalar una central Telefónica PBX para la comunicación de voz en la Universidad, y remplazar los router Mikrotik por unos equipos Fortigate 800E en HA, los cuales proporcionan mayor performance y facilitan la administración de la red.

TERCERO: Se recomienda que la Universidad contrate para sus locales de Santa Rosa, Ccoyahuacho y local Principal, líneas de Internet simétricas con calidad de servicio (Qos) y un SLA no menor al 99.5%.

CUARTO: De acuerdo con lo referido en el punto 3.3 del Capítulo 3 del presente informe. Se recomienda realizar la contratación de un ancho de banda de 150Mb para la operativa óptima de la Universidad Nacional José María Arguedas.

QUINTO: De acuerdo a la metodología PPDIOO propuesta para la administración de la red LAN, dentro de la fase de optimización, se recomienda mantener un constante monitoreo de la red,. De esta forma garantizar la disponibilidad de la red en todo momento y una buena calidad de en la comunicación de voz, video y datos.

REFERENCIAS BIBLIOGRÁFICAS

- Álvarez et al. (2014). Redes Privadas Virtuales. Chile
- Cisco S.I (2008). Cómo las Redes privadas virtuales funcionan.
- Diaz.A.P.A (2010). Diseño e Implementación de una Red Privada Virtual para la Empresa Eléctrica Quito S.A. Ecuador.
- Fernández et al (2006). Redes Privadas Virtuales. España
- Gonzales. M.A. (2006). Redes Privadas Virtuales. México
- Hernández et al (1998). Metodología de la Investigación (2a. edición). México
- Menendez.A.R. (2012). Estudio Del Desempeño e Implementación de una Solución MPLS-VPN sobre Múltiples Sistemas Autónomos Ecuador
- Rincón C. (2003), Modelo matemático para la estimación del rendimiento de una red Ethernet. Volumen 3 Edición No 2. Venezuela
- Stolk. A (2009). Buenas prácticas para la optimización de anchos de banda limitados. Venezuela
- Trujillo, E.M. (2006). Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSEc. Quito, Ecuador.
- Urdaneta. A (2005) Análisis de Tráfico en una Red LAN aplicando la Tecnología de Redes Neuronales. Venezuela
- Peinado.M.M (2012) Proyecto de Guía Rápida De Cacti
- Guerrero.D (1998). SNMP: Administración y Mantenimiento de Redes con Linux
- Perez. I.S (2001). Análisis del protocolo IPSec: el estándar de seguridad en IP
- Diaz.N.J et al (2006) Elaboración e Implementación de laboratorios didácticos para monitoreo del tráfico en la red, antes y después de segmentar en dominios de colisión y broadcast utilizando el open source CACTI Quito .Ecuador
- Junco.R.G et al, (2018) Los recursos de red y su monitoreo. Cuba
- Erazo, G.P (2016). Propuesta de metodología para la implementación de Proyectos de redes – caso de estudio institución financiera local. Quito-Ecuador.

- Ortiz. S.G (2003) Diseño y construcción de un micro web server para el Monitoreo de señales analógicas y digitales. México.
- Asenjo. E.A.C (2006) Optimización e implementación de la red ALN en el instituto de electricidad y electrónica UACH. Chile
- Cruz. M.A (2013) Aplicación para analizar el rendimiento de red. España.
- Albeiro. W.B (2010), Implementación de Redes Privadas Virtuales en la mediana empresa.

ANEXOS

ANEXO 1: SOLICITUD DE ACCESOS Y DOCUMENTACIÓN A LA OSI

N° 013395

Universidad Nacional José María Arguedas
 Identidad y Excelencia para el Trabajo Productivo y el Desarrollo
FORMULARIO ÚNICO DE TRÁMITE

SOLICITO: Accesos y Documentación de la OSI para la ejecución del proyecto de tesis

SEÑOR: Dr. Julio Benito Heredia Paruelo VICE PRESIDENTE DE LA COMISIÓN ORGANIZADORA DE LA UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS.

YO: Bequer Oroscó Pahuara
 Alumna(a): Docente Administrativo
 de la Carrera Profesional: INGENIERÍA DE SISTEMAS
 Código de Matricula N° 1000720102 DNI: 46833183
 Domiciliado (a): Jr. Narvaez Melara 348 - San Jacinto

Ante Ud. con el debido respeto me presento y expongo:

Que, parte de la ejecución de mi tesis que estoy desarrollando, tengo que instalar unos equipos en el local central y las salas de san Jacinto y Celajancha. Cuyo Requite Realizar la instalación de equipos software y una cámara de video y una Headset virtual para el monitoreo de internet, todo esto de manera temporal

Solicito: LA AUTORIZACION DE ACCESO Y COORDINACION CON OSI PARA LA ejecución del proyecto de tesis, considerando mi solicitud por motivos académicos

Trámite Grado de Bachiller Reserva de Matricula Constancia de Estudios
 Trámite Título Profesional Matricula extemporánea Constancia de no Deudor
 Certificado de Estudios Reanudación de Estudios Constancia de Notas
 Otros:

Andahuaylas, 07 de JUNIO de 2018

[Firma]
Firma del Solicitante

Adjunto: 1) 3)
 2) 4)

Pase a:


Universidad Nacional José María Arguedas
 Identidad y Excelencia para el Trabajo Productivo y el Desarrollo
FORMULARIO ÚNICO DE TRÁMITE

N° 013395

Datos del Solicitante: BEQUER OROSCO PAHUARA
 Fecha: 07-06-2018 DNI: 46833183
 Trámite que solicita: ACCESOS Y DOCUMENTACION DE LA OSI PARA LA EJECUCION DEL PROYECTO DE TESIS

ANEXO 2: SOLICITUD DE ACCESOS Y DOCUMENTACIÓN RECIBIDO

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

 **Universidad Nacional José María Arguedas**
Identidad y Excelencia para el Trabajo Productivo y el Desarrollo

FORMULARIO ÚNICO DE TRÁMITE

Nº 013395

SECRETARÍA GENERAL
TRÁMITE DOCUMENTARIO
RECIBIDO

Datos del Solicitante: BEQUEN OROSCO PAHURBA

Fecha: 07-06-2018 DNI: 46833153

Trámite que solicita: ACCESOS Y DOCUMENTACION DE LA OSI PARA LA EJECUCION DEL PROYECTO DE TESIS

Nº REG: 1862 FECHA: 07 JUN 2018
HORA: 11:30
FOTO: 9 FIRMA: [Signature]

ANEXO 3: CONSTANCIA DE TRABAJOS REALIZADOS EMITIDO POR LA OSI

CONSTANCIA DE TRABAJOS REALIZADOS

Mediante el presente documento, se deja constancia que se ha realizado las pruebas y diagnóstico de la infraestructura de red y comunicaciones de la Universidad Nacional José María Arguedas. Se considera exclusivamente el presente como referencia al proyecto de tesis "IMPLEMENTACION Y EVALUACIÓN DE LA PERFORMANCE DE LA COMUNICACIÓN DE VOZ, VIDEO Y DATOS ENTRE LAS SEDES DE LA UNAJMA MEDIANTE UNA RED PRIVADA VIRTUAL" desarrollado por el Bach. BEQUER OROSCO PAHUARA, asociado a la solicitud N°13395 "Accesos y Documentación de la OSI para la ejecución del proyecto de Tesis" con fecha 07/06/18; las pruebas realizadas el día sábado 10 de noviembre del presente año fueron verificadas por la MSc. Ing. Luz Delia Quina Quina en la sede central administrativo y por Bach. Nicmar García Reynaga en la Escuela Profesional de Ingeniería de Sistemas.

ENTIDAD	: Universidad Nacional José María Arguedas
FECHA	: 10/11/2018
PERSONAL A CARGO	: Bequer Orosco Pahuara
DNI	: 46833183
DURACIÓN	: 5 Horas
DESCRIPCION DE TRABAJOS	- Análisis, diagnóstico y pruebas de la red LAN-WAN - Contacto y gestión de velocidad con los proveedores de Internet - Instalación de equipos de redes y comunicaciones de forma temporal, local Central y Escuela Profesional de Ingeniería de Sistemas - Recomendaciones para la administración de la red
FECHA – HORA DE INICIO	: 10/11/2018– 09:00AM
FECHA – HORA DE TERMINO	: 10/11/2018– 14:00PM

Andahuaylas, 12 de noviembre de 2018



UNIVERSIDAD NACIONAL
JOSÉ MARÍA ARGUEDAS
Ing. Yovana Flores Coarasa
JEFE IN DE LA OFICINA DE SISTEMAS DE INFORMACIÓN