UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA
Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA"

AUTOR: RODRIGO JAVIER TORRES BOLAÑOS

DIRECTOR: ING. JORGE LUIS NOGUERA ROSERO

IBARRA – ECUADOR

2014

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1.- IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.
Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información

DATOS DEL CONTACTO	
CÉDULA DE IDENTIDAD	040167354-6
APELLIDOS Y NOMBRES	TORRES BOLAÑOS RODRIGO JAVIER
DIRECCIÓN	LA VICTORIA, LUIS A. MARTÍNEZ DE LA VEGA 2-32 Y HUGO GUZMÁN LARA
E-mail	rjtorres@utn.edu.ec
TELÉFONO FIJO	062615594
TELÉFONO MÓVIL	0996725078
DATOS DE LA OBRA	
TÍTULO	“SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA UNIVERSIDAD TÉCINA DEL NORTE
AUTOR	TORRES BOLAÑOS RODRIGO JAVIER
FECHA	1 DE DICIEMBRE 2014
PROGRAMA	PREGRADO
TÍTULO POR EL QUE SE ASPIRA	INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
DIRECTOR	ING. JORGE LUIS NOGUERA ROSERO

2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, RODRIGO JAVIER TORRES BOLAÑOS, con cédula de identidad Nro. 040167354-6, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

.....

Firma

Rodrigo Javier Torres Bolaños

040167354-6

Ibarra, Diciembre del 2014

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico, que el presente trabajo de grado "SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE" fue desarrollado en su totalidad por el egresado de la Carrera de Ingeniería en Electrónica y Redes de Comunicación Sr. Rodrigo Javier Torres Bolaños, bajo mi supervisión.

.....

Ing. Jorge Luis Noguera Rosero
DIRECTOR DEL PROYECTO

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, RODRIGO JAVIER TORRES BOLAÑOS, con cédula de identidad Nro. 040167354-6, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado "SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE", que ha sido desarrollado para optar el título de Ingeniero en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, Diciembre del 2014

.....

Firma

Rodrigo Javier Torres Bolaños

040167354-6

Ibarra, Diciembre del 2014

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto la obra es original y que es titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

.....

Firma

Rodrigo Javier Torres Bolaños

040167354-6

Ibarra, Diciembre del 2014

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DECLARACIÓN

Yo, Rodrigo Javier Torres Bolaños, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte

Rodrigo Javier Torres Bolaños

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

AGRADECIMIENTO

A mis padres, por brindarme todo el apoyo durante mi etapa estudiantil y ser la inspiración para cada uno de mis logros.

A mi director de Tesis, Ing. Jorge Noguera, quien supo asesorarme de la mejor manera para culminar exitosamente mi trabajo de titulación.

Al IEEE y su Student Branch de la Universidad Técnica del Norte, en quienes encontré una segunda familia, con amigos de todas partes del País.

Al Ing. Carlos Vásquez e Ing. Jaime Michilena quienes a más de ser docentes en la carrera se convirtieron en amigos y recibir su ayuda, consejos, palabras de aliento e incluso regaños lograron formar en mí un profesional de ética y calidad, por todo ello muchas gracias.

Al Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte y sus dirigentes quienes permitieron que realice mi trabajo de titulación en sus instalaciones.

A mi Santísima, que me dio una segunda oportunidad de vida y cada día darme la serenidad y alegría de disfrutar de los míos. Muchas gracias SM porque en tus manos están mis pasos.

Rodrigo Javier Torres Bolaños

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DEDICATORIA

Dedico este proyecto a mis padres Víctor y María quienes son inspiración, a mi abuelo Juan José por inculcarme el estudio desde pequeño, a mi sobrino Elías Alejandro por darme un motivo más para sonreír día a día. A toda mi familia por siempre estar a mi lado cuando más lo necesito.

Javier

CONTENIDO

INDICE DE IMÁGENES

INDICE DE TABLAS

INDICE DE ECUACIONES

RESUMEN

El presente trabajo de titulación consiste en el diseño e implementación un sistema de seguridad perimetral para la red informática de la Universidad Técnica del Norte mediante el uso del Software Libre.

Para el desarrollo del sistema de seguridad perimetral se definió tres etapas de trabajo las cuales fueron: Segmentación de Red, Firewall e IPS. Para la nueva segmentación de la red se extrajo las configuraciones de cada una de las interfaces de los diferentes equipos activos de red que posee la Universidad, ya que solo se realizó un cambio lógico mas no un cambio físico y la información que se necesitaba era el número de la VLAN a la que pertenecía dicha interfaz para que en la nueva configuración la interfaz pertenezca a la misma VLAN, posteriormente se realizó una nueva distribución de VLANs para las diferentes dependencias de la Universidad así como su respectivo direccionamiento IP.

Para la ejecución del Firewall y el IPS se optó por implementar la virtualización, el sistema operativo para la virtualización es Xen-Server el cual posee un administrador de servidores llamado Xen-Center, en este servidor de virtualización se implementó dos máquinas virtuales para el Firewall e IPS. Ambos sistemas se encuentran instalados en el sistema operativo bajo plataforma de software libre CentOS 6.5. Para el manejo y administración del Firewall se utilizó Shorewall y Webmin los cuales permiten ingresar las líneas de políticas de seguridad de una manera más interactiva para el usuario. La implementación del IPS fue desarrollada mediante Suricata el cual es un motor IDS/IPS basado en software libre.

ABSTRACT

This graduation work consist to design and implement a perimeter security system for the computer network of the Tecnica del Norte University by using free software.

For the development of perimeter security system working three stages which we defined: Network Segmentation, Firewall and IPS. For the new network segmentation configurations of each of the interfaces of the different active network equipment's that the University has extracted, as only a logical change was made but not a physical change and the information that needed was the number of the VLAN to which the interface belongs to the new configuration interface belong to the same VLAN, tan a new distribution of VLANs for the different departments of the University as well as their respective routing is performed.

For the implementation of Firewall and IPS was decided to implement virtualization, operating system virtualization is Xen-Server which has a servers administrator called Xen-Center, in this virtualization server was implemented two virtual machines for Firewall and IPS. Both systems are installed on the operating system under free software CentOS 6.5. For the management and administration of the Firewall was used Shorewall and Webmin which allow you to enter lines of security policies in a more interactive way for the user. The implementation of IPS was developed by Suricata which is an IDS / IPS engine based on free software.

PRESENTACIÓN

1. TEMA: SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA "UNIVERSIDAD TÉCNICA DEL NORTE" DE LA CIUDAD DE IBARRA	
2. ÁREA / LÍNEA DE INVESTIGACIÓN: • Networking • Seguridad en Redes • Sistemas Operativos • Administración de Redes	
3. ENTIDAD QUE AUSPICIA: Universidad Técnica del Norte	
4. DIRECTOR: Ing. Jorge Noguera	
5. AUTOR: Rodrigo Javier Torres Bolaños DIRECCIÓN: La Victoria, Luis A. Martínez 2-32 TELÉFONO: 062644774 - 0996725078 CORREO ELECTRÓNICO: rjtb1988@gmail.com	
6. DURACIÓN (Estimado): 6 meses	
7. INVESTIGACIÓN: Nueva ( ) Continuación (X)	
8. PRESUPUESTO (estimado): 5500 Dólares Americanos	
PARA USO DEL CONSEJO ACADÉMICO	
FECHA DE ENTREGA:	FECHA DE REVISIÓN:
APROBADO: SI ( ) NO ( )	FECHA DE APROBACIÓN:
OBSERVACIONES:	

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

PLAN DEL PROYECTO DE TITULACIÓN

Propuesto por:	**Áreas Técnicas del Tema:**
Torres Bolaños Rodrigo Javier	Networking Seguridad en Redes Sistemas Operativos Administración de Redes
Director sugerido:	**Fecha:**
Ing. Jaime Michilena	5 de Junio del 2012

1. Tema

SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA "UNIVERSIDAD TÉCNICA DEL NORTE" DE LA CIUDAD DE IBARRA

2. Problema

La evolución de la tecnología y la constante demanda de seguridad han permitido que los sistemas de seguridad perimetral en redes evolucionen para ofrecer una mayor confiabilidad a los usuarios tanto internos como externos sobre la transparencia y protección de su información para el acceso de diferentes servicios, hoy en día existen un sin número de personas que usan sus conocimientos y ética profesional de una forma incorrecta al ingresar a redes informáticas restringidas ocasionado pérdidas multimillonarias alrededor del mundo. Por ello la seguridad informática se ha convertido en una inversión justificable para toda organización que requiera integridad y seguridad en sus sistemas de administración de la información.

Con el paso de los años la Universidad Técnica del Norte ha crecido en cuanto a su campus universitario y con ello toda su infraestructura tecnológica, lo que permite que miles de personas tanto estudiantes, docentes y trabajadores tengan acceso a los diferentes servicios que presta la Casona. Este incremento en la capacidad de la Red

Informática, ha traído como consecuencia que la segmentación de la Red no esté acorde a las necesidades que esta requiere, lo que permite que la red universitaria tenga un alto número de colisiones en diferentes puntos de la red, debido al broadcast de información que puede generar uno de los tantos usuarios internos. Otro de los inconvenientes es poseer un equipo ASA 5520 el cual se encuentra configurado como firewall pero no posee las políticas de seguridad necesarias lo que hace vulnerable a la red de la Universidad Técnica del Norte a los ataques externos e internos.

Entre los diferentes problemas y ataques a los que esta vulnerable la Red Informática se encuentran: La mayoría de las PCs generan gran cantidad de alertas de virus lo que crea broadcast de información al igual que las peticiones de NetBIOS; entre los ataques se ha detectado muchos de tipo fuerza bruta con la finalidad de conectarse a las IPs públicas de la Universidad, al igual que ataques de denegación de servicio enviando paquetes SYN, entre otros.

En el transcurso de los años el Campus Universitario y a su vez la Infraestructura Tecnológica de la Universidad Técnica del Norte crecerán a medida de las necesidades que ésta requiera, es por ello que las políticas de seguridad implementadas, así como la segmentación de la red, protegerán a toda la Red Informática de los futuros ataques internos y externos, logrando así que la seguridad y confiabilidad de la información entre todos los usuarios de la red, sea confiable y protegido de amenazas informáticas.

3. Objetivos

Objetivo General

- Implementar las políticas de seguridad necesarias en la Red Informática de la Universidad Técnica del Norte, mediante el diseño de la seguridad perimetral, evitando así ataques externos e internos de forma eficiente.

Objetivos Específicos

- Describir las características y requerimientos del servicio de seguridad perimetral, así como también un estudio acerca de la seguridad en redes, para la aplicación en la Red Informática de la Universidad Técnica del Norte.

- Analizar la situación actual de la Infraestructura Lógica de la Red Informática de la Universidad Técnica del Norte, para realizar el dimensionamiento correcto de los segmentos de la red.

- Estudiar los resultados obtenidos en el trabajo de titulación HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA "UNIVERSIDAD TÉCNICA DEL NORTE" para establecer las actualizaciones que necesita el Firewall con respecto a las políticas de seguridad, así como las características del IPS.

- Diseñar el IPS y firewall con las respectivas políticas de seguridad obtenidas en el estudio previo de la HONEYNET, las cuales protegerán a la Red de los posibles ataques externos e internos. Y la segmentación de la Red Informática para la prevención de colisiones dentro de la misma.

- Implementar el sistema de Seguridad Perimetral, la cual protegerá a los sistemas computacionales de la Red Informática de los ataques externos e internos que se generen; así como la configuración de las nuevas VLANs que garantizarán una correcta segmentación de Red.

- Demostrar el funcionamiento de la seguridad perimetral en el entorno de la Red Universidad Técnica del Norte, realizando pruebas que simulen ataques internos y externos a la red.

- Realizar un análisis Económico, mediante una comparación entre los equipos que se posee actualmente y los que se proponen como solución en el proyecto.

4. Alcance

El presente proyecto de titulación consiste en la implementación de las políticas de seguridad necesarias que permitan el bloqueo de amenazas externas hacia la Red Informática de la Universidad Técnica del Norte, así como también el rediseño de la segmentación de la red por medios de VLANs.

Para dar cumplimiento con lo propuesto, se inicia con el análisis del Marco Teórico, en el cual abordaremos las características necesarias para la implementación de la

Seguridad Perimetral, así como también un estudio acerca de la Seguridad de Redes, es imprescindible analizar los fundamentos necesarios que nos permitirán realizar la segmentación de la red mediante VLANs.

Para la realización del diseño del IPS, firewall, y segmentación de la Red, se tomará como punto de partida el análisis realizado a la situación actual de la Estructura Lógica de la Red Informática de la Universidad Técnica del Norte, esto permite efectuar una correcta segmentación a la Red por medio de VLANs estáticas en la mayoría de la red y VLANs dinámicas en los segmentos de red que sea necesario.

Por otra parte disponemos los resultados acerca de los ataques y vulnerabilidades internos y externos que tiene la Red Informática obtenidos en el estudio realizado en el trabajo HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA "UNIVERSIDAD TÉCNICA DEL NORTE", los cuales luego de un análisis permiten establecer las políticas de seguridad para el firewall y el IPS.

La implementación consta en la configuración del firewall, que tiene las políticas de seguridad que permita el bloqueo de ataques externos como internos, hacia y desde la Red Informática , también consta con la instalación y configuración de los equipos necesarios para el IPS que cumplirá los requerimientos para la prevención de intrusos a la Red. Además se configurará los Switchs y Routers que administran la red, con las VLANs resultantes del diseño, para una correcta segmentación de la Red.

Posteriormente a la implementación del sistema de Seguridad Perimetral y VLANs, realizaremos las pruebas necesarias para demostrar el correcto funcionamiento de los mismos atacando externamente a la Red Informática, así como también generando ataques internos en la misma.

Posteriormente se realiza un análisis costo – beneficio tomando en cuenta una comparación entre los equipos que posee la Universidad Técnica del Norte y están en funcionamiento, con los equipos que se presentan como solución en este proyecto.

Para terminar el proyecto de titulación, se da a conocer las conclusiones y recomendaciones obtenidas en el transcurso de la investigación y realización del trabajo.

5. Justificación

La Universidad Técnica del Norte hoy por hoy posee una gran Red Informática dentro de su campus, en el cual se encuentran sus diversos servidores, Routers y Switchs de administración de la red. Por los cuales se cursa gran cantidad de información principalmente del sistema informático que posee la Universidad, pero también información con respecto a todos los estudiantes que pertenecen a la Institución. Es por ello que la Red Informática está expuesta a ataques externos, pero también los usuarios internos de la red pueden atacarla con diferente software malicioso que ocasiona la caída de la red.

La implementación de la Seguridad Perimetral en el entorno de la Red Informática, garantizará la confiabilidad y seguridad de la información que cursen todos los usuarios de la red, y así la protegerá de los diferentes ataques internos y externos que se produzcan.

Tomando en cuenta que hoy en día la Universidad Técnica del Norte está en el proceso de acreditaciones tanto nacional e internacional con el CEAACES Y EL CINDA respectivamente, el desarrollo de este proyecto aportará significativamente en la aprobación de calidad de educación superior que se necesita para las acreditaciones.

6. Contexto

Vinueza Tatiana (2011). HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA “UNIVERSIDAD TÉCNICA DEL NORTE” DE LA CIUDAD DE IBARRA. Tesis de Ingeniería en Electrónica y Redes de Comunicación. Universidad Técnica del Norte, Facultad de ingeniería en Ciencias Aplicadas, Ibarra, Ecuador.

A diferencia de este proyecto el cual está enfocado a la obtención de los diferentes ataques y problemas que ocurren a diario en la Red de la Universidad Técnica del Norte, la implementación de Seguridad Perimetral implementa las políticas de seguridad que sean necesarias para la prevención de los ataques que se puedan generar.

7. Contenidos

- **CAPÍTULO 1**

FUNDAMENTOS DE SEGURIDAD EN REDES

En este capítulo se describirán los aspectos básicos acerca de la seguridad en redes, las características de la Seguridad Perimetral y las particularidades que se necesitan para la segmentación de redes.

- **CAPITULO 2**

ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED INFORMÁTICA

En este capítulo se realizara el estudio de la Red Informática de la Universidad Técnica del Norte teniendo como resultado las necesidades para la segmentación de la red, también se realizará el estudio de los resultados obtenidos en el trabajo HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA "UNIVERSIDAD TÉCNICA DEL NORTE" y obteniendo los requerimientos para la implementación del IPS y firewall.

- **CAPITULO 3**

DISEÑO DE LA SEGURIDAD PERIMETRAL EN EL ENTORNO DE LA RED

Este capítulo constará con los diseños del IPS, firewall y la segmentación de la red, de acuerdo a los resultados obtenidos en el estudio previo. Todos estos diseños permitirán el cumplimiento de la Seguridad Perimetral

- **CAPITULO 4**

IMPLEMENTACIóN DE LA SEGURIDAD PERIMETRAL EN EL ENTORNO DE LA RED

En este capítulo se procederá con la configuración de los equipos necesarios para la implementación de la seguridad perimetral, así como para la IPS, Firewall y Segmentación.

- **CAPITULO 5**

PRUEBAS DE FUNCIONAMIENTO DE LA SEGURIDAD PERIMETRAL

Se simularán varios ataques informáticos externos e internos, los cuales demostrarán el correcto funcionamiento del sistema de Seguridad Perimetral.

- **CAPITULO 6**

ANÁLISIS ECONÓMICO

Se realizará un análisis Costo-Beneficio entre los equipos existentes y los que se utilicen en el desarrollo y solución del Sistema de Seguridad Perimetral.

- **CONCLUSIONES Y RECOMENDACIONES**

Se mencionarán las diversas conclusiones y recomendaciones que den como resultado este proyecto de titulación.

- **BIBLIOGRAFíA**

- **ANEXOS**

8. Cronograma de Actividades

N°	ACTIVIDAD	DURACION																							
		MES 1				MES 2				MES 3				MES 4				MES 5				MES 6			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
A	Recopilación de la Información																								
B	Redacción del Capítulo 1																								
C	Revisión Capítulo 1																								
D	Análisis de la Situación actual de la Red Informática																								
E	Redacción del Capítulo 2																								
F	Revisión Capítulo 2																								
G	Diseño de IPS, Firewall y Segmentación de la Red																								
H	Redacción del Capítulo 3																								
I	Revisión Capítulo 3																								
J	Implementación de la Seguridad Perimetral en la Red de Distribución																								
K	Redacción del Capítulo 4																								
L	Revisión Capítulo 4																								
M	Simulación de ataques externos e internos.																								
N	Obtención de Resultados																								
O	Redacción del Capítulo 5																								
P	Revisión Capítulo 5																								
Q	Elaboración de Conclusiones y Recomendaciones																								
R	Bibliografía y Anexos																								
Se estima un tiempo aproximado de 6 meses (24 semanas)																									

CAPÍTULO I

1. FUNDAMENTOS DE SEGURIDAD DE REDES

En el presente capítulo se presenta toda la fundamentación teórica, necesaria para el desarrollo del trabajo de grado en el cual se hablará acerca de las Redes de Datos, Segmentación de las Redes de Datos, la Seguridad Perimetral de las Redes de Datos, Firewalls, IPS e IDS y finalizaremos con las UTM; siendo estos los temas más relevantes dentro del marco teórico.

1.1. LAS REDES DE DATOS

Desde su creación, el ser humano ha buscado y encontrado la forma de comunicar todos sus pensamientos y necesidades hacia los demás, han transcurrido miles de años y la comunicación sigue latente entre sus principales necesidades; la tecnología que se ha generado en los últimos años ha concedido que las comunicaciones se las realice de una manera más rápida y eficaz alrededor del mundo; el desarrollo de las redes de comunicación de datos ha permitido que una persona pueda enviar y recibir información de un semejante ya sea desde una oficina contigua o del otro lado del mundo.

1.1.1. DEFINICIÓN DE REDES DE DATOS

La red de datos es aquella infraestructura en la que existe un conjunto de dispositivos de red que comparten recursos, estos dispositivos se encuentran interconectados físicamente puede ser por vía alámbrica o inalámbrica y que mediante reglas y protocolos de comunicación posibilitan la transmisión de información entre cada uno de sus usuarios, véase la Imagen 1.

IMAGEN 1.- *Red de datos*

Fuente: *http://www.sat-tecnologia.com/page-Redes+inform%C3%A1ticas-html*

1.1.2. DISPOSITIVOS DE UNA RED DE DATOS

El procedimiento al enviar un mensaje, un correo o navegar por el internet, es transparente para el usuario final, pero para que todo esto ocurra existen varios dispositivos que permiten que la comunicación entre los usuarios ocurra. Los dispositivos de red son todos aquellos equipos de hardware que se encuentran conectados a las diferentes redes y que permiten la transmisión de información entre todos los puntos de la red.

1.1.2.1. Servidor

Son equipos especializados en la compartición de recursos y servicios, poseen gran capacidad de almacenamiento y procesamiento debido a que por estos es posible que circule toda la información de la red. Existen varios tipos de servidores dependiendo su aplicación, servidores de correo, servidores de DNS[1], servidores web, entre los más comunes; y cada uno de los usuarios de la red puede acceder al servidor para utilizar los servicios alojados en éste, observe la Imagen 2.

IMAGEN 2.- *Servidor y su Representación en simulación*
Fuente: *Basado en www.solutekcolombia.com/servidores*

1.1.2.2. Firewall

El firewall o también llamado cortafuegos, es un elemento de hardware o software, Imagen 3, que se utiliza para controlar la información entrante o saliente de una red, dependiendo las políticas de seguridad que el administrador de red haya definido.

[1] DNS = Domain Name System, es el sistema que se utiliza para traducir los nombres de dominios en direcciones IP.

IMAGEN 3.- *Firewall y su Representación en simulación*
Fuente: *Basado en omnitechsupports.com/?p=1146 y*

1.1.2.3. Switch

O conmutador, es el dispositivo encargado de interconectar los segmentos de red, observe la Imagen 4, los Switchs trabajan en la capa 2 del modelo OSI, la transmisión de los datos lo hace de acuerdo a la dirección MAC[2] de destino de los datagramas de red. Cuando se utilizan los Switchs, se consigue unir en una sola red múltiples segmentos de red.

IMAGEN 4.- *Switch y su Representación en simulación*
Fuente: *Basado en santiago.olx.cl/switch-cisco-2960-iid-158208824*

1.1.2.4. Modem

El nombre se debe a las funciones que realiza el equipo, modular y demodular las señales electrónicas para ser transmitidas por las líneas telefónicas, esta señal se llama portadora y las funciones las realiza con una señal llamada moduladora. Imagen 5.

IMAGEN 5.- *Modem y su representación en simulación*
Fuente: *Basado en www.hostingyvirtualizacion.com/modem-adsl/*

[2] MAC = Media Access Control Identificador que poseen las tarjetas o dispositivos de red, este identificador es único a nivel mundial.

1.1.2.5. Router

También se lo llama enrutador, son dispositivos que se encarga de la interconexión de redes, estos equipos operan en la capa tres del modelo OSI, estos dispositivos permiten la comunicación de redes basadas en diferentes protocolos, Imagen 6.

IMAGEN 6.- *Router y su Representación en simulación*

Fuente: *Basado en www.solutekcolombia.com/venta_tecnología/routers_cisco/index.ftm*

1.1.2.6. Bridge

Son dispositivos que operan en la capa dos del modelo OSI, se utilizan para la segmentación de redes, y permite el paso de la información a al segmento de la red, de acuerdo a la dirección física de destino de cada paquete de datos. Estos dispositivos, operan bajo el mismo protocolo de red, véase la Imagen 7.

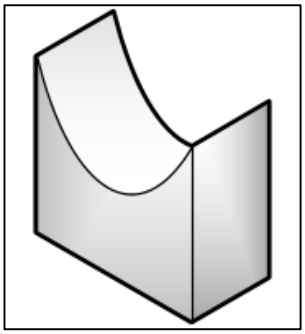


IMAGEN 7.- *Representación en simulación de un bridge*

Fuente: *Office 2013 Visio*

1.1.2.7. Hub

Los Hubs o concentradores, mostrado en la Imagen 8, son dispositivos con los cuales es posible ampliar las redes en cualquier tipo de topología, el número de equipos que se pueden interconectar dependerá del número de puertos de conexión posea. A diferencia del Switch, cuando el Hub recibe información, esta es enviada a todos los dispositivos conectados a él. Hoy no son muy utilizados debido a que se producen muchas colisiones de información en ellos.

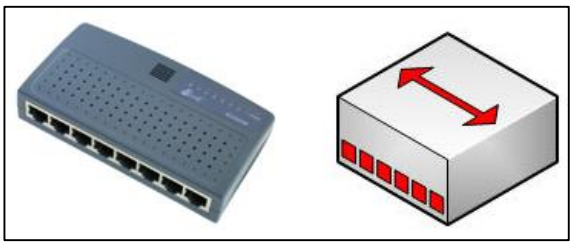


IMAGEN 8.- *Hub y su representación en simulación*
Fuente: *Basado en nestoranaya.blogspot.com/2012/02/dispositivos-de-interconexion-de-redes.html*

1.2. SEGMENTACIÓN DE LA RED DE DATOS

"Hoy en día la interconexión entre redes es más común de lo que parece, desde una simple conexión a internet, ya estamos sumergidos en un sin fin de conexiones, de las que muchas veces como usuarios ni nos damos cuenta de todo lo que acontece detrás de un simple cable de red. Precisamente para mantener un orden detrás de ese cable existe algo que permite la comunicación entre redes, que permite una mejor distribución de todos los datos que por allí viajan, permite un mejor manejo del ancho de banda utilizado por cada usuario en la red, a esa distribución la llamamos Segmentación de Redes." Caicedo N, Universidad Nueva Etapa.

1.2.1. DIRECCIONAMIENTO IP

Antes de entrar de lleno a la segmentación de las redes, se detallará una parte importante en las redes de datos, lo cual es el direccionamiento IP. La dirección IPv4 es el identificador único de un host o equipo dentro de una red, consta de 32 bits divididos en 4 octetos (grupo de 8 bits), en los que se indica el identificador de red y el identificador de host

1.2.1.1. Clases de redes

El direccionamiento IPv4 parte desde 0.0.0.0 hasta 255.255.255.255, es por ello que todo el pull de direcciones se ha divido en varias clases, y su uso dependerá del tamaño de la red y las aplicaciones a emplearse. Hay que tomar en cuenta que la red 0.X.X.X no es asignable debido a que esta designada por la IANA[3] para su identificación local; el pull de direcciones 127.X.X.X esta designado para la maquina propia conocido como loopback.

[3] IANA = Internet Assigned Numbers Authority, es el organismo de administrar las direcciones IP

- **Dirección IPv4 clase A**

En esta clase el primer octeto representa el identificador de red, y los tres octetos restantes representaran el número de hosts. El primer bit de la izquierda es el más importante, ya que este siempre estará seteado en 0.

IMAGEN 9.- Dirección IPv4 clase A
Fuente: http://es.kioskea.net/contents/267-direccion-ip

Se observa en la Imagen 9, que en el octeto de red solo quedan disponibles 7 bits, por lo tanto se tendrá 2^7 = 128 redes. Desde la 0.0.0.0 hasta la 126.255.255.255, pero con el análisis anterior se reduce a las redes 1.0.0.0 hasta la 126.255.255.255.

Para la parte de host se tiene libre los tres últimos octetos es por ello que se podrán tener hasta 2^{24} - 2 = 16 777 214 equipos conectados. Se restan dos direcciones IP por que representaran la IP de red y la IP de broadcast

- **Dirección IPv4 clase B**

En esta clase los dos primeros octetos representan el identificador de red, y los dos octetos restantes representaran el número de hosts. Los dos primeros bits de la izquierda son los más importantes, ya que estos siempre estarán seteados en 1 y 0 respectivamente.

IMAGEN 10.- *Dirección IPv4 clase B*
Fuente: *http://es.kioskea.net/contents/267-direccion-ip*

Se observa en la Imagen 10, que en los octetos de red quedan disponibles 14 bits, por lo tanto se tendrá 2^{14} = 16384 redes. Desde la 128.0.0.0 hasta la 191.255.255.255.

Para la parte de host se tiene libre los dos últimos octetos es por ello que se podrán tener hasta 2^{16} - 2 = 65 534 equipos conectados. Se restan dos direcciones IP por que representaran la IP de red y la IP de broadcast.

- **Dirección IPv4 clase C**

En esta clase los tres primeros octetos representan el identificador de red, y el último octeto restante representa el número de hosts. Los tres primeros bits de la izquierda son los más importantes, ya que estos siempre estará seteados en 1, 1 y 0 respectivamente.

IMAGEN 11.- *Dirección IPv4 clase C*
Fuente: *http://es.kioskea.net/contents/267-direccion-ip*

Se observa en la Imagen 11, que en los octetos de red quedan disponibles 21 bits, por lo tanto se tendrá 2^{21} = 2 097 152 redes. Desde la 192.0.0.0 hasta la 223.255.255.255.

Para la parte de host se tiene libre el último octeto es por ello que se podrán tener hasta 2^8 - 2 = 254 equipos conectados. Se restan dos direcciones IP por que representaran la IP de red y la IP de broadcast.

- **Dirección IPv4 clase D y clase E**

Estas clases de direcciones IPv4, son especiales por que no se utilizan para la asignación de red ni de host. El pull de direcciones clase D va desde 224.0.0.0 hasta 239.255.255.255 y son utilizadas para uso de multicast o multidifusión, en cambio el pull de direcciones clase E esta designado desde 240.0.0.0 hasta 255.255.255.255 y son utilizadas para uso experimental.

1.2.1.2. Máscara de red

La máscara de red es similar a la dirección IPv4, compuesta por 4 octetos de 8 bits, y nos sirve para delimitar e indicar el tamaño de la red y número de equipos y hosts de la misma. La formación de una máscara de red consiste en una secuencia de bits seteados en 1 y seguidos de una secuencia de bits seteados en 0, es por ello que los valores permitidos en cualquiera de los octetos de la máscara de red son: 0, 128, 192, 224, 240, 248, 252, 254 y 255.

En la Tabla 1, se muestra los diferentes pulls de direcciones IPv4, la máscara de red, el número de subredes y de host por cada subred.

TABLA 1.- *Clases de direccionamiento IPv4*

Clase	Direccionamiento	Máscara	N° Red	N° de host
A	1.0.0.0 – 126.255.255.255	255.0.0.0	126	16 777 214
B	128.0.0.0 – 191.255.255.255	255.255.0.0	16 384	65 534
C	192.0.0.0 – 223.255.255.255	255.255.255.0	2 097 152	254
D	224.0.0.0 – 239.255.255.255	Multicast o Multidifusión		
E	240.0.0.0 – 255.255.255.255	Experimentación		

Fuente: *Basado en investigación teórica y práctica*

1.2.1.3. Dirección IPv4 pública y dirección IPv4 privada

Las direcciones IPv4 públicas son aquellas direcciones que se utilizan para identificar un host, servicio o página web en la red global, Internet, y son únicas a nivel mundial. En cambio las direcciones IPv4 privadas son pulls de direcciones de clase A, B y C, que son orientadas para redes LAN, pueden ser utilizadas varias veces a nivel mundial, pero dentro de la intranet no deberá repetirse la IP.

Las direcciones IP privadas son las siguientes:

- ✓ De 10.0.0.0 hasta 10.255.255.255
- ✓ De 169.254.0.0 hasta 169.254.255.255
- ✓ De 172.16.0.0 hasta 172.31.255.255
- ✓ De 192.168.0.0 hasta 192.168.255.255

Las IPs que no consten dentro de estos rangos, clase D, clase E e IPs reservadas, serán IPs públicas.

1.2.2. FUNCIONES BÁSICAS DE UN SWITCH

Se había dado un concepto general del Switch, en esta ocasión se profundizará en las características y funciones que nos brinda este equipo de red, ya que es el encargado de realizar la conmutación de los paquetes para la comunicación en las redes actuales. El Switch es el encargado de encaminar los datos de un segmento de red a otro, rigiéndose a la dirección MAC de destino, cuando por uno de sus puertos ingresa paquetes de información, el Switch lee la dirección MAC destino y envía por el puerto al que pertenezca la MAC destino; además almacena esta dirección MAC en su memoria, para que en el futuro se realice de forma directa la transmisión de los datos.

Dentro del estudio de las funcionalidades y características básicas de un Switch, y que nos permitirá una correcta segmentación de red, se debe tomar en cuenta las siguientes.

1.2.2.1. STP (Spanning Tree Protocol)

Es un protocolo de la capa 2 del modelo OSI, y estandarizado por la IEEE[4] en 802.1d, la función de este protocolo es evitar la formación de bucles en la red debido a la presencia de enlaces redundantes. STP analiza en el Switch cuáles son las rutas lógicas por las que se puede enviar los paquetes de datos a un mismo destino, determina la mejor de estas rutas y bloquea a las demás; lo importante es que luego de haber bloqueado los puertos de las rutas lógicas que no se usarán, aun los sigue supervisando para que, en el momento de fallas por la ruta principal, éste se cierre y STP habilite el siguiente puerto que tenga las mejores prestaciones.

Para que STP elija la ruta lógica a seguir se basara en el costo de enlace, el costo es un valor que STP asigna al puerto del enlace entre Switchs; STP registra todas rutas posibles entre el emisor y receptor, y realiza la sumatoria de los costos en todas las rutas, y la ruta lógica con el menor costo será la principal las demás rutas serán las de redundancia.

1.2.2.2. VLAN (Virtual Local Area Network)

Cuando tenemos una LAN se aprecia que se ha formado una sola red física, con el uso de las VLANs se puede crear varias redes lógicas dentro de una misma red física, permitiendo así deslindarse de las limitaciones físicas.

Cuando se segmenta a la red mediante el uso de VLANs, es posible administrar de mejor manera las aplicaciones y servicios a los que debe acceder cada usuario de la red. Permite una mayor flexibilidad en la administración de la red, ya que si se desea que una estación de trabajo pertenezca a una VLAN, solo es necesario modificar el puerto del Switch al que está conectado.

[4] IEEE = Institute of Electrical and Electronic Enginers, Organismo internacional de estandarización

1.2.2.3. VTP (VLAN Trunking Protocol)

Este es un protocolo propietario de CISCO[5], el cual sirve para la administración y propagación de las VLAN en un entorno de red del mismo dominio VTP. Este protocolo permite crear, borrar y modificar las VLANs en un Switch principal y este replicara las VLANs creadas hacia todos los Switchs que se encuentren en la red.

VTP opera de tres diferentes maneras:

- **VTP Server**

En este modo se puede crear, modificar y borrar las VLANs que se necesitan en la red, el Switch que está configurado como servidor VTP se encargara de propagar toda la información concerniente a las VLANs hacia los demás Switchs clientes o transparentes. Cabe recalcar que en una red de datos debe existir un solo Switch configurado como servidor VTP.

- **VTP Cliente**

Las VLANs no se pueden crear, modificar ni borrar, solamente es capaz de recibir la información y replicarla hacia los demás Switchs.

- **VTP Transparente**

Cuando un Switch se configura en modo VTP transparente replica toda la información de las VLANs provenientes del servidor VTP; puede crear, modificar o borrar las VLANs pero esta información no será replicada solo se lo hará de forma local.

1.2.3. SWITCH CAPA 2, 3 Y 4

Dentro del mercado de comunicaciones existen varios tipos de Switch dependiendo de las aplicaciones y tamaño de la red que se va a instalar. La principal diferencia es la capa en la que pueden trabajar los Switchs.

1.2.3.1. Switch capa 2

Son los conmutadores más básicos y tradicionales, cuya función es de dividir a la red en varios dominios de colisión, son capaces de realizar varias transmisiones de datos sin interferir en los diferentes dominios de colisión, pero no pueden filtrar las difusiones de broadcast o multicast.

[5] CISCO = Empresa dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones

1.2.3.2. Switch capa 3

Estos Switchs a más de tener las prestaciones tradicionales de los Switchs capa 2 poseen algunas funciones de los Routers como por ejemplo soporte de los protocolos de enrutamiento, determinación del camino de transmisión basado en información de la capa de red, soportan enrutamiento entre VLANs evitando así el uso de un Router externo.

1.2.3.3. Switch capa 4

Son Switchs que últimamente están apareciendo en el mercado de las comunicaciones la principal característica de estos Switchs es que, a más de poseer las prestaciones de los Switch capa 2 y 3, se pueden implementar políticas y filtros de seguridad a partir de la información de la capa 4 o superiores del modelos OSI, logrando así filtrado para puertos SNMP[6], FTP[7], TFTP[8], etc.

1.3. SEGURIDAD PERIMETRAL

Las redes de comunicación de las empresas, corporaciones o campus universitarios al momento de conectarlas a la Internet han sido objeto de ataques de piratas cibernéticos, para acceder a la información o denegar los servicios que se presten dentro de la red. La seguridad de los datos que se cursan dentro, desde y hacia una red informática es la principal preocupación de un administrador de red, es por ello que se deben implementar métodos de seguridad para evitar ataques, intrusos e información que puedan alterar el correcto funcionamiento de la red, para ello está la seguridad perimetral de la red.

1.3.1. DEFINICIÓN DE LA SEGURIDAD PERIMETRAL DE RED DE DATOS

“La seguridad perimetral basa su filosofía en la protección de todo sistema informático de una empresa desde “fuera” es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático.
Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red”. Taboada, Eduardo. (2005).

La seguridad perimetral es un método de defensa de las redes informáticas, en el que consiste instalar equipos de comunicaciones en los que se establece las políticas de seguridad necesarias para su óptimo funcionamiento; estos equipos se los coloca entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red.

---

[6] SNMP = Simple Network Management Protocol, Protocolo que facilita el intercambio de información de administración entre dispositivos de red.
[7] FTP = File Transfer Protocol, Protocolo que permite la transferencia de archivos en la red.
[8] TFTP = Trivial File Transfer Protocol, Protocolo de transferencia de archivos más simple que FTP

1.3.2. OBJETIVOS DE LA SEGURIDAD PERIMETRAL DE RED DE DATOS

La implementación de un sistema de seguridad perimetral ayuda a la protección de la red contra los ataques internos y externos de la misma, pero para ello se han planteado los siguientes objetivos que debe cumplir este sistema:

- ✓ Proporcionar mayor productividad a los usuarios de la red interna, permitiendo acceder y visitar sitios seguros en la Internet y además que se asocien al ambiente laboral y no al de entretenimientos y esparcimiento.
- ✓ Proteger los equipos de red y host debido que la mayoría de las amenazas provienen de la Internet, efecto de cómo interactúan los usuarios con la misma.
- ✓ Detectar los equipos con presencia de virus y usuarios que están usando programas maliciosos
- ✓ Optimizar el uso de la Internet para el trabajo de los usuarios de la red, administrando su capacidad y velocidad para cada uno de ellos.
- ✓ Simplificar la conectividad segura hacia la red desde sucursales vía VPN[9].

1.3.3. REQUISITOS DE LA SEGURIDAD PERIMETRAL DE RED DE DATOS

Según Mora, María Esperanza “Una técnica de seguridad informática es un mecanismo o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático”, por lo tanto los requisitos que se deben cumplir en un sistema de seguridad perimetral, a más de los que se señalan en la cita, son los siguientes: identificación, autenticación, control de acceso, y responsabilidad.

1.3.3.1. Identificación

Se denomina identificación al momento en que el usuario se da a conocer al sistema.

1.3.3.2. Autenticación

Es la verificación de que el individuo que se ha identificado al sistema, es seguro.

1.3.3.3. Control de Acceso

Es la administración correcta de los usuarios que acceden a los servicios de una red, mientras que a los usuarios seguros se les da el acceso necesario a los usuarios maliciosos se les deniega el acceso.

[9] VPN = Virtual Private Network, Son redes virtuales para la interconexión de redes privadas.

1.3.3.4. Disponibilidad

Se refiere que los servicios que se ofrecen dentro de la red, estén operativos el 100% del tiempo, y en caso de fallas tengan una tiempo de recuperación rápida.

1.3.3.5. Confidencialidad

Trata sobre la protección de la información que los usuarios seguros cursan dentro de la red de datos ante usuarios no autorizados.

1.3.3.6. Integridad

Es la protección de los datos y transmisiones contra las alteraciones no autorizadas o accidentales que puedan ocurrir dentro de la red.

1.3.3.7. Responsabilidad

Es realizar un seguimiento y almacenamiento de todas las actividades seguras, accidentales y no autorizadas que se den dentro de la red, tanto por los usuarios seguros como usuarios maliciosos

1.3.4. ATAQUES O AMENAZAS INFORMÁTICAS

Los ataques o amenazas son todo aquel programa o individuo que ingresa a la red con el fin de dañar el correcto funcionamiento de los servicios que se brindan en la misma. Desde inicios de la Internet han existido personas dedicadas a encontrar las vulnerabilidades y debilidades de las redes de datos a nivel mundial para poder acceder a toda la información de las mismas, además existen programas maliciosos que se aprovechan de dichas vulnerabilidades para dañar la información y equipos de la red.

1.3.4.1. Formas de atacar a una red de datos

Para atacar a una red existen varias formas, dependiendo de la finalidad del ataque, las cuales describimos a continuación.

- **Ataques de Interrupción**

El objetivo principal de este ataque es deshabilitar los servicios que se estén brindando en la red; al momento de que se produce el ataque y queda inutilizado el servicio, es detectado por el administrador de la red.

- **Ataques de Modificación**

Cuando un atacante ha logrado acceder a los recursos de una red, modifica un documento o archivo de un servicio para obtener información o a su vez para dejarlo inutilizable.

- **Ataques de Acceso**

Son ataques que lo único que se desea es acceder a los servicios que se brindan en la red, un claro ejemplo es acceder a una red protegida para utilizar el internet que se brinda en ella.

- **Ataques de Falsificación**

Consiste en suplantar la identidad de un usuario seguro, para acceder a los documentos o archivos de los servicios privados de la red.

1.3.4.2. Tipos de amenazas

Las amenazas que afectan a las redes de datos provienen de cualquier lugar, desde personas curiosas o especializadas en ciencias computacionales hasta programas informáticos que se propagan en la Internet.
A continuación se enumera los tipos de amenazas que existen en la red:

- **Hackers**

Son personas altamente capacitadas que acceden a las redes privadas, con la finalidad de encontrar las vulnerabilidades, generalmente son personas que no realizan daños en la red.

- **Crackers**

Son de características similares a los Hackers, pero se diferencian en que el principal objetivo es dañar los servicios de la red, pueden realizarlo por voluntad propia pero la mayoría de veces lo hacen con fines de lucro.

- **Men in the Middle**

También conocido como JANUS, consiste en que el atacante de la red recepta la información entre dos puntos de la red, es capaz de leerla, y modificarla a voluntad sin que los puntos de la red se den cuenta del ataque.

- **Fuerza bruta**

Consiste en acceder a los servicios de red protegidos, y para ello adivina la contraseña ingresando todas las posibilidades de la misma hasta conseguirlo.

- **Ingeniería Social**

Los atacantes que usan la ingeniería social, utilizan su don de gente para convencer a los usuarios seguros que le brinden información privada, y así poder acceder a la red y atacarla.

- **Spam**

Este ataque consiste en enviar correos no deseados o correo basura de forma masiva a todos los usuarios de la red, los cuales tienen contenido malicioso o información basura.

- **Denegación de servicios**

Consiste en atacar un servicio de la red, de tal modo que éste quede inhabilitado.

- **Malware**

Software que fue creado con la única intención de dañar los servicios y equipos de red.

- **Virus**

Son programas informáticos creados para dañar los computadores del usuario final, los virus trabajan de forma transparente para el usuario y además tiene la capacidad de reproducirse, quiere decir puede propagarse hacia otros ordenadores sin abandonar el ya infectado.

- **Gusanos**

Son malware que tienen la capacidad de duplicarse por sí mismos, generalmente, la diferencia con los virus es que no necesitan archivos anfitriones para sobrevivir y se propagan por redes locales o por correo electrónico.

- **Adware**

Son programas informáticos que se instala en el computador sin que el usuario lo note, tienen la capacidad de descargar y mostrarle al usuario anuncios publicitarios.

- **Botnets**

Son malware que poseen códigos maliciosos, los cuales al momento de infectar un dispositivo, éste se vuelve un robot y puede ser controlado por el atacante de la red.

- **Phishing**

Consiste en el robo de información personal o empresarial del usuario, esto se realiza mediante la falsificación de información de un usuario seguro o de confianza.

- **Rogue**

Es una aplicación que simula ser un anti-malware, pero realiza exactamente lo contrario buscar en la red malware e instalarlo.

- **Spyware**

Son programas que se especializan en recopilar toda la información del usuario, sin el consentimiento del mismo. Generalmente se utiliza para la obtención de contraseñas del usuario.

- **Troyanos**

Son aplicaciones que simulan ser seguros, logrando así que el usuario ejecute estas aplicaciones y así poder instalarse en el sistema. A diferencia de los virus y gusanos, los troyanos no pueden propagarse por sí solos.

- **Spoofing**

Son ataques en los que se utiliza la suplantación de identidad para poder acceder a los diferentes servicios de la red.

1.3.5. MODELOS DE SEGURIDAD INFORMÁTICA

"Un modelo de seguridad es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información. Al decir formal queremos expresar que estará redactado fundamentalmente en términos técnicos y matemáticos" Aguilera, Purificación (2010)
Existen varios modelos de seguridad, dependiendo las funciones y operaciones que se empleen en él. Los modelos de seguridad los podemos clasificar en tres grandes grupos:

1.3.5.1. Modelo de la matriz de acceso

En este modelo se definen tres elementos: sujeto, objeto y tipo de acceso. Consiste en que a un sujeto tiene acceso total o parcial a un objeto del sistema o un sujeto no tiene acceso a un objeto u objetos del sistema.

1.3.5.2. Modelo de acceso basado en funciones de control

Es muy similar a la matriz de acceso, pero en este caso no se define el acceso por quien es el sujeto sino porque función cumple el sujeto en el sistema, un sujeto puede ser usuario de un servicio y puede ser administrador de otro servicio en la misma red; para el primer servicio podrá tener acceso parcial y para el otro acceso total.

1.3.5.3. Modelo de multinivel

"Se basa en la jerarquía de los datos. Los usuarios tendrán acceso a un nivel u otro de la jerarquía en función de las autorizaciones que les hayan sido dadas." Aguilera, Purificación (2010)

El modelo de seguridad a emplearse será mediante la Matriz de acceso ya que se definirá las subredes como el sujeto, los servicios de la red como objeto y se establecerá el tipo de acceso en este caso permitir o denegar.

1.3.6. POLÍTICAS DE SEGURIDAD

"Es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema." Huerta, Antonio (2002)

Las políticas de seguridad son las normas que deben cumplir los sistemas de seguridad en las acciones del personal que trabaje en la empresa o tenga acceso a la red. Las políticas de seguridad deben de cumplir los objetivos de la seguridad: **Identificación**, **Autenticación**, **Control de Acceso**, **Disponibilidad**, **Confidencialidad**, **Integridad** y **Responsabilidad.**

Las políticas de seguridad deben estar enfocadas en 3 aspectos: Los equipos que soportan, la información a proteger y los usuarios que acceden a ella; sujeto, objeto y tipo de acceso, método de la matriz de acceso.

Para establecer cuáles serán las políticas de seguridad se debe cumplir con un esquema sistematizado[10]:

- ✓ Identificar los recursos de la organización
- ✓ Definir los riesgos
- ✓ Definir la administración de los recursos informáticos
- ✓ Definir el acceso sobre los recursos informáticos
- ✓ Definir los procesos que se usaran para la autenticación
- ✓ Definir clara y detalladamente, que constituye el uso apropiado o no de los medios de comunicación electrónicos y servicios de la compañía
- ✓ Definir claramente, que clase de información puede ser accedida y distribuida por y que medios
- ✓ Definir, que controles van a ser colocados
- ✓ Notificar a los usuarios de los procedimientos de auditoria, monitoreo, revelación de la información y las consecuencias del incumplimiento

[10] Esquema tomado de "Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors, utilizando tecnología UTM (Unified Threat Management)" Alulema, Diana; 2008

- ✓ Identificar a aquellos responsables de la ejecución de seguridad y cómo las políticas y procedimientos se harán seguir
- ✓ Desarrollar los pasos a seguir ante un evento de incumplimiento de la política, una brecha de seguridad o un desastre.

1.3.7. TECNOLOGÍAS DE SEGURIDAD DE LA INFORMACIÓN

Son las herramientas que se emplean para brindar la seguridad necesaria a los servicios de la red, cumpliendo con los objetivos y las políticas de seguridad. En el mercado existen varios métodos de seguridad que son:

1.3.7.1. Firewalls

Son dispositivos de software o hardware en el que pasa todo el tráfico de entrada y salida de la red, y dependiendo de las políticas de seguridad se encarga de denegar o permitir el paso de la información.

1.3.7.2. Administración de cuentas

La encriptación es una manera Es el medio en que todos los usuarios seguros, tienen su usuario y contraseña para acceder a los recursos de la red, este tipo de seguridad es muy susceptible a la ingeniería social.

1.3.7.3. Detección y prevención de intrusos

Es el método de detección de intrusos es aquel que detecta al usuario o usuarios que ingresan de forma no autorizada a la red, y el método de prevención de intrusos evita que accedan usuarios no autorizados a la red, en caso de que esto suceda bloquea al host que sea detectado como intruso.

1.8.7.4. Antivirus

Son programas informáticos que se especializan en la detección y eliminación de malware que puede existir dentro de un equipo o host, aunque son muy efectivos para determinados malware, no todos los antivirus pueden eliminarlos por completo.

1.3.7.5. Biometría

Es un método de identificación de usuarios muy efectivo, debido a que las claves para poder ingresar generalmente son huellas dactilares, retina de los ojos o la voz, y estos son únicos de cada persona. Es un método muy seguro para la autenticación de usuarios.

1.3.7.6. Encriptación

de codificar la información para evitar que pueda ser leída por terceros, los únicos que saben las contraseñas para encriptar y desencriptar son el emisor y receptor.

1.3.7.7. Acceso remoto

Este método sirve para poder acceder a hosts y servicios desde cualquier parte dentro y fuera de la red, de manera segura debido a que solo quien conozca la contraseña podrá ingresar al servidor de acceso remoto.

1.3.7.8. Firma digital

Son esquemas matemáticos que se envían junto a un archivo o documento, el cual permite demostrar la autenticidad y seguridad del emisor.

1.3.7.9. VPN

Las Virtual Private Network o Redes Privadas Virtuales, permiten realizar una conexión segura entre dos puntos de la red, pero geográficamente distantes, este túnel virtual se encuentra en la Internet, pero solo podrá accederse entre los puntos que se realice la VPN.

1.3.8. NIVELES DE SEGURIDAD

Dependiendo las características de la red, de los equipos y de la seguridad que posee la red; puede clasificarse en un nivel el cual califica si nuestra red es segura o no. La seguridad de la red puede estar clasificada de la siguiente forma.

1.3.8.1. Nivel de seguridad D

Es el nivel más bajo de seguridad, indica que no posee seguridad alguna y que el sistema completo no es confiable. No existe seguridad respecto a hardware, los sistemas operativos se ven comprometidos fácilmente y no posee autenticación para usuarios.

1.3.8.2. Nivel de seguridad C1

Es un sistema de seguridad discrecional. El hardware posee limitada seguridad y los usuarios deben acceder a los servicios con su usuario y contraseña.

1.3.8.3. Nivel de seguridad C2

Resuelve los inconvenientes de los anteriores niveles de seguridad, además de poseer las características del nivel de seguridad C1, tiene la capacidad de controlar a los usuarios dependiendo el nivel de autorización que posea cada uno. Además este nivel de seguridad exige que se realice una auditoria por cada evento que suceda en el sistema.

1.3.8.4. Nivel de seguridad B1

Este nivel es llamado nivel de Protección de Seguridad Equitativa, debido a que posee seguridad multinivel, como información secreta e información ultra-secreta.

1.3.8.5. Nivel de seguridad B2

Es conocido como Protección Estructurada, es necesario que todos los objetos de la red se encuentren correctamente etiquetados.

1.3.8.6. Nivel de seguridad B3

Se llama también Dominios de Seguridad, refuerza todos los dominios con la instalación de hardware adicional. Además existe un monitor de usuarios, y este es quien acepta o deniega el acceso a los servicios dependiendo de las políticas establecidas.

1.3.8.7. Nivel de seguridad A

Es el nivel más alto de seguridad, para poder tener este nivel de seguridad debe de emplearse todos los niveles anteriores. Tanto el software como el hardware poseen las seguridades necesarias contra usuarios no autorizados.

1.4. FIREWALL

Las grandes y pequeñas empresas, las universidades y cualquier red que sea conectada deben estar protegidas contra los ataques de usuarios maliciosos que estén dentro y fuera de la red, es por eso que los firewalls son una herramienta esencial en la seguridad de redes informáticas.

1.4.1. DEFINICIÓN DE UN FIREWALL

La Microsoft lo define como: “Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.” Imagen 12.

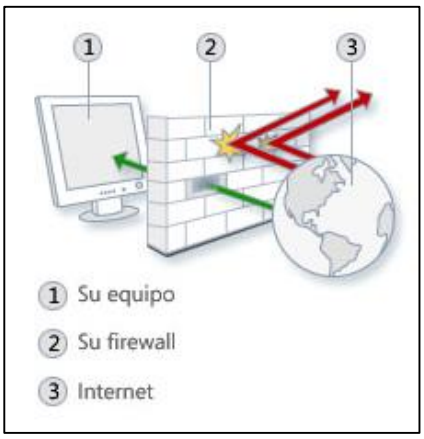


IMAGEN 12.- *Representación de Firewall*

Fuente: *http://windows.microsoft.com/es-xl/windows7/what-is-a-firewall*

1.4.2. MODELOS DE FIREWALLS

Dependiendo del tipo de filtrado que realizan, los firewalls se clasifican en:

1.4.2.1. Firewalls de filtrado de paquetes o a nivel de red

Son firewalls que analizan la información contenida en la cabecera de los paquetes de datos, y así decidir si el paquete accede a la red local o no. La información analizada es la IP origen, la IP destino, tipo de paquete el número de puerto de la aplicación origen y destino, en la Tabla 2 se muestra reglas de seguridad configuradas en un firewall.

TABLA 2.- Ejemplo de reglas de Firewall

N° Regla	Acción	IP Origen	IP Destino	Protocolo	Puerto
1	Denegar	192.168.1.20	190.95.196.211	udp	22
2	Aceptar	192.168.1.0/24	190.95.196.211	udp	22
3	Negar	Any	any	any	Any

Fuente: *Firewall de la Universidad Técnica del Norte*

1.4.2.2. Servidores Proxys o firewalls a nivel de aplicación

Son firewalls que filtran las aplicaciones, es decir trabaja en la capa 7 del modelo OSI a diferencia del filtrado de paquetes que trabaja en la capa 4. Cabe mencionar que se debe conocer el puerto de cada una de las aplicaciones que se quiera controlar.

1.4.3. ARQUITECTURAS DE FIREWALLS

Consiste en las diferentes formas en que se pueden utilizar y configurar los equipos destinados a formar parte del firewall

1.4.3.1. Dual-Homed Host

Esta arquitectura es muy simple, el equipo Dual-Homed Host se conecta entre la red a proteger y la red externa; y en este equipo se configurará todas las políticas del firewall a emplearse

1.4.3.2. Screened Host

Se utiliza dos equipos para esta arquitectura, un enrutador que permite conectar las redes internas y externas, pero se configura el filtrado de paquetes para que las redes no se conecten directamente. Y un host que se encuentra en la red interna el cual es el único que recibirá las conexiones externas luego de haber sido filtrados por el Router (Screened Host).

1.4.3.3. Screened Router

El único equipo encargado de la seguridad será el Router que se coloca entre la red interna y externa, este equipo a más del filtrado de paquetes permite realizar un enrutamiento selectivo el cual permite o bloquea los paquetes.

1.4.3.4. Screened Subnet

Esta arquitectura consiste en colocar una subred entre la red interna y la red externa, esta subred se la conoce como DMZ. Para garantizar la máxima seguridad se coloca Screened Host en los límites de la DMZ hacia la red interna y la red externa.
El firewall a implementarse en la red de la Universidad Técnica del Norte pertenece a la arquitectura Screened Subnet ya que la red universitaria posee una DMZ.

1.4.4. TIPOS DE FIREWALLS EXISTENTES EN EL MERCADO

La seguridad informática hoy en día es muy importante para las redes de comunicación, es por eso que existen empresas especializadas en brindar este tipo de servicio, y para ello se ha generado dos tipos de firewalls.

1.4.4.1. Firewall de software

Son programas informáticos destinados a la protección de los equipos, este software monitorea el tráfico entrante y bloquean ataques maliciosos provenientes de la red a la que se encuentran conectados. Son fáciles de usar e instalar en los equipos a monitorear, existen dos versiones de firewalls gratuitos y comerciales.

1.4.4.2. Firewall de hardware

Son equipos físicos destinados a la protección de una LAN, poseen características de procesamiento de gran capacidad debido a la gran cantidad de tráfico que debe analizar para permitir o denegar el acceso de un paquete de datos a la red. La instalación de estos firewalls son mucho más complicadas que los firewalls de software y generalmente lo realiza personal capacitado.

1.4.5. FIREWALL BAJO PLATAFORMA DE SOFTWARE LIBRE

Un método para la implementación de un firewall, es mediante el uso de Software Libre, lo que permite que los costos de instalación y licencias se reduzcan significativamente, y para ello existen las IP-tables en Linux.

1.4.5.1. Las IP-Tables

Es un sistema de firewall vinculado al kernel de Linux, que permite al administrador de la red digitar las reglas que analizarán los paquetes de datos que ingresan, salen o pasan por nuestra red, para el direccionamiento IPv4. Para el direccionamiento IPv6 se llaman IP6tables. Para crear las reglas de las IP-tables que analizaran los paquetes se analiza varios aspectos.

- **Camino del paquete de datos**

Se refiere a si el paquete entra, sale o pasa por la red.
INPUT = Entra a la red
OUTPUT = Sale de la red
FORWARDING = Pasa por la red

- **Interfaz por la que entra o sale el paquete de datos**

Se debe especificar la interfaz por la que se analizara el tráfico de paquetes, pueden ser:
eth0 = Tarjeta Ethernet
wlan0 = Tarjeta Inalámbrica

- **IP de origen y destino del paquete**

Puede definirse una IP de un host específico o de un rango de direcciones IP.

- **Protocolo de paquetes**

Se debe de indicar el protocolo que se analizará en la transmisión de datos, los cuales pueden ser TCP, UDP, ICMP[11], etc.

- **NAT**

Para realizar el nateo de direcciones se puede hacer de dos diferentes formas.

PREROUTING = Nateo antes de realizar el enrutamiento
POSTROUTING = Nateo después de realizar el enrutamiento

Un ejemplo de la línea de IP-table es el siguiente:

Iptables -A INPUT -s 172.20.0.0/16 -p tcp --dport 3128 -j ACCEPT

1.4.6. DISEÑO DE SISTEMAS FIREWALL

Para un diseño correcto del firewall se debe analizar conscientemente los servicios que se necesitan proteger dentro de una red, además saber a qué usuarios dentro y fuera de la red se les permitirá el acceso a dichos servicios, todas estas necesidades se las especificará en las políticas de seguridad.
Cabe recalcar que existen dos políticas para la configuración de un firewall que hay que tomar en cuenta. La primera **todo lo que no es específicamente negado se permite**, ésta política es poco segura ya que permite el acceso a usuarios no autorizados debido a que no se niega su petición en las reglas del firewall. La segunda política es **todo lo que no es específicamente permitido se niega**, esta es la más segura ya que depende del administrador de la red establecer a quienes se brindará el acceso a los diferentes servicios de la red, y lo que no se configure como permitido simplemente no logrará tener los servicios.

[11] ICMP = Internet Control Message Protocol, protocolo de control y notificación de errores

1.5*. IPS*

Otra de las tecnologías hoy por hoy usadas son los IPS también llamados Sistema de Prevención de Intrusos.

1.5.1. DEFINICIÓN DE UN IPS

Es un sistema de protección de la red diseñado para evitar los ataques maliciosos a la red, a diferencia con los IDS que solo identificaba y alertaba de los ataques y usuarios malignos.

1.5.1. TIPOS DE IPS

Al igual que en los IDS, existen varios tipos de sistemas de prevención de intrusos.

1.5.1.1. NIPS

Son sistemas de prevención de intrusos a nivel de red, los cuales buscan todos los ataques que se produzcan hacia la red y los bloquea.

1.5.1.2. WIPS

Wireless IPS, su funcionamiento es idéntico al de las NIPS con la diferencia que éstas controlan la seguridad de una red inalámbrica, cuando encuentra un usuario maligno lo bloquea para que no realice daños a la red.

1.5.1.2. HIPS

Son IPS basados en Host, su funcionamiento es observar todos los eventos que ocurran en el host que se haya instalado e indicar si el comportamiento del host es una amenaza o no.

1.5.2. CARACTERÍSTICAS DE LOS IPS

Las características que deben cumplir los IPS son:

- ✓ Identificar, registrar, bloquear e informar las actividades maliciosas en la red.
- ✓ Debe ser continuamente operativo, y en caso de fallas debe levantar el servicio automáticamente.
- ✓ Actualizar los filtros conforme detecta ataques.
- ✓ 100% efectivo, no debe ser fácil de engañar.
- ✓ Debe ser capaz de generar reportes periódicamente para el análisis de la red.

1.5.3. VENTAJAS Y DESVENTAJAS DE LOS IPS

A continuación se describe algunas de las ventajas y desventajas que poseen los IPS.

1.5.3.1. Ventajas

- ✓ Maximiza la seguridad, ya que no solo detecta sino que bloquea los ataques.
- ✓ Es una defensa completa contra los ataques de diferente tipo.
- ✓ Su configuración e instalación es muy fácil, con los conocimientos necesarios del administrador.
- ✓ Escalable con el crecimiento de la red que protege.
- ✓ Requiere menos control por parte del administrador en comparación con los IDS.

1.5.3.2. Desventajas

- ✓ La mala configuración de un IPS, puede añadir latencia a la red.
- ✓ Si el listado de firmas no se actualiza, puede ser víctima de nuevos ataques o malware generados recientemente.

1.5.4. FORMAS DE DETECTAR INTRUSOS

La detección de los intrusos o tráfico malicioso se la puede realizar de diferentes formas.

1.5.4.1. Detección basada en firmas

Charalampos, Zois dice “Esta detección se basa en una seria de reglas o firmas establecidas para reconocer a un determinado conjunto de posibles amenazas o ataques. Sin embargo como este tipo de detección funciona parecido a un Antivirus el administrador de la red debe verificar que las firmas estén constantemente actualizadas”.

1.5.4.2. Detección basada en políticas

“En este tipo de detección el IPS requiere que se declaren muy específicamente las políticas de seguridad.” Charalampos, Zois.

1.5.4.3. Detección basada en anomalías

En este modo de detección encontramos dos formas de hacerlo.

- **Detección estadística de anormalidades**

En este tipo de detección, el IPS analiza el tráfico de la red por un determinado tiempo, así crea su patrón de seguridad, en el momento que el tráfico de la red no coincida con el patrón

de seguridad, el IPS generará una alarma y bloqueara al usuario que genere ese tráfico de datos.

- **Detección no estadística de anormalidades**

Tiene el mismo funcionamiento que la detección estadística, salvo que en este método el administrador es quien determina el patrón de seguridad para la comparación.

1.5.4.4. Detección por Honey Pot

En la red se instala una Honey Pot, la cual se encarga de atraer a los atacantes y usuarios maliciosos; en el momento que realicen su cometido el IPS guarda ésta información para su base de datos logrando así bloquearlos antes de que ataque a la red.

1.6. UTM (UNIFIED THREAT MANAGEMENT)

Para el funcionamiento de un sistema de seguridad perimetral, es necesario la implementación de varios sistemas de control de los diferentes servicios que se prestan en la red, firewalls, proxys, anti-spam, entre otros. Por ello que la administración de todos estos sistemas se las debe centralizar y la gestión de amenazas unificadas es una excelente opción.

1.6.1. DEFINICIÓN DE UTM

Cameron, Voodberg, Giecco, Berhard & Quinn (2010) afirman que “UTM o Gestión de Amenazas Unificadas es un conjunto de características diseñadas para proporcionar la inspección de capa de aplicación, del tráfico que atraviesa una red. Al igual que en la detección y prevención de intrusiones (IDP por sus siglas en inglés), los dispositivos de seguridad que admiten características UTM descifran e inspeccionan los protocolos de capa superior para detectar tráfico malicioso o simplemente no reconocido.” Imagen 13.

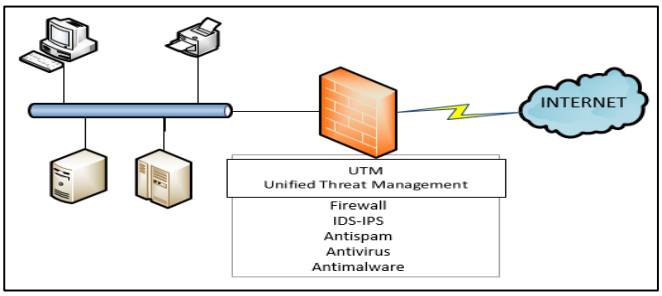


IMAGEN 13.- *Ubicación del UTM*

Fuente*: Basado en http//searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security*

1.6.2. CARACTERÍSTICAS DE UTM

Las principales características que debe tener y cumplir el Gestor de Amenazas Unificadas son:

- ✓ Cumplir con las funciones de un Firewall
- ✓ Filtrar correo, antispam
- ✓ Detección y bloqueo de malwares
- ✓ Filtrar contenido WEB y URL
- ✓ Prevención y Detección de Intrusos, IDS e IPS
- ✓ Soporte de VPN y SSL[12]

Gracias a la gran escalabilidad que posee el sistema UTM, el progreso de las tecnologías de seguridad han llevado a los Gestores de Amenazas Unificadas a un nuevo nivel conocido como XTM o Extensible Threat Management que es la nueva generación en gestores de amenazas. Los XTM a más de tener las funciones y características básicas de los UTM desarrollan nuevas aplicabilidades de seguridad, entre las que se puede destacar:

- ✓ Implementación de seguridad en mensajería
- ✓ Prevención de pérdida de datos
- ✓ Gestión centralizada mediante interfaces gráficas
- ✓ Autenticación de usuarios de la red automáticamente
- ✓ Monitorización de los eventos de la red

1.6.3. VENTAJAS DEL UTM

La implementación de un sistema centralizado de seguridad como lo es el UTM, tiene muchas ventajas descritas a continuación:

- **Complejidad reducida**

Como UTM es una mescla de todos los productos, esto simplifica la selección de productos, la integración de los productos y el continuo apoyo hacia los mismos.

[12] SSL = Secure Cockets Layer o Capa de conexión segura es un protocolo criptográfico que proporciona comunicaciones seguras.

- **Facilidad de implementación**

Los productos de la UTM pueden ser fácilmente instalados y mantenidos. Todos estos productos se pueden acceder a través de sistemas remotos.

- **Flexibilidad**

UTM es flexible, con grandes y centralizados firewalls basados en software.

- **Mínima interacción del operador**

UTM reduce los casos de llamadas de auxilio del sistema y mejora la seguridad. Se utiliza un enfoque de caja negra para limitar el daño relacionado con los dispositivos de red.

- **Facilidad en la solución de problemas**

Cuando la caja negra deja de funcionar, UTM los envían fuera de su sistema para que una persona solucione los problemas. Esto lo puede hacer incluso una persona no técnica; este enfoque es mucho más útil para sistemas remotos.

1.6.4. PARAVIRTUALIZACIÓN

Consiste en simular sistemas operativos sobre otro sistema operativo que funciona como hipervisor permitiendo lograr la virtualización. En la Paravirtualización cada sistema funcionara como máquina virtual y se comportaran como un equipo independiente con la característica que compartirán los recursos del host anfitrión, como tarjeta de red, discos duros, memorias RAM[13], etc.; en la Imagen 14 se muestra el esquema de la paravirtualización.

IMAGEN 14.- *Esquema de paravirtualización*
Fuente: *http://www.baitic.com/tag/paravirtualizacion*

[13] RAM = Random Access Memory, memoria del ordenador a la que se puede acceder aleatoriamente.

1.6.4.1. Hypervisor

El hypervisor es el supervisor de los recursos del host anfitrión para todas las máquinas virtuales de cada sistema a implementarse en el equipo de red. Cumple varias funciones dentro del host anfitrión que son:

- ✓ Planificación del tiempo de utilización del CPU por cada sistema huésped.
- ✓ Protección de la memoria a utilizarse entre las máquinas virtuales.
- ✓ Encaminamiento de interrupciones.
- ✓ Mantenimiento del tiempo.
- ✓ Paso de los mensajes entre máquinas virtuales.

1.6.4.2. Ventajas de la paravirtualización

Al momento de paravirtualizar los servicios de la red, logramos optimizar recursos, y se obtienen grandes ventajas:

- ✓ Mejorar el rendimiento de los dispositivos del host anfitrión como dispositivos de entrada-salida, CPU, memorias.
- ✓ Los sistemas operativos, tanto el anfitrión como huéspedes, se comunican directamente con los recursos físicos del equipo.
- ✓ Reduce la carga del procesador significativamente en comparación con la virtualización.

1.6.4.3. Desventaja de la paravirtualización

Cuando se centraliza los servicios mediante paravirtualización generalmente no se tienen dificultades salvo unas cuantas:

- ✓ El equipo anfitrión debe ser de grandes capacidades con respecto a procesamiento y almacenamiento de datos.
- ✓ Los sistemas operativos deben de ser modificables.

1.6.5. SOLUCIONES COMERCIALES DE PARAVIRTUALIZACIÓN

La paravirtualización se encuentra en desarrollo global, ya que todas las empresas dedicadas a las tecnologías de la información se encuentran generando aplicaciones que permitan explotar toda la aplicabilidad de la paravirtualización.

Dependiendo la plataforma de sistema operativo, propietario o software libre, se tienen varios software que permiten la paravirtualización, a continuación se describe brevemente el mejor y más utilizado para cada una de las plataformas.

1.6.5.1. Sin Plataforma

La aplicación vSphere/ESX(i) de la licencia de máquinas virtuales WMware, es el hypervisor más extendido y comercializado entre todos debido a que funciona bajo cualquier plataforma de sistema operativo.

1.6.5.2. Microsoft

Esta empresa ha lanzado su propio hypervisor conocido como Hyper-V, su última versión es el Hyper-V Server 2008 R2 el cual no cumple las mismas funciones que el hypervisor de WMware, es por eso que aún no es considerado como un hypervisor que garantice la paravirtualización.

1.6.5.3. Linux

Xen y XenServer son las versiones de hypervisores para plataformas de software libre, el cual posee muchas de las características del WMware aunque aún tiene inconvenientes en la compatibilidad con el tipo de hardware empleado. La diferencia entre Xen y XenServer es que, la primera es un parche que se aplica al kernel del sistema operativo, Linux, el cual hay que configurar para su funcionamiento; y la segunda opción se puede descargar como ISO el cual viene con el instalador integrado y de esta forma instalarlo y comenzar a funcionar inmediatamente, cabe destacar que XenServer requiere licencia para cada servicio que se instale en el host anfitrión.

CAPÍTULO II

2. ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED INFORMÁTICA

En el presente capítulo se describe la situación actual de la red informática de la Universidad Técnica del Norte, en el que se detallará las topologías lógicas y físicas de cada uno de los edificios que pertenecen al establecimiento, así como los equipos de red existentes para la comunicación y el servidor firewall que posee la institución. Además se realizará el estudio de los resultados obtenidos en el trabajo de titulación HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA “UNIVERSIDAD TÉCNICA DEL NORTE” realizado por la Ing. Tatiana Vinueza, para la obtención de las políticas de seguridad necesarias en la red.

2.1. UNIVERSIDAD TÉCNICA DEL NORTE

Naranjo, Miguel “La Universidad Técnica del Norte, es una joven institución de educación superior que desarrolla su labor académica e investigativa, para contribuir y auspiciar el desarrollo del país y de manera especial de la zona UNO del Ecuador (Imbabura, Carchi, Esmeraldas y Sucumbíos)”.

2.2.1. DESCRIPCIÓN FÍSICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE

La casona universitaria se encuentra en el sector El Olivo, Av. 17 de julio 5-21, Fig. 21, ésta posee una infraestructura física de calidad y cuenta con diferentes dependencias en todos los edificios, los cuales tenemos: Edificio Central, Facultad de Ingeniería en Ciencias Aplicadas (FICA), Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales (FICAYA), Facultad de Ciencias Administrativas y Económicas (FACAE), Facultad de Educación Ciencia y Tecnología (FECYT), Facultad de Ciencias de la Salud (FCCSS), Biblioteca, Auditorio Agustín Cueva, Centro Académico de Idiomas (CAI), Instituto de Postgrado y Coliseo, Colegio Anexo Universitario, Hospital Antiguo San Vicente de Paúl, Granja La Pradera y Granja Yuyucocha, en la Imagen 15 se muestra la Universidad Técnica del Norte.

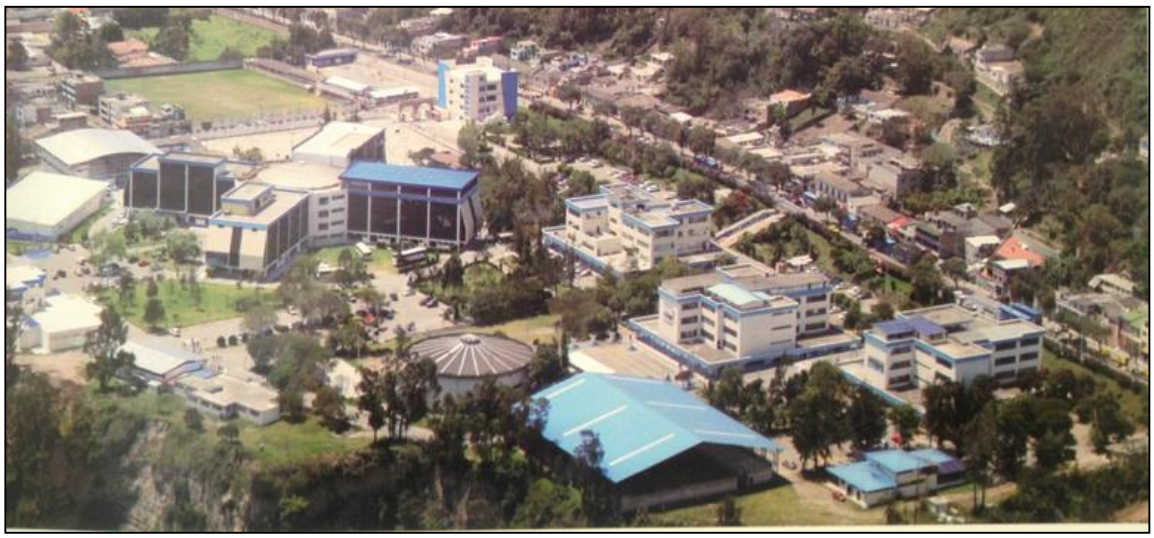


IMAGEN 15.- *Vista aérea de la Universidad Técnica del Norte*
Fuente: *Informe de Gestión 2012-2013, Universidad Técnica de Norte*

2.1.2. PERSONAL DE LA UNIVERSIDAD TÉCNICA DEL NORTE

En la universidad existen 790 trabajadores entre empleados y docentes, véase la Tabla 3, y 6607 estudiantes de las diferentes facultades, véase la Tabla 4

TABLA 3.- *Distribución del personal de la Universidad Técnica del Norte. Diciembre 2013*

Cargo Desempeñado	N° Empleados
Empleados a nombramiento	250
Empleados a contrato	82
Docentes a nombramiento	191
Docentes a contrato	267
TOTAL	790

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 4.- *Distribución de los estudiantes por facultad, Marzo 2014*

Facultad	N° de alumnos
Facultad de Ingeniería en Ciencias Aplicadas	1423
Facultad de Ciencias Administrativas y Económicas	1737
Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales	1012
Facultad de Educación Ciencia y Tecnología	1468
Facultad de Ciencias de la Salud	967
TOTAL	**6607**

Fuente: *Dirección de Desarrollo Tecnológico en Informático – UTN*

2.2. TOPOLOGÍAS DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE

La red de comunicaciones de la Universidad Técnica del Norte está representada en dos diferentes maneras: Topología Física y Topología Lógica.

2.2.1. TOPOLOGÍA FÍSICA

Esta topología se refiere a la disposición física o el lugar donde se encuentran cada uno de los equipos de red existentes, Imagen 19.

2.2.2. TOPOLOGÍA LÓGICA

Indica cómo se comunican las estaciones de trabajo o equipos dentro de la red física, Imagen 20.

2.3. DISTRIBUCIÓN LÓGICA DE LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE

La Universidad Técnica del Norte posee un contrato de servicio de internet de 300 Mbps con TELCONET S.A., éste ISP[14] provee de un pull de direcciones públicas de clase C 192.95.X.X/27 (por confidencialidad se han ocultado los dos últimos octetos de la dirección IP). Para la red interna la Universidad posee dos direccionamientos, el primero dedicado a la DMZ con el pull de direcciones 10.24.X.X/24 (por confidencialidad se han ocultado los dos

[14] ISP = Internet Service Provider, Empresa encargada de proveer servicio de internet al usuario final.

últimos octetos de la dirección IP); y el segundo direccionamiento es 172.20.0.0/16 el cual es dedicado en su totalidad para la red interna de la Universidad. En la tabla 5 se puede observar el direccionamiento IP que posee la Universidad.

TABLA 5.- *Direccionamiento IP de la Red Universitaria*

DESCRIPCIÓN	SUBRED	MÁSCARA DE SUBRED
Zona Desmilitarizada (DMZ)	10.24.X.X	255.255.255.0
Red Externa	190.95.X.X	255.255.255.224
Red Interna	172.20.0.0	255.255.0.0

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

La red interna se encuentra segmentada mediante VLANs, las cuales se hallan asignadas a cada una de las facultades y dependencias de la Universidad, en la Tabla 6 se encuentran detalladas cada una de las VLANs existentes.

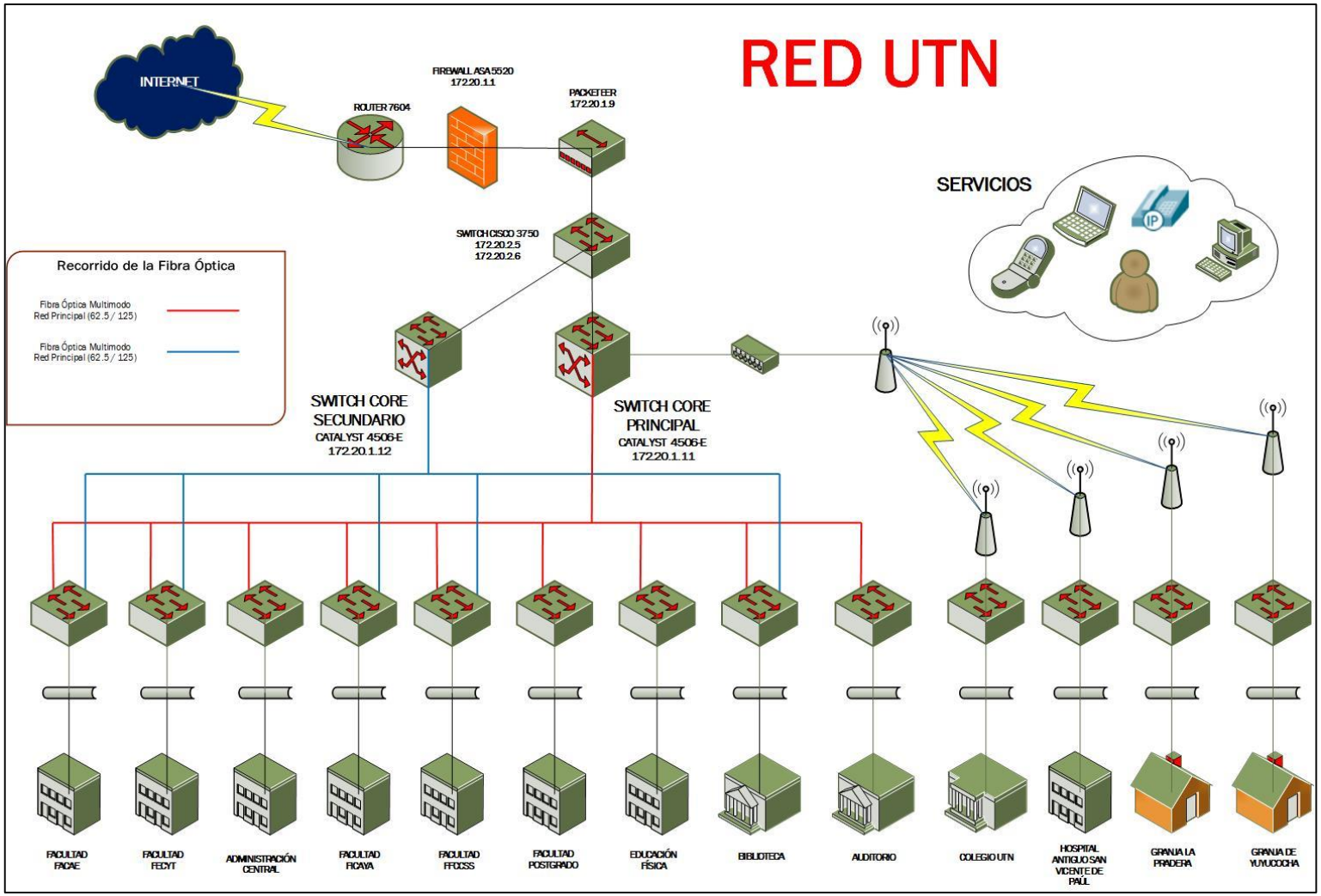


IMAGEN 16.- *Topología Física de la red Universitaria*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

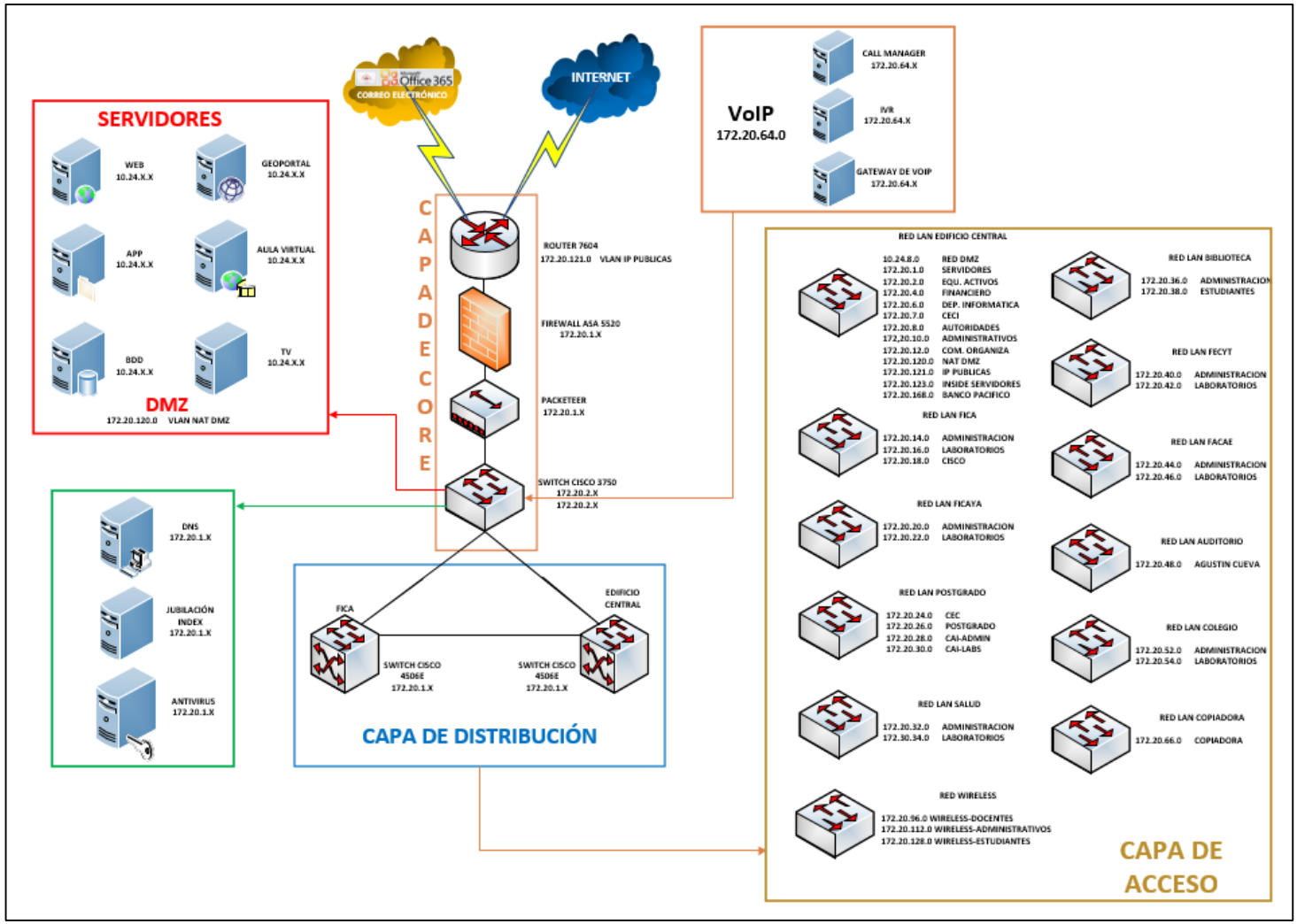


IMAGEN 17.- *Topología Lógica de la Red Universitaria*

Fuente: *Dirección de Desarrollo Tecnológico e Informático*

***6.- TABLA** Distribución de las VLANs en la Red Universitaria*

UBICACIÓN	DESCRIPCIÓN	ID DE VLAN	SUBRED	MASCARA DE SUBRED
Edificio Central	Servidores	1	172.20.1.0	255.255.255.0
	Equipos Activos	2	172.20.2.0	255.255.255.0
	Financiero	4	172.20.4.0	255.255.255.0
	Departamento de Informática	6	172.20.6.0	255.255.255.0
	CECI	7	172.20.7.0	255.255.255.0
	Autoridades	8	172.20.8.0	255.255.255.0
	Administrativos	10	172.20.10.0	255.255.255.0
	Comunicación Organizacional	12	172.20.12.0	255.255.255.0
	Telefonía IP	64	172.20.64.0	255.255.254.0
	NAT-DMZ-Interno	120	172.20.120.0	255.255.255.0
	IPs Públicas	121	----	----
	Enlace B. del Pacífico	168	172.20.168.0	255.255.255.0
FICA	Administración	14	172.20.14.0	255.255.255.0
	Laboratorios	16	172.20.16.0	255.255.254.0
	Academia Cisco	18	172.20.18.0	255.255.255.0
FICAYA	Administración	20	172.20.20.0	255.255.255.0
	Laboratorios	22	172.20.22.0	255.255.255.0
CEC	Administración	24	172.20.24.0	255.255.255.0

Postgrado	Administración y Labs.	26	172.20.26.0	255.255.255.0
CAI	Administración	28	172.20.28.0	255.255.255.0
	Laboratorios	30	172.20.30.0	255.255.255.0
FCCSS	Administración	32	172.20.32.0	255.255.255.0
	Laboratorios	34	172.20.34.0	255.255.254.0
Biblioteca	Administración	36	172.20.36.0	255.255.255.0
	Laboratorios	38	172.20.38.0	255.255.254.0
FECYT	Administración	40	172.20.40.0	255.255.255.0
	Laboratorios	42	172.20.42.0	255.255.255.0
FACAE	Administración	44	172.20.44.0	255.255.254.0
	Laboratorios	46	172.20.44.0	255.255.255.0
Auditorio A. Cueva	Auditorio	48	172.20.48.0	255.255.255.0
Colegio UTN	Administración	52	172.20.52.0	255.255.255.0
	Laboratorios	54	172.20.54.0	255.255.255.0
Copiadora	Copiadora	66	172.20.66.0	255.255.255.0
Wireless	Docentes	96	172.20.96.0	255.255.248.0
	Administrativos	112	172.20.112.0	255.255.248.0
	Estudiantes	128	172.20.128.0	255.255.224.0

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

2.4. EQUIPOS DE RED EXISTENTES EN LA UNIVERSIDAD TÉCNICA DEL NORTE

Los equipos que posee la universidad para la red informática, están distribuidas en cada una de las dependencias de la misma, el cuarto de comunicaciones principal se encuentra en la planta central de la Universidad, desde allí se realiza la interconexión a las diferentes facultades y dependencias de la Universidad. Desde el Edificio Central se comunica mediante enlaces de fibra óptica hacia las siguientes facultades: FICA, FICAYA, FACAE, FECYT, FCCSS, Instituto de Educación Física, Biblioteca, Auditorio Agustín Cueva, Instituto de Postgrado. Para el backup de la red, se lo realiza mediante el Switch Core existente en la FICA, sin embargo hacia el CAI existe tan solo un enlace directo de fibra óptica desde el Core de la FICA, la redundancia se realiza mediante enlaces de fibra óptica hacia todas los edificios exceptuando al Auditorio Agustín Cueva, Instituto de Postgrado Instituto de Educación Física; desde éste último se realiza un enlace de fibra óptica hacia el rack de la piscina.

Hay que recalcar que el servicio de backup se encuentra inhabilitado debido a que el enlace principal desde el Switch Core del Edificio central hacia el Switch Core en la FICA y backup, ambos de fibra óptica, están instalados por el mismo camino físico (ductería),
La Universidad al contar con Granjas Experimentales, Colegio Universitario, Hospital San Vicente de Paul, y todos estos alejados a la casona universitaria, dispone de enlaces de radio para poder llegar a dichas dependencias, logrando así que quienes trabajan y estudian allí accedan a los diferentes servicios que presta la red universitaria. En la Imagen 16 se muestra la topología física de la red, indicando como se interconectan los Switchs de acceso hacia los Switch Core que posee la universidad.

En la Imagen 17 se detallan las 3 capas de red: Core, Distribución, y Acceso. Los equipos mostrados son: Packet Shaper 3500 el cual nos permite el control de ancho de banda y administración de la red, lastimosamente el control de ancho de banda no se lo está realizando debido a que si se activa ésta característica al equipo, limitaría el ancho de bando a tan solo 45 Mbps y la Universidad posee un contrato de 300 Mbps; los Switch Catalyst 3750G uno de fibra y otro de cobre son parte del rack principal en el Edificio Central y permiten la interconexión de varios equipos en el rack; Wireless LAN Controler o WLC por sus siglas en inglés, éste equipo es el encargado de la administración de la red inalámbrica de la Universidad; en la DMZ de la universidad se encuentran la mayoría de los servidores de los diferentes servicios de la red universitaria: WEB, Aplicaciones.

Base de Datos, Streaming del Canal y la Radio, Campus Virtual, Repositorio Digital, son algunos de los servidores que se albergan en la DMZ; la telefonía IP de la universidad se lo realiza mediante los equipos correspondientes Gateway de Voz, Call Manager y el IVR[15]; el firewall de la universidad es un Cisco ASA 5520 del cual se hablará posteriormente;

A continuación se detallan los equipos que existen en cada una de las facultades y edificios que posee la Universidad.

2.4.1. EDIFICIO CENTRAL

En el edificio central se encuentra el cuarto de equipos principal de la red universitaria, allí están alojados varios equipos para la distribución de la red en la planta central, los equipos están distribuidos de la siguiente manera:

- **Cuarto de equipos**

TABLA 7.- *Equipos de Red en el Cuarto de Equipos del Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Catalyst 4506-E	
		Puertos de Fibra Óptica	12
		Puertos RJ-45	144
2	1	Catalyst 3750-X UTP	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Planta Baja**

TABLA 8.- *Equipos de Red en la Planta Baja del Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – PLANTA BAJA			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

[15] IVR = Interactive Voice Response, permite realizar grabaciones para que el servicio de voz interactúe con el usuario de forma automática.

- **Segundo Piso**

TABLA 9.- *Equipos de Red en el Segundo Piso del Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – PRIMER PISO			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48
2	1	Switch Catalyst 2960	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Auditorio José Martí**

TABLA 10.- *Equipos de Red en el Auditorio José Martí del Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – JOSÉ MARTÍ			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Canal UTV**

TABLA 11*.- Equipos de Red en el Canal UTV del Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – CANAL UTV			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: Dirección de Desarrollo Tecnológico e Informático - UTN

- **Terraza**

TABLA 12.- *Equipos de Red en la Terraza del Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – TERRAZA			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48
2	1	Switch 3COM 4400SE	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático*

- **Garita**

TABLA 13.- *Equipos de Red en la Garita perteneciente al Edificio Central*

EQUIPOS DE RED EN EL EDIFICIO CENTRAL – GARITA			
N°	Cantidad	Equipo	# de puertos
1	1	Switch 3COM 400SE	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Auditorio Agustín Cueva**

TABLA 14.- *Equipos de Red en el Cuarto de Equipos del Auditorio Agustín Cueva*

EQUIPOS DE RED EN EL AUDITORIO AGUSTÍN CUEVA – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch 3COM 4400SE	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

2.4.2. FICA

En la Facultad de Ingeniería en Ciencias Aplicadas se encuentran varios equipos de red, pero principalmente se encuentra el equipo con el cual se permite la redundancia a toda la red de la Universidad. Los equipos que existen en la facultad se encuentran distribuidos en diferentes dependencias.

- **Cuarto de equipos**

TABLA 15.- *Equipos de Red en el Cuarto de Equipos de la FICA*

EQUIPOS DE RED EN LA FICA – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Catalyst 4506-E Puertos de Fibra Óptica	12
		Puertos RJ-45	144

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio I**

TABLA 16.- *Equipos de Red en el Laboratorio I de la FICA*

EQUIPOS DE RED EN LA FICA – LABORATORIO I			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio II**

TABLA 17.- *Equipos de Red en el Laboratorio II de la FICA*

EQUIPOS DE RED EN LA FICA – LABORATORIO II			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio III**

TABLA 18.- *Equipos de Red en el Laboratorio III de la FICA*

EQUIPOS DE RED EN LA FICA – LABORATORIO III			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48
2	1	Switch Catalyst 2960	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio IV**

TABLA 19.- *Equipos de Red en el Laboratorio IV de la FICA*

EQUIPOS DE RED EN LA FICA – LABORATORIO IV			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Sala de Investigación**

TABLA 20.- *Equipos de Red en la Sala de Investigación de la FICA*

EQUIPOS DE RED EN LA FICA – SALA DE INVESTIGACIÓN			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Sala de Profesores**

TABLA 21.- *Equipos de Red en la Sala de Profesores de la FICA*

EQUIPOS DE RED EN LA FICA – SALA DE PROFESORES			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio de Cisco**

TABLA 22.- *Equipos de Red en el Laboratorio de Cisco de la FICA*

EQUIPOS DE RED EN LA FICA – CISCO			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológic Informático – UTN*

2.4.3. FICAYA

En la Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales existen varios equipos de red, además de que a la facultad pertenecen la Granjas experimentales que posee la universidad en donde también se encuentran instalados equipos, estos equipos son:

- **Cuarto de equipos**

TABLA 23.- *Equipos de Red en el Cuarto de Equipos de la FICAYA*

EQUIPOS DE RED EN LA FICAYA – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Cisco Linksys SRW2024	24
2	1	Switch Cisco SLM 2024	24

		Gigant			
3	1	Switch 3C17304 SS3	3COM	4228G	24
4	1	Switch 3C17203 SS3	3COM	4400	24
5	1	Switch SR224	Cisco	Linksys	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Granja experimental Yuyucocha**

TABLA 24.- *Equipos de Red en la Granja Yuyucocha de la FICAYA*

EQUIPOS DE RED EN LA FICAYA – YUYUCOCHA				
N°	Cantidad	Equipo		# de puertos
1	1	Switch SG-300-28	Cisco	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Granja experimental La Pradera**

TABLA 25.- *Equipos de Red en la Granja La Pradera de la FICAYA*

EQUIPOS DE RED EN LA FICAYA – LA PRADERA				
N°	Cantidad	Equipo		# de puertos
1	1	Switch SRW248G4	Linksys	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

2.4.4. FACAE

En la Facultad de Ciencias Administrativas y Económicas existen varios equipos para la distribución de red en el edificio, los cuales se los enumera a continuación:

- **Cuarto de Equipos**

TABLA 26.- *Equipos de Red en el Cuarto de Equipos de la FACAE*

EQUIPOS DE RED EN LA FACAE – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	2	Switch 3COM 4400SE	24
2	1	Switch 3COM 4400	24
3	1	Switch 3COM 5500G	48
4	2	Switch TPLINK TLSG2224 WEP	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio IV**

TABLA 27.- *Equipos de Red en el Laboratorio IV de la FACAE*

EQUIPOS DE RED EN LA FACAE – LABORATORIO IV			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960G	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

2.4.5. FECYT

En la Facultad de Educación Ciencia y Tecnología existen varios equipos de red, que se encuentran en diferentes dependencias de la misma, además el instituto de educación física pertenece a la FECYT, dichos equipos se describen a continuación:

- **Cuarto de equipos**

TABLA 28.- *Equipos de Red en el Cuarto de Equipos de la FECYT*

EQUIPOS DE RED EN LA FECYT – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Catalyst 2960	48
2	1	Switch Catalyst 2960	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio I**

TABLA 29.- *Equipos de Red en el Laboratorio I de la FECYT*

EQUIPOS DE RED EN LA FECYT – LABORATORIO I			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio II**

TABLA 30.- *Equipos de Red en el Laboratorio II de la FECYT*

EQUIPOS DE RED EN LA FECYT – LABORATORIO II			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio MAC**

TABLA 31.- *Equipos de Red en el Laboratorio IV de la FECYT*

EQUIPOS DE RED EN LA FECYT – LABORATORIO IV			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Coordinación de Carreras**

TABLA 32.- *Equipos de Red en la Coordinación de Carreras de la FECYT*

EQUIPOS DE RED EN LA FECYT – COORDINACION DE CARRERAS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Instituto de Educación Física**

TABLA 33.- *Equipos de Red en el Instituto de Educación Física perteneciente a la FECYT*

EQUIPOS DE RED EN LA FECYT – INSTITUTO DE EDUCACIÓN FÍSICA			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Piscina Semi-Olímpica UTN**

TABLA 34.- *Equipos de Red en el Cuarto de Equipos de la Piscina Semi-Olímpica UTN*

EQUIPOS DE RED EN LA PISCINA – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch 3COM 4200	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

2.4.6. FCCSS

En la Facultad de Ciencias de la Salud existen pocos equipos de red, así como también en el antiguo Hospital San Vicente de Paúl, el que pertenece a la casona universitaria. Los equipos se detallan a continuación.

- **Cuarto de Equipos**

TABLA 35.- *Equipos de Red en el Cuarto de Equipos de la FCCSS*

EQUIPOS DE RED EN LA FCCSS – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch 3COM 4400	48

Fuente*: Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Antiguo Hospital San Vicente de Paúl**

TABLA 36.- *Equipos de Red en el Antiguo Hospital San Vicente de Paúl perteneciente a la FCCSS*

EQUIPOS DE RED EN LA FECYT – ANTIGUO HSVP			
N°	Cantidad	Equipo	# de puertos
1	1	Switch TP-LINK TL-SG 2216 WEB	24
2	1	Switch TP-LINK TL-SF 1024	16

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

2.4.7. BIBLIOTECA

En la biblioteca universitaria existen varios equipos de red distribuidos en varias dependencias, las cuales son las siguientes:

- **Cuarto de Equipos**

TABLA 37.- *Equipos de Red en el Cuarto de Equipos de la Biblioteca*

EQUIPOS DE RED EN LA BIBLIOTECA – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48
2	1	Switch SG 300-52	48
3	1	Switch SG 200-18	18
4	1	Switch 3COM 5500 SG	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Hemeroteca**

TABLA 38.- *Equipos de Red en la Hemeroteca de la Biblioteca*

EQUIPOS DE RED EN LA BIBLIOTECA – HEMEROTECA			
N°	Cantidad	Equipo	# de puertos
1	1	Switch 3COM 3C16792A	16

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **IC3**

TABLA 39.- *Equipos de Red en el IC3 de la Biblioteca*

EQUIPOS DE RED EN LA BIBLIOTECA – IC3			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Cisco SG200-50	48

Fuente*: Dirección de Desarrollo Tecnológico e Informático – UTN*

2.4.8. CAI

En el edificio del Centro Académico de Idiomas, se encuentran los siguientes equipos:

- **Cuarto de Equipos**

TABLA 40.- *Equipos de Red en el Cuarto de Equipos del CAI*

EQUIPOS DE RED EN EL CAI – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Linksys SRW2048	48
2	1	Switch Linksys SRW2024	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Tercer Piso**

TABLA 41.- *Equipos de Red en el Tercer Piso del CAI*

EQUIPOS DE RED EN EL CAI – TERCER PISO			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Linksys SRW2048	48
2	2	Switch 3COM 3C17304A 4200	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

2.4.9. POSTGRADO

En el nuevo edificio de postgrado se ha instalado varios equipos de red, que se detallan a continuación.

- **Cuarto de Equipos**

TABLA 42.- *Equipos de Red en el Cuarto de Equipos de Postgrado*

EQUIPOS DE RED EN POSTGRADO – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 4503E	48
2	2	Switch Catalyst 2960S	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Primer Piso**

TABLA 43.- *Equipos de Red en el Primer Piso de Postgrado*

EQUIPOS DE RED EN POSTGRADO – PLANTA ALTA			
N°	Cantidad	Equipo	# de puertos
1	3	Switch Catalyst 2960S	48
2	1	Switch Catalyst 2960S	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

2.4.10. COLEGIO UNIVERSITARIO

En el colegio anexo a la Universidad Técnica del Norte, existen los siguientes equipos de red:

- **Cuarto de Equipos**

TABLA 44.- *Equipos de Red en el Cuarto de Equipos del Colegio Universitario*

EQUIPOS DE RED EN EL COLEGIO UNIVERSITARIO – CUARTO DE EQUIPOS			
N°	Cantidad	Equipo	# de puertos
1	1	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

2.4.11. BIENESTAR ESTUDIANTIL

En el edificio de Bienestar Estudiantil, existen los siguientes equipos de red:

- **Primer Piso**

TABLA 45.- *Equipos de Red en el primer piso de Bienestar Estudiantil*

EQUIPOS DE RED EN BIENESTAR ESTUDIANTIL – PRIMER PISO			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Catalyst 2960	48

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Segundo Piso**

TABLA 46.-*Equipos de Red en el segundo piso de Bienestar Estudiantil*

EQUIPOS DE RED EN BIENESTAR ESTUDIANTIL – SEGUNDO PISO			
N°	Cantidad	Equipo	# de puertos
1	2	Switch Catalyst 2960	48
2	1	Switch 3COM 4400 SE	24

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Los equipos detallados son todos los que existen y se encargan de la distribución de los servicios en toda la red universitaria y mediante los cuales se realizara la segmentación de red.

2.5. FIREWALL CISCO ASA 5520

Los virus y otros códigos maliciosos pueden dañar los recursos y servicios de la red de comunicaciones universitaria. El ataque de spyware y contenido de Internet no deseado puede afectar seriamente la productividad de todos quienes acceden a la red logrando exponer a las personas al robo de identidad. El Cisco ASA 5520 perteneciente a la Serie 5500 anti-X Edition permite proteger a la red contra ataques maliciosos proveniente de las redes externas e internas de las organizaciones mediante una solución todo en uno, proporcionando una fuerte protección y control para las comunicaciones empresariales en red, detiene las amenazas de red, incluyendo virus, gusanos, spyware , el spam y el phishing, además de controlar el correo no deseado y contenido web al tiempo que reduce los costes operativos y la complejidad de la implementación y gestión de soluciones de múltiples puntos.

El equipo firewall de la Universidad Técnica del Norte posee 4 puertos Gigabit Ethernet y un puerto de Management, el puerto de Management sirve para ver las funcionalidades del equipo como por ejemplo: Consumo del procesador, temperatura del procesador, etc.; de los puertos Gigabit Ethernet se encuentran utilizados 3 destinados para el enlace con la red interna (inside), red externa (outside) y la granja de servidores (DMZ). En la Imagen 18se muestra los puertos Gigabit Ethernet y sus respectivas direcciones IP (Las direcciones IPs se encuentran protegidas por términos de privacidad).

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length
GigabitEthernet0/0	outside	Yes	0	190.95.196.X 2800:68:19::X	255.255.255.224 64
GigabitEthernet0/1	inside	Yes	100	172.20.1.X 2800:68:19:1::X	255.255.255.0 64
GigabitEthernet0/2	DMZ	Yes	60	10.24.X.X 2800:68:19:2408::X	255.255.255.0 64
GigabitEthernet0/3		No			
Management0/0		No			

IMAGEN 18.- *Configuración de los puertos GigabitEthernet del firewall ASA 5520*

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

En el Firewall que posee la universidad, también se encuentra configurado las reglas de ruteo necesarias para que, luego de aplicar las reglas de seguridad encamine el tráfico hacia la interfaz correcta. En la Imagen 19 se observa algunas de las reglas de ruteo que se encuentran configuradas dentro del Cisco ASA 5520, tanto para el direccionamiento IPv4 como IPv6. En la interfaz inside se encuentran varias reglas las cuales redirigen el tráfico hacia la red interna de la Universidad, mientras que la outside se encuentra la salida hacia el exterior de la red, el redireccionamiento de tráfico hacia la DMZ se lo hace mediante NATEO.

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
inside	10.1.199.0	255.255.255.0	172.20.1.	1	None
inside	10.1.218.X	255.255.255.255	172.20.1.X	1	None
inside	10.1.231.X	255.255.255.255	172.20.1.X	1	None
inside	10.1.231.X	255.255.255.255	172.20.1.X	1	None
inside	10.1.231.X	255.255.255.255	172.20.1.X	1	None
inside	172.20.2.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.4.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.6.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.7.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.8.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.10.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.12.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.14.0	255.255.255.0	172.20.1.X	1	None
inside	172.20.16.0	255.255.254.0	172.20.1.X	1	None
inside	172.20.128.0	255.255.224.0	172.20.1.X	1	None
inside	172.30.34.0	255.255.254.0	172.20.1.X	1	None
inside	192.168.10.0	255.255.255.0	172.20.1.X	1	None
inside	2800:68:19:6::	64	2800:68:19:1::X	1	None
inside	2800:68:19:7::	64	2800:68:19:1::X	1	None
outside	0.0.0.0	0.0.0.0	190.95.196.X	1	None
outside	::	0	2800:68:19::X	1	None

IMAGEN 19.- *Reglas de ruteo configuradas en el Firewall Cisco ASA 5520*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Dentro de la administración del firewall, se encuentra configurado las diferentes IPs para el acceso a la interfaz del Cisco ASA, entre ellas se encuentra las IP de los host o subredes de la red universitaria las cuales tienen acceso mediante la inside del dispositivo; mientras que por la outside se encuentran configuradas las IPs públicas que tienen acceso al firewall. En la Imagen 20 se muestran algunas de las IPs y rangos de IPs que pueden acceder vía web o por el software de administración llamado Cisco ASDM.

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	172.20.1.x	255.255.255.255
ASDM/HTTPS	inside	172.20.101.x	255.255.255.255
ASDM/HTTPS	inside	172.20.128.x	255.255.255.255
ASDM/HTTPS	inside	172.20.128.x	255.255.255.255
ASDM/HTTPS	inside	172.20.16.x	255.255.255.255
ASDM/HTTPS	inside	172.20.x.x	255.255.255.0
ASDM/HTTPS	inside	172.20.x.x	255.255.255.0
ASDM/HTTPS	outside	181.112.0.0	255.255.0.0
ASDM/HTTPS	outside	181.198.77.128	255.255.255.224
ASDM/HTTPS	outside	186.42.0.0	255.255.0.0

IMAGEN 20.- *IPs y Rango de IPs que tienen acceso a las configuraciones del Firewall*

Fuente: *Dirección de Desarrollo Tecnológico e Informático*

Para poder configurar las reglas del firewall se deben crear los objetos de red, los cuales son las IP que se van a utilizar para las diferentes reglas; estos objetos pueden ser conjunto de IPs o solamente una IP como host. En la Imagen 21 se indica varios de los objetos de red que se encuentran configurados en el firewall, entre las cuales se observa las IP de Facebook, rapidshare, Claro y el pull de direcciones de la DMZ.

Name	IP Address	Netmask	Description
A-195.122.131.5	195.122.131.5	255.255.255.255	rapidshare
A-195.122.131.6	195.122.131.6	255.255.255.255	rapidshare
A-195.122.131.7	195.122.131.7	255.255.255.255	rapidshare
A-195.122.131.8	195.122.131.8	255.255.255.255	rapidshare
A-195.122.131.9	195.122.131.9	255.255.255.255	rapidshare
Claro1	200.25.197.202	255.255.255.255	
Claro2	200.57.178.163	255.255.255.255	
DMZ-network	10.24.8.0	255.255.255.0	
Facebook00	69.171.228.0	255.255.255.128	
Facebook01	69.171.229.0	255.255.255.128	
Facebook02	69.171.234.0	255.255.255.128	

OBJETOS DE IMAGEN 21*.- red configurados en el Firewall*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Si se desea bloquear o permitir algún servicio o aplicación por ciertos intervalos de tiempo, se debe crear un rango de tiempo dependiendo de las necesidades del administrador del firewall. En la Imagen 22 se observa la pantalla de configuración de los intervalos de tiempo en los cuales se permitirá o denegará los servicios.

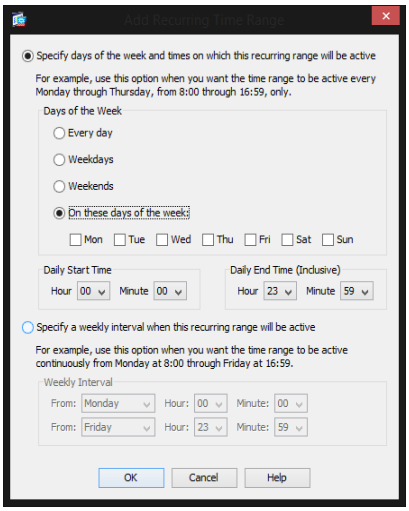


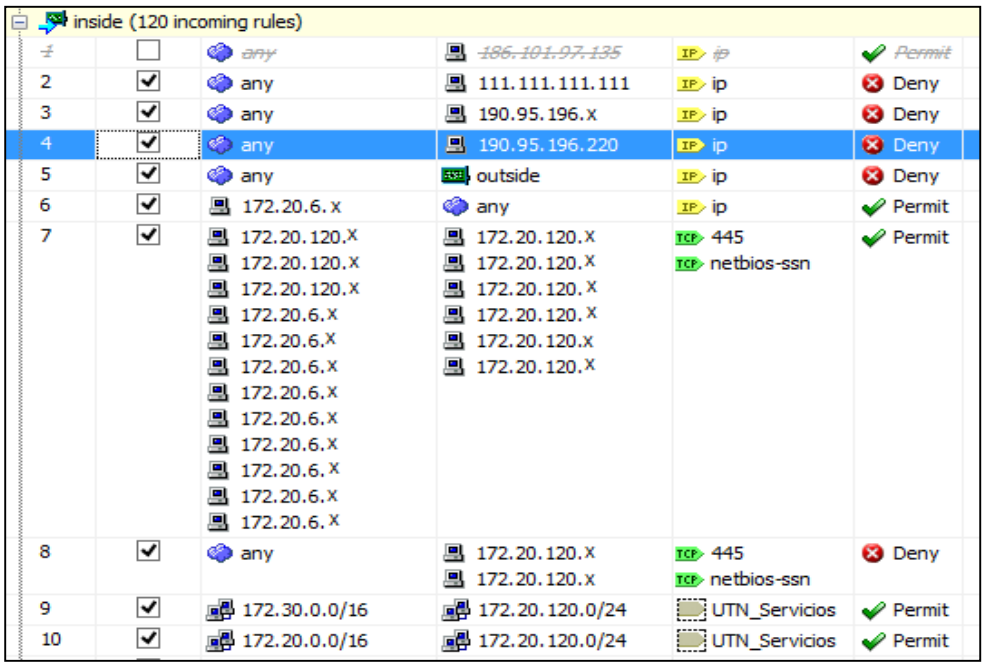
IMAGEN 22.- *Configuración de los intervalos de tiempo en el Firewall*
Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

El Firewall Cisco ASA 5520 nos permite realizar el NATEO entre las diferentes interfaces de red, en la interfaz hacia DMZ se tiene realizado un NATEO entre la red de la DMZ y la VLAN perteneciente a la misma así como hacia la salida a la internet; en la interfaz de outside se realiza el NATEO para que toda la red universitaria pueda tener salida hacia el internet, en la Imagen 23 podemos observar algunas de las configuraciones del NAT para la DMZ (se ha ocultado el último octeto de las IPs por seguridad).

#	Type	Original			Translated	
		Source	...	...	Interface	Address
DMZ (34 Static rules)						
1	Static	10.24.8.X			inside	172.20.120.X
2	Static	10.24.8.X			inside	172.20.120.X
3	Static	10.24.8.X			outside	190.95.196.X
4	Static	10.24.8.X			inside	172.20.120.X
5	Static	10.24.8.X			inside	172.20.120.X
6	Static	10.24.8.X			outside	190.95.196.X
7	Static	10.24.8.X			inside	172.20.120.X
8	Static	10.24.8.X			outside	190.95.196.X
9	Static	10.24.8.X			inside	172.20.120.X
10	Static	10.24.8.X			outside	190.95.196.X

IMAGEN 23.- *Configuraciones del NAT*
Fuente: *Dirección de Desarrollo tecnológico e Informático – UTN*

Lo más importante dentro del firewall son las reglas de acceso las cuales nos indicarán que servicio o aplicación se permite o deniega y hacia que IP lo hará, en el firewall que posee la universidad se encuentran configuradas varias reglas de acceso orientadas a un host o a una determinada VLAN. En la Imagen 24 se muestran varias de las reglas de acceso configuradas en el firewall.



inside (120 incoming rules)

≠	☐	any	186.101.97.135	ip	Permit
2	☑	any	111.111.111.111	ip	Deny
3	☑	any	190.95.196.x	ip	Deny
4	☑	any	190.95.196.220	ip	Deny
5	☑	any	outside	ip	Deny
6	☑	172.20.6.x	any	ip	Permit
7	☑	172.20.120.x 172.20.120.x 172.20.120.x 172.20.6.x 172.20.6.x 172.20.6.x 172.20.6.x 172.20.6.x 172.20.6.x 172.20.6.x 172.20.6.x 172.20.6.x	172.20.120.x 172.20.120.x 172.20.120.x 172.20.120.x 172.20.120.x 172.20.120.x	445 netbios-ssn	Permit
8	☑	any	172.20.120.x 172.20.120.x	445 netbios-ssn	Deny
9	☑	172.30.0.0/16	172.20.120.0/24	UTN_Servicios	Permit
10	☑	172.20.0.0/16	172.20.120.0/24	UTN_Servicios	Permit

IMAGEN 24.- *Reglas de seguridad configuradas en el Firewall*

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

2.6. ESTUDIO DE LOS RESULTADOS EN EL TRABAJO "HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE"

La implementación del firewall e IPS es indispensable para la seguridad de la información en una red de datos, pero para su funcionamiento se deben implementar correctas políticas de seguridad las cuales permitirán un mayor control de los ataques hacia la red. En un trabajo realizado anteriormente en la red universitaria el cual constaba en la realización de una honeynet virtual se realizaron pruebas para determinar cuáles son los ataques más recurrentes desde y hacia la red; los resultados fueron los siguientes:

2.6.1. CONEXIONES A LOS HONEYPOT

Tabla 47.- Conexiones Los honeypot se encargan de atraer a los atacantes simulando ser sistemas vulnerables, en estos se han detectado una gran cantidad de conexiones e intentos de ataques en un total de 1513 conexiones o ataques de las cuales 823 pertenecen al protocolo TCP, 628 corresponden al protocolo UDP y tan solo 12 a conexiones ICMP, en la Tabla 47 se observa el número de conexiones esquematizado.

TABLA 48.-*Realizadas a los honeypots*

Protocolo	Conexiones	Porcentaje (%)
TCP	823	54
UDP	678	45
ICMP	12	1
TOTAL	1513	100

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

De las conexiones realizadas a los honeypots se han determinado cuáles son los puertos lógicos más frecuentes de dichas conexiones y se muestra en la Tabla 48.

TABLA 49.- *Puertos de destino más frecuentes del total de conexiones registradas en los honeypots*

PROTOCOLO	PUERTO	DESCRIPCIÓN	CONEXIONES	PORCENTAJE %
TCP	445	Microsoft - DS	593	39
UDP	1101	PT2- Discover	428	28
TCP	135	EPMAP	205	14
UDP	137	NetBios	166	11
TCP	80	HTTP	75	5
TOTAL			1467	97

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

Como se observa en la Tabla 49, el mayor puerto de destino es el TCP/445 correspondiente a Microsoft-DS el cual es un servicio de Microsoft para la compartición de recursos, este puerto se utiliza para el establecimiento de sesiones TCP, la compartición de archivos e impresoras y para las comunicaciones entre los controladores de dominio de Windows 2000 y superiores, en los sistemas operativos Windows éste puerto permanece abierto permitiendo a los hackers y gusanos aprovechar esta vulnerabilidad para infectar a los equipos.

El segundo puerto de destino es el UDP/1101 empleado por Sebek[16], pero es el tráfico que se ha generado debido al intercambio de información cliente/servidor en la herramienta utilizada para la captura de datos, propia del trabajo realizado.

El 14% de las conexiones corresponde al puerto TCP/135 que pertenece al EPMAP[17] que permite determinar el listado de servicios disponibles en los equipos remotos, de igual manera que el Microsoft-DS (TCP/445) se lo considera muy importante para los sistemas operativos Windows y se encuentran activos predeterminadamente, este puerto puede ser utilizado para ataques DoS[18] si se establece un número elevado de conexiones simultaneas.

En cuarto lugar se tiene el puerto UDP/137 perteneciente al NETBIOS[19] el cual es el encargado de la compartición de recursos y archivos en sistemas operativos Windows, este puerto es muy vulnerable por encontrarse habilitado predeterminadamente permitiendo a los hackers y malwares cometer intrusiones malintencionadas.

Por último se encuentra el puerto TCP/80 perteneciente a HTTP pero este tráfico se genera debido a la navegación en la página web que se ha implementado en uno de los honeypots, propias del trabajo realizado.

2.6.2. ACTIVIDADES RECOLECTADAS EN LA RED INTERNA

Analizado el tráfico generado hacia los honeypots, se determinó que el origen es la red interna de la Universidad y un porcentaje mínimo se genera en direcciones IP externas, por lo que se ha registrado 108744 alertas, distribuidas en 14 categorías y corresponden a 284 alertas únicas, desde 12367 puertos de origen hacia 9014 puertos de destino. En la Tabla 49 se muestra la distribución de las alertas generadas de acuerdo a la clase de protocolo.

[16] Sebek: Es una herramienta de captura de datos diseñado para capturar las actividades del atacante en un honeypot
[17] EPMAP: End Point Mapper
[18] DoS = Denegación de Servicio
[19] NETBIOS: Network Basic Input Output System

TABLA 50.- *Número de alertas disparadas de acuerdo a la clase de protocolo*

PROTOCOLO	NÚMERO DE ALERTAS	PORCENTAJE %
UDP	82179	75,6
TCP	26477	24,3
ICMP	88	0,1
TOTAL	108744	100

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

Todas las alertas han sido clasificadas en 14 categorías detalladas en la Tabla 50.

TABLA 51.- *Clasificación de alertas registradas en BASE*[20]

CLASIFICACIÓN	NÚMERO DE ALERTAS	PORCENTAJE %
Policy-violation (Violación de políticas)	65653	60,37
Trojan-activity (Actividad troyana)	16517	15,19
Attemted-recon (Intentos de reconocimiento)	8451	7,77
Shellcode-detect (Detección de shellcode)	5983	5,50
Web-application-attack (Ataques a aplicaciones WEB)	2989	2,74
Misc-attack (Ataques varios)	2442	2,25
Bad-unknown (Actividad maliciosa desconocida)	1886	1,73
Not-suspicious (No sospechoso)	1656	1,52
Misc-activity (Actividad maliciosa variada)	1126	1,04
Attempted-admin (Atentado en contra de la administración)	688	0,63
Desclasificado (Alertas provenientes de los procesadores)	678	0,62
Attempted-do (Intentos de ataques DOS)	649	0,60
System-call-detected (Detección de llamados de sistema)	22	0,02
Non-standard-protocol (Protocolos no estandarizados)	13	0,01
TOTAL	108744	100

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

[20] BASE= Basic Analysis and Security Engine

Luego de clasificar todas las alertas generadas, se procede al análisis de las alertas únicas más frecuentes que pertenecen a las categorías más representativas, en la Tabla 51 se muestra las 5 alertas únicas que ocurrieron con mayor frecuencia dentro de la red universitaria.

TABLA 52.- *Alertas únicas más frecuentes registradas por BASE*

ALERTA	CLASIFICACIÓN	OCURRENCIA	PORCENTAJE %
ET TFTP Outbound TFTP Read Request	Policy-violation	61959	57
ET TROJAN Posible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	Trojan-activity	7244	7
GPL SHELLCODE x86 NOOP	Shellcode-detected	5200	5
ET SCAN Potential SSH Scan OUTBOUND	Attempted-recon	4004	4
ET TROJAN Storm Worm Encrypted Traffic Outbound Likely Connect Ack	Trojan-activity	3169	3

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

La alerta **"ET TFTP Outbound tftp read request"** se produce cuando se realiza una solicitud de lectura de un archivo de configuración a través del protocolo TFTP, estas alertas fueron generadas por dos Switch CISCO que solicitaban acceso a archivos inexistentes en la red, mediante el comando "no service config" se ha deshabilitado las peticiones de acceso a este archivo. Por otro lado la alerta **"ET TROJAN Posible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)"** indica la presencia de un gusano Conficker que se actualiza mediante redes de intercambio P2P, es el que realiza la creación de un archivo autorun.inf en la carpeta RECYCLER en los sistemas operativos Windows.
Mientras que la alerta **"GPL SHELLCODE x86 NOOP"** es la cual se encarga de detectar shellcode malicioso, los cuales se encargan de explotar vulnerabilidades en los sistemas. En

cuanto la alerta **“ET SCAN Potential SSH Scan OUTBOUND”** informa sobre ataques de fuerza bruta en contra de los equipos activos de la red utilizando SSH. Por último la alerta **“ET TROJAN Storm Worm Encrypted Traffic Outbound – Likely Connect Ack”** detectando la actividad del gusano Storm, el cual es un malware del tipo Caballo de Troya que se distribuye por la red a través del correo electrónico.

Luego de analizar las reglas únicas más frecuentes generadas en BASE, se describe los puertos de origen y destino más frecuentes por los cuales se generan las alertas, en la Tabla 52 se muestra los quince puertos de origen más frecuentes mientras que en la Tabla 53 se muestran los quince puertos de destino más frecuente.

TABLA 53.- *Puertos de origen de las alertas más frecuentes registradas por BASE*

PUERTO	OCURRENCIA
53	4149
58161/udp	3861
137/tcp	3411
445/udp	1508
1900/tcp	1491
2950/tcp	799
80/tcp	721
9069/tcp	568
27001/udp	548
3299/udp	505
4370/tcp	424
19003/udp	403
1113/udp	341
41555/tcp	306

Fuente: *“Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte”, Ing. Tatiana Vinueza (2012)*

TABLA 54.- *Puertos de destino de las alertas más frecuentes registradas por BASE*

PUERTO	OCURRENCIA
69	61959
80/udp	11337
22/tcp	6697
445/tcp	4479
137/tcp	3411
1900/udp	1515
49188/udp	868
10180/tcp	797
53/udp	783
2001/tcp	754
10480/udp	648
17480/udp	504
10680/udp	340
8799/tcp	279

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

Todas estas alertas que se han generado desde diferentes IPs de la red interna de la Universidad provenientes de Switchs cisco y de varios equipos pertenecientes a diferentes facultades de la casona universitaria, a continuación en la Tabla 54 se muestra las IPs que generan mayor alertas.

TABLA 55.- *Direcciones IP de origen más frecuentes registradas en BASE*

DIRECCIÓN IP ORIGEN	TOTAL ALERTAS
172.20.1.X	30998
172.20.1.X	30961
172.20.18.254	6473
172.20.1.158	5689
172.20.16.103	4017
172.20.18.201	1429
8.8.8.8	1164
172.20.18.253	1098
172.20.6.15	868
172.20.18.252	847
172.20.32.248	740
172.20.10.160	737
172.20.14.112	721
172.20.16.11	659
172.20.18.249	549

Fuente: *"Honeynet virtual hibrida en el entorno de red de la Universidad Técnica del Norte", Ing. Tatiana Vinueza (2012)*

Como se observa, las alertas más frecuentes se han generado en las VLANs pertenecientes a la academia CISCO - UTN, Administrativos y Laboratorios de la Facultad de Ingeniería en Ciencias Aplicadas, Administrativos de la Facultad de Ciencias de la Salud, Administrativos del Edificio Central y del Departamento de Informática, así como varios equipos activos de la red.

En la Tabla 55[21] se muestra el análisis a cada uno de los puertos de origen y destino que generaron la mayor cantidad de peticiones según BASE. Estos resultados permitirán que se tomen los correctivos necesarios en la implementación del Firewall y del IPS. Cabe recalcar que se ha realizado el análisis solamente a los mostrados en el informe del trabajo HONEYNET Virtual Híbrida en el Entorno de Red de la Universidad Técnica del Norte por parte de la Ing. Tatiana Vinueza.

TABLA 56.- *Análisis de resultados obtenidos en el trabajo HoneyNet Virtual Híbrida en el Entorno de Red de la Universidad Técnica del Norte*

N°	# de Puerto	Tipo de Puerto		Tipo	Descripción	Acción
		TCP	UDP			
1	22	SCTP		SSH	Secure Shell Protocol	Permitir
2	22	X		SSH	Secure Shell Protocol	Permitir
				Amenaza	Shaft	Denegar
				Troyanos	InCommand, Shaft, Skun	
3	22		X	SSH	Secure Shell Protocol	Permitir
				Amenaza	pcAnywhere	Denegar
4	53	X		Amenazas	Civcat, Esteems, W32.Dasher, W32.Spybot	Denegar
				Troyanos	ADM worm, li0n, MuSka52	
5	53		X	Domain	Domain Name Server	Permitir
6	69	X		TFTP	Trivial File Transfer Protocol	Permitir
				Amenazas	W32.Evala.Worm, W32.Mockbot	Denegar
				Troyanos	Virus Troyano BackGate Kit, Nimda, Pasana, Storm, Storm worm, Theef	
7	69		X	TFTP	Trivial File Transfer Protocol	Permitir
				Amenazas	W32.Blaster.Worm, W32.Bolgi.Worm, W32.Cycle, W32.Zotob	Denegar
				Troyano	Pasana	
8	80	SCTP		HTTP	Hypertext Transfer Protocol	Permitir
9	80	X		HTTP	Hypertext Transfer Protocol	Permitir

[21] El análisis de los puertos se los realizo desde http://es.adminsub.net/tcp-udp-port-finder el cual permite saber las características de cada uno de los mismos.

				Amenazas	711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2k Plug-Ins, Banito, Bebshell, Cafeini, CGI Backdoor, Civcat, Eaghouse, Executor, God Message, God Message Creator, Hesive, Hexem, Hooker, IISworm, Ketch, Lodear, Mindos, MTX, Muquest, Mydoom, NCX, Reverse WWW Tunnel Backdoor, RingZero, Seeker, Tabela, W32.Beagle, W32.Bobax, W32.Gaobot, W32.HLLW.Doomjuice, W32.HLLW.Heycheck, W32.HLLW.Polybot, W32.Ifbo, W32.Pinkton, W32.Spybot, W32.Tdiserv, W32.Theals, W32.Welchia, W32.Yaha, WAN Remote, Web Server CT, WebDownloader, Xeory, Zombam	Denegar
				Troyanos	711 trojan (Seven Eleven), AckCmd, BlueFire, Cafeini, Duddie, Executor, God Message, Intruzzo, Latinus, Lithium, MscanWorm, NerTe, Nimda, Noob, Optix Lite, Optix Pro, Power, Ramen, Remote Shell, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Scalper, Screen Cutter, Seeker, Slapper, Web Server CT, WebDownloader	
10	80		X	HTTP	Hypertext Transfer Protocol	Permitir
				Amenazas	W32.Beagle, W32.Bobax	Denegar
				Troyano	Penrox	
11	137	X		Netbios-ns	NETBIOS Name Service	Permitir
				Amenaza	Chode	Denegar
				Troyano	Chode, Nimda	
12	137		X	Netbios-ns	NETBIOS Name Service	Permitir
				Amenaza	Femot, Msinit	Denegar
				Troyano	Bugbear, Msinit, Opaserv, Qaz	
13	445	X		Microsoft-ds	Microsoft-DS	Denegar
				Amenazas	Netdepix, Otinet, Rtkit, Secefa, W32.Aizu, W32.Bobax, W32.Bolgi.Worm, W32.Cissi, W32.Cycle, W32.Explet, W32.HLLW.Deborms, W32.HLLW.Deloder,	

					W32.HLLW.Gaobot, W32.HLLW.Lioten, W32.HLLW.Moega, W32.HLLW.Nebiwo, W32.HLLW.Polybot, W32.Ifbo, W32.Janx, W32.Kibuv.Worm, W32.Kiman, W32.Korgo, W32.Mytob, W32.Reatle, W32.Sasser, W32.Scane, W32.Slackor, W32.Spybot, W32.Wallz, W32.Welchia, W32.Yaha, Randex, W32.Zotob	
				Troyano	Nimda	
14	445		X	Microsoft-ds	Microsoft-DS	Denegar
15	1113	X		LTP	Licklider Transmission Protocol	Denegar
				Amenaza	Hatckel	
16	1113		X	LTP	Licklider Transmission Protocol	Denegar
				Amenaza	Hatckel	
17	1900	X		SSDP	Simple Service Discovered Protocol	Denegar
18	1900		X	SSDP	Simple Service Discovered Protocol	Denegar
19	2001	X		Amenaza	Der Spaher, OICQSer, Panda, Glimpse, Trojan Cow	Denegar
				Exploradores	Der Späher	
				Troyanos	TrojanCow, DerSpaeher, Duddie, Glacier, Protoss, Senna Spy Trojan Generator, Singularity	
20	2001		X	Wizard	CAPTAN Test Stand System	Denegar
				Troyano	Scalper	
21	2950	X	X	ESIP	ESIP	Denegar
22	3299	X	X	pdrncs	Lenguaje entre computadoras que ayuda a que la comunicación sea más eficiente.	Denegar
23	4370	X	X	Elpro_tunnel	ELPRO V2 Protocol Tunnel	Denegar
24	8879	X		irdmi	Web Service, iTunes Radio streams	Denegar
25	8879		X	irdmi	QuickTime Streaming Server	Denegar
26	9069	X		No Asignado		Denegar
27	9069		X	irdmi	QuickTime Streaming Server	Denegar
28	10180	X	X	No asignado		Denegar

29	10480	X	X	Aplicaciones	Servidor dedicado de Juegos: SWAT-4, FIFA 2007	Denegar
30	10680	X	X	No Asignado		Denegar
31	17480	X	X	No Asignado		Denegar
32	19003	X	X	No Asignado		Denegar
33	27001	X		Flex-lm	FLEX LM, FlexLM	Denegar
				Amenaza	QuakeWorld	
34	27001		X	Flex-lm	FLEX LM	Denegar
				Aplicaciones	Servidor Dedicado de Juegos: Steam	
				Amenaza	QuakeWorld	
35	41555	X		Aplicaciones	Servidor Dedicado de Juegos: Brothers in Arms	Denegar
36	41555		X	No Asignado		Denegar
37	49188	X	X	Aple	XSAN Filesystem Access	Denegar
38	58161	X	X	Aple	XSAN Filesystem Access	Denegar

Fuente: *Basado en Investigación Teórica – Práctica*

A más de estos puertos se habilitarán los necesarios para cada uno de los servicios que presta la universidad.

CAPÍTULO III

3. DISEÑO DE LA SEGURIDAD PERIMETRAL EN EL ENTORNO DE LA RED

El presente capítulo corresponde al diseño del sistema de seguridad perimetral a implementarse en el entorno de red de la Universidad Técnica del Norte. Se encuentra organizado en tres secciones importantes: la nueva distribución y segmentación de la red universitaria, el diseño del Firewall y por último el diseño del IPS.

3.1. NUEVA DISTRIBUCIÓN Y SEGMENTACIÓN DE LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE

El primer paso para la seguridad perimetral en la red de la Universidad Técnica del Norte es tener una correcta distribución lógica de red, así como también un direccionamiento IP ordenado en cada uno de los dispositivos de red que posee las dependencias universitarias, además se empleará un nuevo e innovador tipo de nombres para cada uno de los equipos activos de red los cuales se observa en el Anexo 01.

3.1.1. DISTRIBUCIÓN LÓGICA DE LA RED

La distribución lógica de la red ha sido diseñada de acuerdo a las necesidades y dependencias de la universidad, para ello se va a utilizar la red 10.24.8.0/24 para la DMZ, 172.16.0.0/16 para la parte administrativa, la red 172.17.0.0/16 para los laboratorios y acceso de estudiantes a la internet, la red 172.18.0.0/24 para el enlace hacia la copiadora que existe junto al edificio central y la red 192.168.10.0/24 para el enlace que se tiene entre la Universidad y el banco del pacífico.

En total existirán 40 VLANs distribuidas en las diferentes redes, de las cuales 20 son para la parte administrativa de las diferentes dependencias de la Universidad, véase la Tabla 56; 14 destinadas para los laboratorios de las facultades y para las diferentes Wireless implementadas, véase la Tabla 57; y las 6 VLANs restantes son para las IPs Públicas, la red DMZ, VLAN Nativa, enlace hacia la copiadora y enlace hacia el banco del Pacífico respectivamente, véase la Tabla 58.

TABLA 57.- *Distribución de VLANs en la red 172.16.0.0/16*

RED 172.16.0.0 MÁSCARA 255.255.0.0				
N°	**UNIDAD**	**VLAN**	**SUBRED**	**MASK**
1	Edif. Central - Equipos Activos de Red	1	172.16.1.0	255.255.255.0
2	Edif. Central - Administración WLC	6	172.16.7.0	255.255.255.0
3	Edif. Central - Telefonía IP	8	172.16.8.0	255.255.254.0
4	Edif. Central - Departamento de Informática	12	172.16.12.0	255.255.255.0
5	Edif. Central – Autoridades	14	172.16.14.0	255.255.255.0
6	Edif. Central – Financiero	16	172.16.16.0	255.255.255.0
7	Edif. Central - Comunicación Organizacional	18	172.16.18.0	255.255.255.0
8	Edif. Central – Administrativos	20	172.16.20.0	255.255.255.0
9	Empresa Pública – Uemprende	22	172.16.22.0	255.255.255.0
10	Auditorio Agustín Cueva	24	172.16.24.0	255.255.255.0
11	FICA – Administrativos	44	172.16.44.0	255.255.255.0
12	FICAYA - Administrativos	52	172.16.52.0	255.255.255.0
13	FECYT - Administrativos	60	172.16.60.0	255.255.255.0
14	FACAE - Administrativos	68	172.16.68.0	255.255.255.0
15	FCCSS – Administrativos	76	172.16.76.0	255.255.255.0
16	Postgrado - Administrativos	84	172.16.84.0	255.255.255.0
17	CAI – Administrativos	92	172.16.92.0	255.255.255.0
18	Biblioteca - Administrativos	100	172.16.100.0	255.255.255.0
19	Colegio Universitario - Administrativos	108	172.16.108.0	255.255.255.0

Fuente: *Basado en investigación teórica y práctica*

TABLA 58.- *Distribución de VLANs en la red 172.17.0.0/16*

RED 172.17.0.0 MÁSCARA 255.255.0.0				
N°	**UNIDAD**	**VLAN**	**SUBRED**	**MASK**
1	FICA - Laboratorios	40	172.17.40.0	255.255.254.0
2	FICAYA - Laboratorios	48	172.17.48.0	255.255.254.0
3	FECYT - Laboratorios	56	172.17.56.0	255.255.254.0
4	FACAE - Laboratorios	64	172.17.64.0	255.255.254.0
5	FCCSS - Laboratorios	72	172.17.72.0	255.255.254.0
6	Postgrado - Laboratorios	80	172.17.80.0	255.255.254.0
7	CAI - Laboratorios	88	172.17.88.0	255.255.254.0
8	Biblioteca - Laboratorios	96	172.17.96.0	255.255.254.0
9	Colegio Universitario	104	172.17.104.0	255.255.254.0
10	Wireless - Docentes	112	172.17.112.0	255.255.248.0
11	Wireless - Administrativos	120	172.17.120.0	255.255.248.0
12	Wireless - Estudiantes	128	172.17.128.0	255.255.224.0
13	Wireless - Eventos 1	160	172.17.160.0	255.255.248.0
14	Wireless - Eventos 2	168	172.17.168.0	255.255.248.0

Fuente: *Basado en investigación teórica y práctica*

TABLA 59.- *Otras redes existentes en la Red Universitaria*

OTRAS REDES A EMPLEARSE				
N°	**UNIDAD**	**VLAN**	**SUBRED**	**MASK**
1	IPs Públicas	3	-	-
2	Red de la DMZ	4	10.24.8.0	255.255.255.0
3	NAT DMZ Interno	5	-	-
4	VLAN Nativa	39	-	-
5	Enlace Copiadora	201	172.18.0.0	255.255.255.0
6	Enlace Banco del Pacífico	202	192.168.10.0	255.255.255.0

Fuente: *Basado en investigación teórica y práctica*

Luego de haber realizado la distribución de las VLANs y su correspondiente direccionamiento IP para cada una de las redes que se implementarán, se procede a realizar un nuevo diseño lógico de la red universitaria, en la Imagen 25 se muestra el nuevo diseño lógico a implementarse en la red de la Universidad Técnica del Norte.

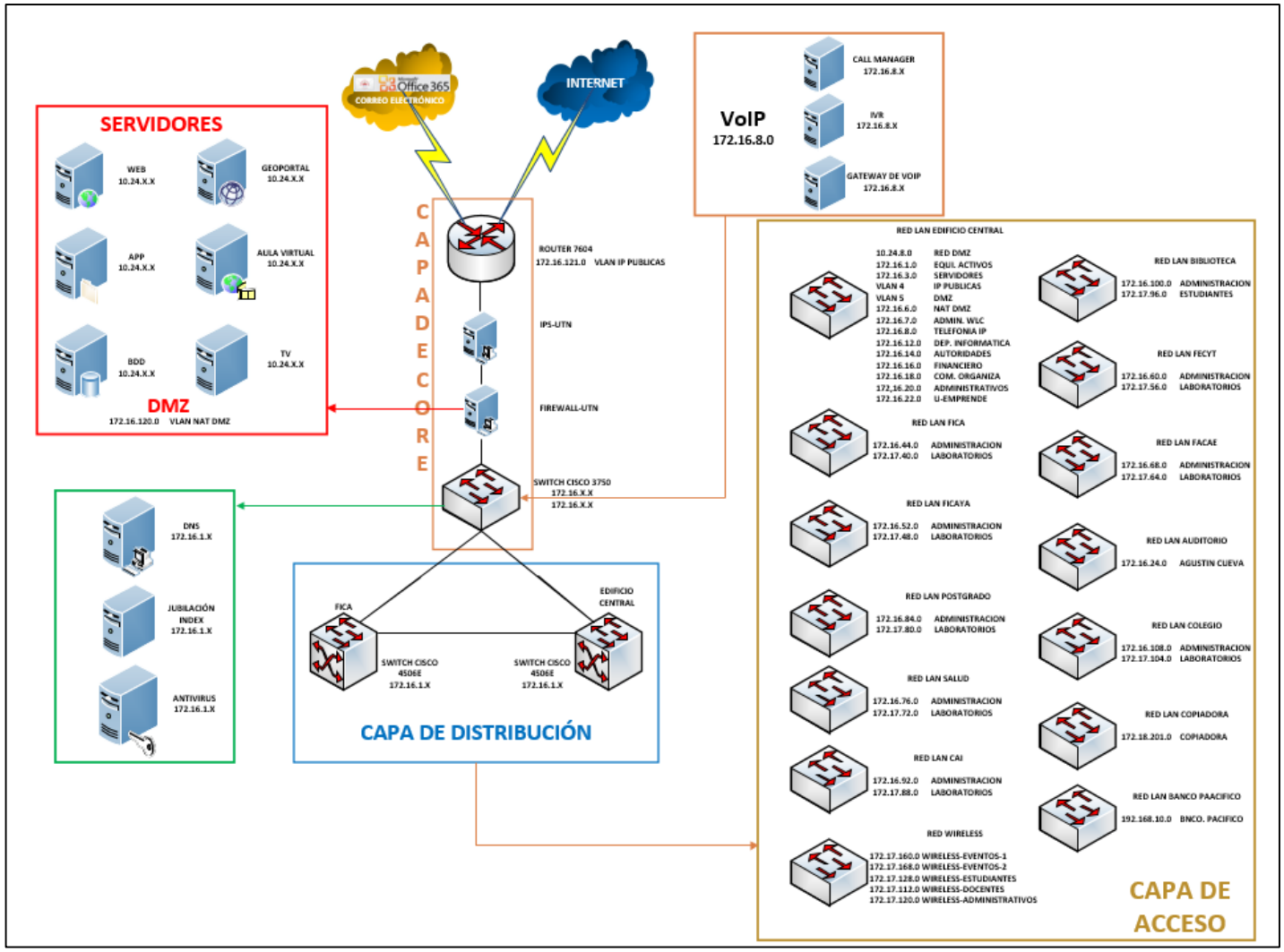


IMAGEN 25.- *Topología lógica a implementarse en la red universitaria*

Fuente: *Basado en la topología actual de la Red Universitaria y la investigación teórica y Práctica*

El Firewall e IPS de la red de datos de la Universidad Técnica del Norte se lo realiza por medio de un UTM, por ello en la Imagen 26 se muestra la estructura del Servidor de virtualización para la implementación de las máquinas virtuales.

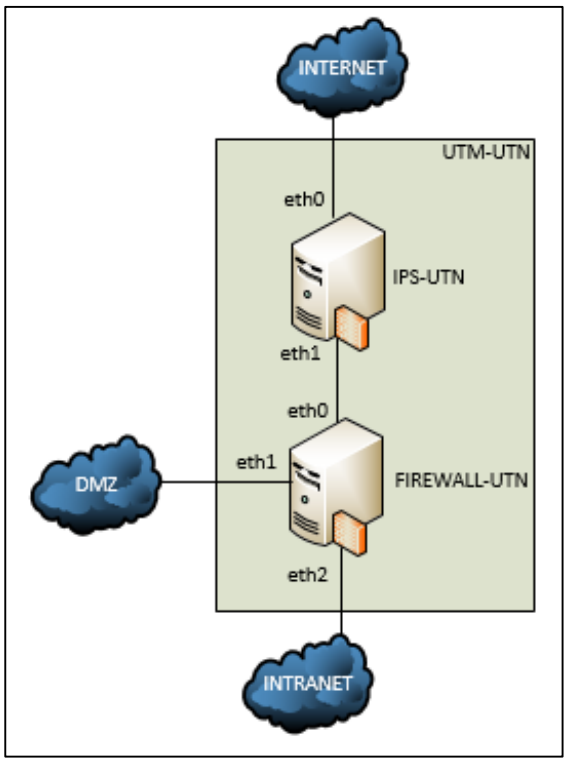


IMAGEN 26.- *Estructura de la UTM implementada en la red de datos*
Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

3.1.2. DISTRIBUCIÓN DE IPs

Para la distribución de las IPs en cada una de las subredes se deberá tomar en cuenta que las 20 primeras IPS no podrán ser utilizadas para usuarios finales ya que están destinadas para el uso del administrador de la red, es decir las IPs desde 172.X.X.1 hasta 172.X.X.20 serán reservadas, a excepción del direccionamiento IP en la VLAN 1.

3.1.2.1. VLAN 1 - Equipos activos de red

Esta VLAN está destinada para todos los equipos activos de red que posee la universidad, específicamente debe ser la VLAN 1 ya que existen equipos 3COM, TPLink, LinkSys que obligatoriamente deben pertenecer a esta VLAN para su administración. El pull de direcciones es 172.16.1.0/24 es decir se tiene 254 IPs utilizables, pero en caso de crecimiento se puede usar el pull 172.16.1.0/23 con un total de 510 IPs utilizables.

En la Tabla 59 se muestran las direcciones IP para los equipos activos de red:

TABLA 60.- *Direcciones IP para los equipos de la Red Universitaria*

DISTRIBUCIÓN DE IPs EN LA VLAN 1			
N°	**UNIDAD**	**IPs**	
		DESDE	**HASTA**
1	Edificio Central	172.16.1.1	172.16.1.20
2	FICA	172.16.1.21	172.16.1.40
3	FICAYA	172.16.1.41	172.16.1.60
4	FECYT	172.16.1.61	172.16.1.80
5	FACAE	172.16.1.81	172.16.1.100
6	FCCSS	172.16.1.101	172.16.1.120
7	Postgrado	172.16.1.121	172.16.1.140
8	CAI	172.16.1.141	172.16.1.160
9	Biblioteca	172.16.1.161	172.16.1.180
10	Colegio Universitario	172.16.1.181	172.16.1.200

Fuente: *Basado en investigación teórica y práctica*

Hay que recalcar que los equipos que existen en las granjas La Pradera y Yuyucocha pertenecen a la FICAYA, los equipos del Instituto de Educación Física y la Piscina pertenecen a la FECYT, los equipos del Auditorio Agustín Cueva y la Garita pertenecen al Edificio Central.

3.1.2.2. VLAN 3 – IPs Públicas

En esta VLAN no existirá direccionamiento IP internos solamente servirá para establecer que puertos pertenecerán y se podrá configurar al equipo con una de las IPs públicas que posee la Universidad.

3.1.2.3. VLAN 4 - DMZ

La VLAN de la DMZ no posee direccionamiento en la red 172.X.X.X ya que los equipos y servidores que se encuentren dentro de la misma tendrán un direccionamiento diferente, en la red 10.24.8.0/24

3.1.2.4. VLAN 5 - NAT DMZ Interno

Esta VLAN se utilizará para el NAT interno hacia los servidores que se encuentren instalados en la VLAN 4, tiene direccionamiento IP la red 172.16.5.0/24 quiere decir para 234 hosts, las IPs utilizables serán a partir de 172.16.5.21/24. El cuarto octeto corresponderá al último octeto de la IP utilizada en la VLAN 4, es decir si un servidor en la VLAN 4 tiene la IP 10.24.8.21 la IP para su correspondiente NAT en la VLAN 5 será 172.16.5.21.

3.1.2.5. VLAN 6 - Administración Wireless Lan Controler

Esta VLAN está destinada para los equipos de administración para las diferentes Wireless que existen en la Universidad, el pull de direcciones IPs es 172.16.6.0/24 es decir para 234 hosts o equipos, siendo la primera IP utilizable la 172.16.7.21/24.

3.1.2.6. VLAN 8 - Telefonía IP

La VLAN 8 estará destinada para todos los equipos de la telefonía IP para la red Universitaria, el pull de direcciones es 172.16.8.0/23 es decir para 490 equipos de telefonía pero con un posible crecimiento a 1002 equipos bajando un bit a la máscara, es decir el pull de direcciones 172.16.8.0/22, siendo la primera IP a utilizar la 172.16.8.21.

3.1.2.7. VLAN 12 - Departamento de Informática

Los equipos y hosts que pertenecen al Departamento de Informática estarán en la VLAN 12 la cual tiene como pull de direcciones IP la 172.16.12.0/24 es decir para 234 hosts, y con un crecimiento hasta 490 hosts al bajar un bit en la máscara de red es decir 172.16.12.0/23, la primera IP utilizable será la 172.16.12.21.

3.1.2.8. VLAN 14 - Autoridades

La VLAN 14 está dispuesta para todas las autoridades de la universidad: Rector, Vicerrectores, Decanos, Sub-decanos, etc., éstos tendrán el pull de direcciones IP de 172.16.14.0/24 con un total de 234 IPs y un crecimiento hasta 490 IPs reduciendo la máscara un bit es decir 172.16.14.0/23, la primera IP a ser utilizada es la 172.16.13.21.

3.1.2.9. VLAN 16 - Financiero

El departamento financiero pertenecerá a la VLAN 16 la cual tiene como pull de direcciones IP 172.16.16.0/24 para un total de 234 hosts y con un crecimiento de hasta 490 hosts reduciendo la máscara de red en un bit es decir 172.16.16.0/23, la primera IP a ser utilizada es la 172.16.16.21.

3.1.2.10. VLAN 18 - Comunicación Organizacional

El departamento de Comunicación Organizacional que posee la universidad está comprendido por la radio universitaria y el canal universitario estos pertenecerán a la VLAN 18 que posee el pull de direcciones 172.16.18.0/24 el cual comprende de 234 IPs hábiles, con un crecimiento se puede llegar a tener 490 IPs hábiles reduciendo la máscara de red en un bit quedando 172.16.18.0/23, la primera IP utilizable será la 172.16.18.21.

3.1.2.11. VLAN 20 - Administrativos

La VLAN 20 estará dedicada para quienes conforman la parte administrativa del Edificio Central así como para quienes se encuentran en el edificio de bienestar estudiantil, el pull de direcciones para esta VLAN es 172.16.20.0/24 es decir para 234 host y se ha tomado en cuenta un crecimiento de hasta 490 hosts reduciendo un bit a la máscara de red es decir 172.16.20.0/23, la primera IP utilizable es 172.16.20.21.

3.1.2.12. VLAN 22 - U-Emprende

La empresa pública perteneciente a la Universidad tendrá la VLAN 22 y un direccionamiento IP 172.16.22.0/24 es decir para 234 host y se puede tener un crecimiento de hasta 490 host al reducir un bit en la máscara de subred quedando así 172.16.22.0/23 y la primera IP utilizable será la 172.16.22.21.

3.1.2.13. VLAN 24 - Auditorio Agustín Cueva

Para todas las dependencias que existen en el auditorio Agustín Cueva se ha designado la VLAN 24 con un pull de direcciones 172.16.24.0/ es decir para 234 host, pudiendo tener un crecimiento de hasta 490 hosts al reducir un bit en la máscara de red quedando 172.20.16.0/23 y siendo la primera IP utilizable la 172.20.16.21.

3.1.2.14. VLANs - Laboratorios

En cada una de las dependencias universitarias existen los laboratorios a los cuales los estudiantes tienen acceso diariamente es por ello que a cada uno se le ha asignado una VLAN determinada en la red 172.17.0.0/16, cada una de estas VLANs tiene un pull de direcciones con máscara 255.255.254.0 es decir /23 para 490 hosts pero se puede incrementar hasta 2026 host recorriendo 2 bits la máscara de res es decir 255.255.248.0 o /21 y las primeras IPs asignables a los host es la 172.17.X.21.

3.1.2.15. VLANs - Administrativos

Las diferentes facultades y dependencias de la Universidad poseen una parte administrativa es por ello que se ha asignado a cada una, una VLAN respectivamente en la red 172.16.0.0/16, estas VLANs poseen un pull de direcciones de máscara 255.255.255.0 o /24 es decir existen 234 IP utilizables pero se puede realizar un crecimiento de hasta 1002 host recorriendo 2 bits a la máscara de red es decir 255.255.252.0 o /22, y la primera IP utilizable será 172.16.X.21 en cada una de las VLANs.

3.1.2.16. VLAN 112 - Wireless Docentes

Esta VLAN se ha asignado a una de las Wireless existentes en la Universidad que es destinada para que se conecten exclusivamente los docentes universitarios, se tiene una capacidad para 2026 hosts en el pull de direcciones IP 172.17.112.0/21 y la primera IP utilizable es la 172.17.112.21.

3.1.2.17. VLAN 120 - Wireless Administrativos

Esta VLAN se ha asignado la Wireless destinada para que se conecten exclusivamente las personas del área administrativa de la Universidad, se tiene una capacidad para 2026 hosts en el pull de direcciones IP 172.17.120.0/21 y la primera IP utilizable es la 172.17.120.21.

3.1.2.18. VLAN 128 - Wireless Estudiantes

En la Universidad existe una red Wireless para el uso de los estudiantes y se le ha asignado la VLAN 128 y el pull de direcciones es 172.17.128.0/19 es decir puede tener 8170 hosts conectados, de la misma manera la primera IP utilizable es 172.17.128.21.

3.1.2.19. VLANs 160 y 168 - Wireless Eventos

Cuando se realicen eventos de cualquier índole en el campus de la Universidad se activaran redes Wireless a las cuales se les ha asignado las VLANs 160 y 168, tendrán un pull de direcciones de máscara 255.255.248.0 o /21 y cada una tendrán una capacidad de alojamiento para 2026 host, la primera IP utilizable será 172.17.X.21.

3.1.2.20. VLAN 201 - Enlace Copiadora

La copiadora existente a las afueras del edificio central y la existente dentro de la Biblioteca poseen su propio enlace de red y se le ha asignado la VLAN 201 además se encuentra con un direccionamiento IP diferente a las anteriores VLANs el cual es 172.18.0.0/24 es decir posee 234 IP hábiles para host y la primera IP utilizable es la 172.18.0.21.

3.1.2.21. VLAN 202 - Enlace Banco del Pacífico

La Universidad Técnica del Norte posee un enlace directo hacia el Banco del Pacífico, entidad en la que se tiene las cuentas bancarias; por ello se tiene un enlace de red directo hacia ellos en la VLAN 202 y el direccionamiento IP es 192.168.10.0/24.

3.2. EQUIPO SERVIDOR, SOFTWARE DE VIRTUALIZACIÓN Y SISTEMA OPERATIVO

La implementación del Sistema de Seguridad Perimetral requiere de equipos con grandes prestaciones de procesamiento y almacenamiento, además para aprovechar las capacidades del mismo es imprescindible la virtualización de los recursos. Los sistemas operativos a instalar en cada una de las máquinas virtuales son bajo la plataforma GNU/Linux.

3.2.1. DESCRIPCIÓN DEL EQUIPO SERVIDOR

En el cuarto de equipos principal de la Universidad Técnica del Norte existe un servidor IBM Power 710, véase la Imagen 27, en el cual se desea instalar el sistema operativo para la virtualización de los diferentes servicios del sistema de seguridad perimetral a implementarse.

IMAGEN 27.- *Servidor IBM Power 710 Express*

Fuente: *IBM Power 710 and 730 Technical Overview and Introduction*

El servidor IBM Power 710 es un servidor de 2U (Unidades de Rack) para montaje en Rack, con un socket para procesador de 4-Nucleos de 3.0GHz, 6-Nucleos de 3,7 GHz y 8-Nucleos de 3,55 GHz según la configuración. Incluye 4 slots DIMM DDR3 para memorias RAM hasta un máximo de 8 slots DIMM DDR3 con una tarjeta de sockets de memoria adicional logrando así un máximo de 64 GB de memoria RAM. Posee 4 tarjetas de red PCI 10/100/1000 los cuales se pueden configurar en 2 adaptadores de red de 10 GB mediante IVE (Integrated Virtual Ethernet).

Para los equipos IBM de la serie Power Express existe un software de Virtualización propietario de la marca, para acceder a este software es necesario hacerlo mediante un partner ya que es quien asigna el ID para los servicios de IBM, en la Imagen 28 se muestra el intento de descarga del Software de Virtualización IBM VIOS, debido a que no se posee un ID IBM no se tiene acceso a dicho software.

IMAGEN 28.- *Fallo de descarga del Software IBM VIOS*

Fuente: *http://www-933.ibm.com/support/fixcentral/vios/downloadFixes?parent=Virtualization%2Bsoftware&product=ibm/vios/5765G34&release=2.2.3.3&platform=All&includeIso=false&function=fixId&fixids=VIOS_2.2.3.3-IV61263&includeRequisites=1&includeSupersedes=0&downloadMethod=htt*

Tomando en cuenta que el mainframe del equipo IBM Power 710 Express solamente acepta sistemas operativos bajo las plataformas Linux Power, Red Hat Enterprise Linux y Suse Server, es indispensable la adquisición de un equipo servidor el cual permita la instalación de los servicios de virtualización basados en open source. Se recomienda un equipo servidor HP Proliant ya que a diferencia de los IBM puede instalarse cualquier sistema operativo, en este caso el servidor de virtualización bajo software libre, en las Tablas 60 y 61 se muestra una comparación entre los equipos para servidores HP Proliant de bastidor y torres respectivamente

Luego del análisis comparativo de los servidores HP Proliant y revisando los requerimientos para la instalación del servidor de virtualización descritos en el Anexo 04, se sugiere la adquisición del equipo Hp Proliant DL320e Gen8 v2 ya que brinda las características necesarias para dicho servidor de virtualización. En la Tabla 62 se muestra las características que debe poseer el servidor a adquirirse.

TABLA 61.- *Comparación de equipos servidores HP Proliant de Bastidor*

Servidores HP Proliant de Bastidor				
N	Característica	Modelo de Servidor HP Proliant		
		DL320e Gen8 v2	DL360p Gen8	DL380p Gen8
1	Diseño Físico			
2	Procesador	Xeon E3-1200v3 Intel Pentium Intel Core i3	Xeon E5-2600v2	Xeon E5-2600v2 Xeon E5-2600
3	# de Procesadores	1	1-2	1-2
4	Núcleo de procesador disponible	4-2	12-10-8-4	12-10-8-6-4-2
5	Memoria Máxima	32 GB	768 GB	768bGB
6	Ranuras de memoria	4 DIMM (máx.)	24 DIMM (más)	24 DIMM (máx.)
7	Descripción de unidad	2 SAS/SATA/SSD grandes 4 SAS/SATA/SSD pequeños	4 SAS/SATA/SSD grandes 10 SAS/SATA/SSD pequeños 8 SAS/SATA/SSD pequeños	4 SAS/SATA/SSD grandes 10 SAS/SATA/SSD pequeños 8 SAS/SATA/SSD pequeños
8	Controladora de red	Adaptador Ethernet de 1 GB 2 puertos por controlador	Adaptador Ethernet de 1 GB 4 puertos por controlador o Adaptador Ethernet de 10 GB 2 puertos por controlador	Adaptador Ethernet de 1 GB 4 puertos por controlador o Adaptador Ethernet de 10 GB 2 puertos por controlador
9	Form Factor	1U	1U	2U

Fuente: *http://www8.hp.com/ec/es/products/servers/proliant-servers.html#tab=TAB2*

***TABLA 62**.- Comparación de equipos servidores HP Proliant tipo Torre*

Servidores HP Proliant tipo Torre						
N	Característica	Modelo de Servidor HP Proliant				
		ML10	ML350e Gen8 v2	ML310e Gen8 v2	ML350e Gen8	ML350p Gen8
1	Diseño Físico					
2	Procesador	Intel Pentium	Xeon E5-2400v2	Xeon E3-1200v3 Intel Core i3 Intel Pentium	Xeon E5-2400	Xeon E5-2600 Xeon E5-2600 v2
3	# de Procesadores	1	2-1	1	2-1	2-1
4	Núcleo de procesador disponible	2	10-8-6-4	4-2	8-6-4	12-10-8-6-4-2
5	Memoria Máxima	32 GB	32 GB	32GB	192	768
6	Ranuras de memoria	4 DIMM (máx.)	12 DIMM (máx.)	4 DIMM (máx.)	12 DIMM (máx.)	24 DIMM (máx.)
7	Descripción de Unidad	1 SATA grande	4 SAS/SATA/SSD LFF o 8 SAS/SATA/SSD SFF	4 SAS/SATA/SSD LFF o 8 SAS/SATA/SSD SFF	4 SATA grandes 18 SAS/SATA/SSD grandes 24 SAS/SATA/SSD pequeños	24 SAS/SATA/SSD SFF 18 SAS/SATA/SSD LFF
8	Controladora de red	Adaptador Ethernet 1GB	Adaptador Ethernet 1GB 2 puertos por controladora	Adaptador Ethernet 1GB 2 puertos por controladora	Adaptador Ethernet 1GB 2 puertos por controladora	Adaptador Ethernet 1GB 4 puertos por controladora
9	Form Factor	4U	5U	4U	5U	5U

Fuente: *http://www8.hp.com/ec/es/products/servers/proliant-servers.html#tab=TAB2*

TABLA 63.- *Características del servidor HP Proliant a adquirir*

Servidor HP Proliant DL320e Gen8 v2		
N°	Descripción	Requerimiento
1	Procesador	Xeon E3-1200v3
2	# de Procesadores	1
3	Núcleo de procesador	4
4	Memoria	4*8 GB DIMM
5	Hard Disk	2 TB
6	Controladora de red	2 Adaptadores Ethernet de 1 GB
7	Form Factor	1U de Rack

Fuente*: Basado en Investigación Teórica Práctica*

3.2.2. SOFTWARE DE VIRTUALIZACIÓN CITRIX XEN-SERVER

Para implementar los distintos servidores que se necesitan para el Sistema de Seguridad Perimetral, es necesario la creación de máquinas virtuales, en el mercado existen varios software para la gestión de máquinas virtuales muchos de ellos son propietarios y toca adquirir mediante el pago de una licencia, en cambio existe gestores de máquinas virtuales bajo plataforma del Open Source. En la Tabla 63 se muestra una comparación entre diferentes software para la gestión de máquinas virtuales.

TABLA 64.- *Comparación entre software de gestion de máquinas virtuales*

COMPARACIÓN ENTRE SOFTWARE PARA MAQUINAS VIRTUALES				
Característica	VMWare	Microsoft	IBM	Citrix
Versión	vSphere 5.5	HyperV 2012R2	PowerVM 2.2.2	XenServer 6.2
Cuadrante de Gartner	Lider	Lider	Lider	Challenger
Precio Servidor	$ 2875 Socket	$ 6154 2 Sockets	$ 2800 Socket	Gratis o $500 Enterprise
Precio Administrador	$ 4995	$ 3607	Incluido en Serv.	Gratis
Memoria Max por Host	4TB	4TB	16TB	1TB
CPU max por core	Ilimitado	Ilimitado	Ilimitado	Ilimitado
CPU max por MV	64	64	64	16 Win / 32 Linux
Max RAM por MV	1TB	1TB	32TB	128GB
Advanced Net. SW	No	Si	Si	Si
VLAN	Si	Si	Si	Si
PVLAN	No	Si	No	No
IPv6	Si	Si	Si	Si (Enterprise)
Network QoS	Si	Si	Si	Si
Monitoreo de Tráfico	No	Si	Si	Si

Fuente: *http://www.virtualizationmatrix.com*

Luego de la comparación entre varios gestores de máquinas virtuales se determina el uso de Citrix Sen el cual es un Sistema operativo Open Source que permite la administración eficiente de Máquinas Virtuales, además de la capacidad de gestionar los recursos de almacenamiento, procesamiento y Networking mediante la paravirtualización. En la Imagen 29 se muestra la arquitectura del Sistema Operativo XenServer, y en el Anexo 04 se muestre el procedimiento de Instalación del Servidor de Máquinas Virtuales con Xen Server.

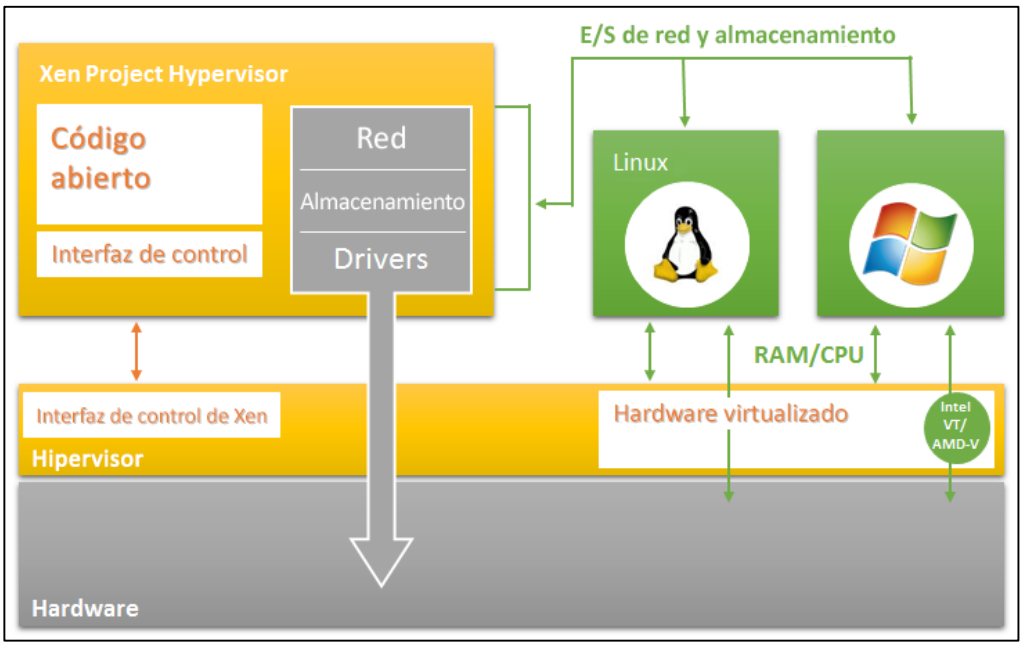


IMAGEN 29.- *Diagrama de arquitectura Citrix Xen-Server*

Fuente: *http://www.citrix.es/products/xenserver/tech-info.htm*

I

3.2.3. SISTEMA OPERATIVO PARA EL FIREWALL DEL SISTEMA DE SEGURIDAD PERIMETRAL

La implementación del Firewall y el IDS se lo realizarán en la distribución de Software Libre Red Hat específicamente CentOS, la cual es una distribución empresarial gratuita además de ser robusto, estable, fácil de instalar y utilizar. El sistema operativo CentOS está diseñado para servidores ya que provee seguridad y estabilidad en su distribución además de un fácil mantenimiento y administración para el usuario. CentOS brinda varias ventajas al usuario:

- ✓ Confiabilidad.- La distribución de Software Libre CentOS puede estar ejecutándose en un equipo por largo tiempo sin requerir de ninguna actualización del sistema, aproximadamente tardan en generar actualizaciones en un promedio de 5 años.
- ✓ Velocidad.- CentOS trabaja mucho más rápido que las demás distribuciones de Linux debido a que ejecuta solo las versiones básicas del software, y el procesador no se satura al intentar ejecutar varias aplicaciones diferentes.
- ✓ Seguridad.- Las aplicaciones en CentOS tienen una menor posibilidad de contener malwares que pueden atacar al funcionamiento del Sistema Operativo.
- ✓ Multiplataforma.- La distribución de CentOS soporta casi todas las arquitecturas como Intel x86, Intel Pentium I-II-III-IV, Intel Celeron entre otras, así como AMD, Apple Macintosh, y para el proyecto de seguridad perimetral es compatible con el Mainframe de IBM.

En el Anexo 05 se muestra el proceso de instalación del Sistema Operativo bajo Software Libre CentOS 6.5.

3.3. FIREWALL

La implementación del Firewall se lo realiza mediante la utilización de las IP-Tables realizando configuraciones en la consola del sistema operativo, pero existe un método gráfico en el cuál, el usuario puede configurar los parámetros necesarios y la interfaz gráfica es la que incluye los comandos que se emplean para la configuración del Firewall en sus respectivos scripts, esto se lo realiza mediante Shorewall y Webmin.

Como ya se explicó en el capítulo I, se utilizará la política de **todo lo que no es específicamente permitido se niega,** será necesario habilitar los puertos de comunicación que necesitan cada uno de los servicios que presta la Universidad en su red informática.

3.3.1. SHOREWALL

Eastep, Tom (2003) lo define como “Una herramienta de alto nivel para configurar Netfilter. Usted describe los requisitos de firewall, Gateway usando las entradas en el conjunto de archivos de configuración. Shorewall lee los archivos de configuración y con la ayuda de iptables, iptables-restore, y las demás utilidades configura Netfilter y el subsistema de la red de Linux”.

Para la configuración del Shorewall se debe ingresar los datos en algunos ficheros en texto simple y éste creará las reglas del firewall a través de iptables.

Las características de prestaciones de Shorewall son las siguientes:

- ✓ Tres modos de operación: Router, Firewall o Gateway.
- ✓ Ilimitado número de interfaces
- ✓ División de la red en zonas, para mejor control.
- ✓ Múltiples interfaces por zona y viceversa
- ✓ Listas negras de sub-redes e IPs individuales
- ✓ Soporte operacional
- ✓ Soporte VPN, Masquerading, Port Forwarding, NAT Proxy ARP
- ✓ Soporte para control de tráfico y cogestión

3.3.2. WEBMIN

Es una interfaz basada en web para la administración del sistema Linux, permitiendo al usuario una fácil interacción entre él y las funcionalidades del sistema operativo eliminando la necesidad de editar manualmente los archivos de configuración, en este caso permitirá un fácil manejo del Firewall Shorewall.

3.3.3. ESCANEO DE PUERTOS HABILITADOS

Una de las políticas de seguridad a implementarse es bloquear todo y permitir lo estrictamente necesario, por ello es indispensable realizar un escaneo de los puertos que se encuentran habilitados en cada uno de los servicios que presta la universidad; dichos servicios se encuentran en la DMZ y mediante la configuración de NAT se tiene acceso a la Red LAN y a la WAN.

Para descubrir las IPs que se encuentran con servicios de la red Universitaria se utiliza el Sistema Operativo de Software Libre Kali Linux, el cual es un Open Source bajo la plataforma de Debian que esta orientado a la auditoria y seguridad informática, dentro de este sistema operativo existe una herramienta para el mapeo de puertos habilitados el cual se llama ***nmap***.

Se realiza un escaneo de IPs para analizar los puertos de comunicación que se encuentran habilitados para ello se utiliza el comando:

*nmap –sP 172.20.120.**

Mediante el código -sP realiza una búsqueda de las IPs activas desde la 172.20.120.0 hasta la 172.20.120.255, como resultado tenemos que existen 22 IPs asignadas a diferentes servicios de la red Universitaria.

Luego del descubrimiento de las diferentes IPs se realiza el análisis de los puertos habilitados en las mismas. Mediante el comando ***nmap -sV X.X.X.X***, donde -sV a mas de descubrir los puertos abiertos, trata de descubrir los servicios y versiones que se alojan en el mismo. En la Tabla 64 se muestra el resultado del escaneo de puertos en la red interna.

TABLA 65.- *Escaneo de puertos en los servicios de la red Universitaria*

N°	IP Interna	Servicio UTN	Puerto Encontrado
1	172.20.120.12	svrapp2.utn.edu.ec	22/tcp (ssh) 5801/tcp (vnc-http) 5802/tcp (vnc-http) 5901/tcp (vnc) 5902/tcp (vnc) 5903/tcp (vnc) 5904/tcp (vnc) 5906/tcp (vnc)

			5907/tcp (vnc) 5910/tcp (vnc) 5911/tcp (vnc) 5915/tcp (vnc)
2	172.20.120.13	apex.utn.edu.ec	22/tcp (ssh) 139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 1521/tcp (Oracle-tns) 5901/tcp (vnc) 5902/tcp (vnc)
3	172.20.120.14	svrapp3.utn.edu.ec	22/tcp (ssh) 139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 5900/tcp (vnc) 5901/tcp (vnc) 5903/tcp (vnc) 5904/tcp (vnc) 5906/tcp (vnc) 5907/tcp (vnc) 7001/tcp (http) 9001/tcp (http) 9002/tcp (tcpwrapped)
4	172.20.120.15	terminalserver.utn.edu.ec	139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 3389/tcp (ms-wbt-server?) 5800/tcp (vnc-http) 5900/tcp (vnc)
5	172.20.120.16	svrapp1.utn.edu.ec	22/tcp (ssh) 389/tcp (ldap) 636/tcp (ssl/ldapssl?) 1521/tcp (oracle-tns) 5801/tcp (vnc-http) 5802/tcp (vnc-http) 5901/tcp (vnc) 5902/tcp (vnc) 5903/tcp (vnc) 7778/tcp (http)
6	172.20.120.31	repositorio.utn.edu.ec	22/tcp (ssh) 80/tcp (http) 139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 5432/tcp (postgresql) 5901/tcp (vnc) 8080/tcp (http)
7	172.20.120.32	geoportal.utn.edu.ec	80/tcp (http) 139/tcp (netbios-ssn) 443/tcp (ssl/http) 445/tcp (netbios-ssn) 3306/tcp (mysql) 5432/tcp (postgresql) 5801/tcp (vnc-http) 5901/tcp (vnc)
8	172.20.120.38		139/tcp (netbios-ssn) 445/tcp (netbios-ssn)

9	172.20.120.42		80/tcp (http) 443/tcp (ssl/http) 902/tcp (ssl/vmware-auth)
10	172.20.120.33		139/tcp (netbios-ssn) 445/tcp (netbios-ssn)
11	172.20.120.44	utn.edu.ec	80/tcp (http) 445/tcp (netbios-ssn) 3389/tcp (ms-wbt-server?)
12	172.20.120.45	appweb.utn.edu.ec	22/tcp (ssh) 7001/tcp (http) 9001/tcp (http) 9002/tcp (http)
13	172.20.120.46	biblioteca.utn.edu.ec	80/tcp (http) 139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 5800/tcp (vnc-http) 5900/tcp (vnc)
14	172.20.120.47	online.utn.edu.ec	80/tcp (http) 1111/tcp (http) 1935/tcp (rtmp) 3389/tcp (ms-wbt-server?)
15	172.20.120.48		139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 5800/tcp (vnc-http) 5900/tcp (vnc)
16	172.20.120.49		139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 554/tcp (rtsp) 5800/tcp (vnc-http) 5900/tcp (vnc)
17	172.20.120.50	webinar.utn.edu.ec	80/tcp (http) 135/tcp (msrpc) 139/tcp (netbios-ssn) 445/tcp (netbios-ssn) 1111/tcp (http) 1433/tcp (ms-sql-s) 1935/tcp (rtmp) 2909/tcp (tcpwrapped) 11110/tcp (printer) 49152/tcp (msrpc) 49153/tcp (msrpc) 49154/tcp (msrpc) 49156/tcp (msrpc) 49158/tcp (msrpc) 49163/tcp (msrpc)
18	172.20.120.61	eventos.utn.edu.ec	22/tcp (ssh) 80/tcp (http) 443/tcp (ssl/http) 3306/tcp (mysql) 8080/tcp (http)

Fuente: *Software de escaneo de puertos NMAP*

Los puertos mencionados en la anterior tabla han sido comprobados por los administradores de cada uno de los servicios que posee la universidad, y han corroborado que los datos obtenidos son correctos.

3.3.4.- IPs PÚBLICAS

La Universidad Técnica del Norte al poseer un contrato del servicio de internet con las IPs 190.95.196.192/27, tiene a su haber 32 IP públicas las cuales serán distribuidas para cada uno de los servicios de la red mediante NAT, y se muestran en la Tabla 65:

TABLA 66.- *Distribución de IPs Públicas*

DISTRIBUCIÓN DE IPs PÚBLICAS		
N°	IP Pública	Servicio
1	190.95.196.192/27	Red CEDIA UTN Ibarra
2	190.95.196.193/27	CPE TN - Gateway
3	190.95.196.194/27	IP Firewall UTN
4	190.95.196.195/27	IP Servidor de Aplicaciones 1
5	190.95.196.196/27	IP Servidor de Aplicaciones 2
6	190.95.196.197/27	IP Servidor de Aplicaciones 3
7	190.95.196.198/27	IP Servidor de Aplicaciones Bienestar Universitario
8	190.95.196.199/27	IP Servidor WEB
9	190.95.196.200/27	IP Repositorio UTN
10	190.95.196.201/27	IP GeoPortal UTN
11	190.95.196.202/27	IP Servidor Adobe Connect
12	190.95.196.203/27	IP Servidor Streaming
13	190.95.196.204/27	IP Servidor de Virtualización (CLOUD)
14	190.95.196.205/27	IP Servidor de Potgrado
15	190.95.196.206/27	IP Servidor Biblioteca
16	190.95.196.207/27	IP Eventos UTN
17	190.95.196.208/27	IP Servidor de Terminal Server

18	190.95.196.209/27	IP Quipux
19	190.95.196.210/27	IP Servidor Aula Virtual
20	190.95.196.211/27	IP MCU Sony UTN
21	190.95.196.212/27	IP Colegio de Contadores
22	190.95.196.213/27	IP Servidor Radius
23	190.95.196.214/27	IP NAT Red Administrativos (172.16.0.0/16)
24	190.95.196.215/27	IP NAT Red Laboratorios (172.17.0.0/16)
25	190.95.196.216/27	IP NAT Wireless Docentes (172.17.112.0/21)
26	190.95.196.217/27	IP NAT Wireless Administrativos (172.17.120.0/21)
27	190.95.196.218/27	IP NAT Wireless Estudiantes (172.17.128.0/19)
28	190.95.196.219/27	IP NAT Wireless Eventos
29	190.95.196.220/27	
30	190.95.196.221/27	
31	190.95.196.222/27	
32	190.95.196.192/27	Broadcast Red CEDIA UTN Ibarra

Fuente: *Dirección de Desarrollo Tecnológico Informático*

3.4. IPS

El Sistema de Prevención de Intrusos estará configurado mediante el proyecto Suricata, el cual es un motor IDS/IPS bajo la plataforma del Open Source. El antecesor a éste es el IDS por excelencia Snort el cual ha sido por años el mejor Sistema de Detección de Intrusos, pero a partir del año 2009 hasta la actualidad (Junio del 2014), la comunidad de OISF[22] ha llevado a Snort a un nuevo nivel llamado Suricata.

3.4.1. CARACTERÍSTICAS DE SURICATA

A continuación se presentan las características por las que Suricata es considerado el mejor IPS bajo la plataforma del Open Source.

[22] OISF = Open Information Security Fundation

3.4.1.1. MOTOR DE TRABAJO

Suricata trabaja en modo IDS o IPS, Monitorea la seguridad de la red, análisis offline de archivos PCAP[23], grabación del tráfico mediante el uso del log PCAP y tratamiento automático de los archivos PCAP. Todos estos modos de trabajo ubican a Suricata como uno de los mejores IDS/IPS de la actualidad.

3.4.1.2. COMPATIBILIDAD CON SISTEMAS OPERATIVOS

Suricata es compatible con cualquier plataforma de sistema operativo tales como: Linux, FreeBSD, OpenBSD, Mac OS X y Windows. Debido a que su arquitectura es Open Source no es recomendable trabajar en los sistemas operativos Windows debido a que se reducen algunas de las características propias del software libre.

3.4.1.3. CONFIGURACIÓN

A diferencia de Snort el cual su archivo de configuración era Snort.conf; en Suricata se tiene el archivo Suricata.yaml el cual se encuentra organizado y es legible tanto por el software como por el administrador.

3.4.1.4. SOPORTE TCP/IP

El motor de flujo para el análisis de TCP/IP es escalable ya que posee un completo soporte para IPv6, también posee la decodificación de túneles para: Teredo, IP-IP, IPv6-IPv4, IPv4-IPv6 y GRE[24].

3.4.1.5. ANALIZADOR DE PROTOCOLOS

Suricata tiene un motor donde analiza los paquetes de IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, RAW, SLL, VLAN y QinQ. Así como también el análisis en la capa de aplicación para HTTP, SSL, TLS, SMB, SMB2, DCERPC, SMTP, FTP, SSH, DNS.

3.4.1.6. MOTOR DE ANÁLISIS PARA HTTP

Posee un analizador HTTP integrado en la librería libhtp, analiza el archivo lo extrae y guarda hasta el origen del URL. Posee palabras clave para que coincidan con los buffers.

---

[23] PCAP = Packet Capture, Archivos de captura de datos.
[24] GRE = Generic Routing Encapsulation; Protocolo para el establecimiento de túneles virtuales a través de la Internet.

3.4.1.7. SALIDA DE RESULTADOS

Mediante el módulo de estadísticas que posee Suricata cuenta los elementos de rendimiento y muestra los resultados del análisis dependiendo la necesidad del administrador: HTTP logs, TLS logs, logs de alertas rápidas, PCAP logs, syslogs, peticiones y respuesta DNS, entre otros. Una de las desventajas que posee Suricata es que por default presenta sus resultados mediante logs, si se desea acceder mediante WEB o una GUI es necesario crear mediante un framework como por ejemplo Codeigniter, Java, o cualquier otro desarrollador de aplicaciones WEB.

3.4.1.8. FILTRADO DE ALERTAS/EVENTOS

Los motores de filtrado de las diferentes alertas y eventos que posee Suricata pueden ser configurados de tres maneras: filtrado de alertas por cada regla, filtrado de alertas globales, y filtrado de alertas por host o red.

3.4.1.9. REPUTACIÓN IP

Suricata luego de analizar los paquetes comparte la información de direcciones IP que poseen mala reputación con las demás organizaciones afines al desarrollo del software.

3.4.1.10. MULTI-THREADING

La principal característica de Suricata es Multi-Threading que consiste en analizar los paquetes en varios hilos (Threads) logrando así aprovechar el rendimiento multinúcleo de los procesadores actuales, estableciendo que cada uno de los núcleos del procesador analice uno o varios hilos del motor de Suricata.

Cada Hilo existen 4 módulos: Adquisición de Datos, Decodificación de Paquete, Flujo de Datos y Detecciones y Salidas. El módulo de adquisición de datos es aquel que se encarga de leer el paquete desde la red; el módulo de decodificación del paquete es el que interpreta el paquete; en el módulo de flujo de datos se cumplen tres pasos: traking o asegurar la conexión de red, reconstruir el paquete original y finalmente analizar el paquete comparando con las firmas de seguridad. Por último el módulo de detecciones y salidas se analiza todas las alertas y eventos y se muestra en los logs. En la imagen 30 se muestra un esquema de trabajo de los módulos de cada hilo de Suricata.

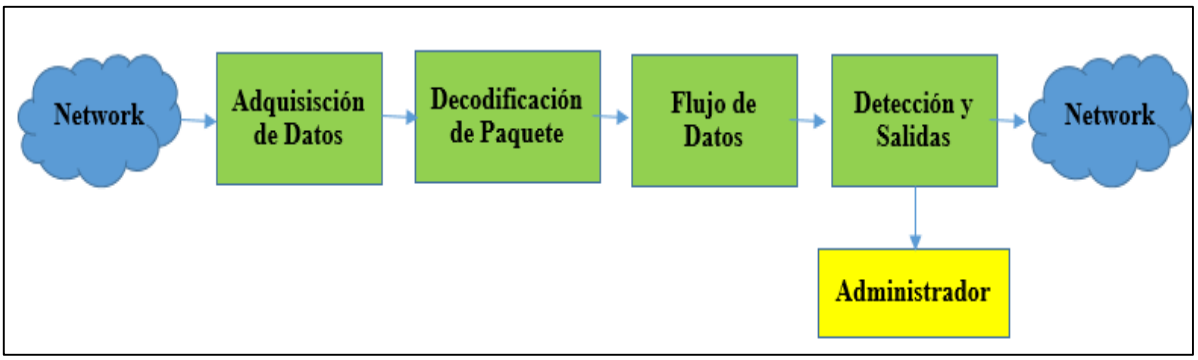


IMAGEN 30.- *Esquema de los módulos de Suricata*
Fuente: *Basado en Investigación Teórica - Práctica*

3.4.2. COMPARATIVA CON OTROS IDS/IPS COMERCIALES

En el mercado existen varias empresas que brindan los servicios de IDS/IPS cada una de ellas son propietarias y para obtener los beneficios que ofertan es necesario cancelar la licencia de funcionamiento, a diferencia de Suricata que es Open Source. En la Imagen 31 se muestra el cuadrante de Gartner de los IPS a fecha Julio del 2012. SourceFire es la empresa desarrolladora del IDS/IPS basado en software libre Snort y se observa que se encuentra en segundo lugar de los líderes según Gartner, es por eso la confiabilidad que se tiene al Open Source para temas de Seguridad Informática.

IMAGEN 31.- *Cuadrante de Gartner de los IPS*
Fuente: *http://itsecdom.blogspot.com/2012/08/el-cuadrante-magico-de-gartner-ips.html*

A continuación se presenta una comparación entre Suricata y los IPS propietarios, véase Tabla 66.

TABLA 67.- *Comparación de Suricata vs IPS propietarios*[25]

N°	Característica	IDS/IPS Propietarios	Suricata
1	Multi-Threading	NO	SI
2	Soporte para IPv6	Cisco, IBM, Stonesoft	SI
3	IP Reputation	Cisco	SI
4	Detección Automática de Protocolos	NO	SI
5	Aceleración con GPU	NO	SI
6	Variables Globales/Flowbit	NO	SI
7	GeoIP	NO	SI
8	Análisis Avanzado de HTTP	NO	SI
9	HTTP Access Logging	NO	SI
10	SMB Access Logging	NO	SI
11	Anomaly Detection	SI	NO
12	Alta disponibilidad	SI	SI
13	GUI de Administración	SI	NO
14	Open Source	NO	SI

Fuente: *"Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial", ESPOL 2011*

[25] Tabla obtenida de "Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial", ESPOL 2011

3.5. METODOLOGIA PARA LA IMPLEMENTACION DE POLITICAS DE SEGURIDAD.

Hoy en día la información que transcurre por la red de datos asi como la automatización de los servicios prestados por la Universiad son reconocidos como un activo valioso para la entidad, es por ello que se requiere contar con estrategias tecnológicas que permitan el control y administración de los datos de manera efectiva.

Con la presentación de la presente metodología de Seguridad Perimetral, donde se incluyen las políticas de administración y gestión de todos los componentes de redes y comunicaciones; la Universidad Técnica del Norte pretende establecer conductas del buen uso de la red de datos a todo el personal universitario, logrando así reducir a un minimo los ataques informáticos y en caso de suceder uno, solucionarlo de manera eficiente y efectiva.

3.5.1.- SOBRE LA SEGURIDAD PERIMETRAL DE LA RED

“La seguridad perimetral basa su filosofía en la protección de todo sistema informático de una empresa desde fuera, es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático.” Taboada, Eduardo. (2005). Es por ello que se deben cumplir requisitos para tener una completa seguridad de la información en la red.

3.5.1.1.- Identifiación

Se denomina identificación al momento en que el usuario se da a conocer al sistema.

3.5.1.2.- Autenticación

Es la verificación de que el individuo que se ha identificado al sistema, es seguro.

3.5.1.3.- Control de Accesso

Es la administración correcta de los usuarios que acceden a los servicios de red.

3.5.1.4.- Disponibilidad

Se refiere que los servicios que se ofrecen dentro de la red, estén operativos al 100% del tiempo y en caso de fallas tengan un tiempo de recuperación rápido.

3.5.1.5.- Confidencialidad

Trata sobre la protección de la información que los usuarios seguros cursan dentro de la red de datos ante usuarios no autorizados.

3.5.1.6.- Integridad

Es la protección de los datos y transmisiones contra las alteraciones no autorizadas o accidentales que pueden ocurrir dentro de la red.

3.5.1.7.- Responsabilidad

Es realizar un seguimiento y almacenamiento de todas las actividades seguras, accidentales y no autorizadas que se den dentro de la red.

3.5.2.- GLOSARIO DE TÉRMINOS

Para la comprensión de las políticas de seguridad es necesario el entendimiento de los siguientes términos.

- ✓ **Administrador de Red.-** Persona capacitada y especializada en gestionar los recursos de red informática.
- ✓ **Cableado Estructurado.-** Tendido de cables de par trensado, coaxial y fibra óptica, debidamente certificado y etiquetado.
- ✓ **Cuarto de Comunicación.-** Es el área dedicada al alojamiento exclusivo de equipos informáticos asociado al cableado de telecomunicaciones.
- ✓ **Dirección IP.-** Es una etiqueta numérica compuesta por cuatro números enteros entre 0 y 255 el cual es único e identifica al equipo dentro de la red.
- ✓ **DMZ.-** Zona desmilitarizada, sector de la red donde se encuentran alojados los servidores
- ✓ **LAN.-** Red de área local
- ✓ **SSID.-** Service Set Identifier, nombre asignado a una red Wireless.
- ✓ **Subred.-** Porcion de la red, que constituye una nueva red lógica.
- ✓ **Usuario.-** Persona que utiliza los recursos de la red de datos, previo a su autenticación y registro dentro del sistema.
- ✓ **WAN.-** Red de área global.

3.5.3.-COMITÉ ORGANIZACIONAL

La presente metodología para la seguridad informática será estructurada por ingenieros en Sistemas Informáticos y Redes de Comunicación, de la Dirección de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte, la estructuración de este comité es planteada por el Director del DDTI y esta compuesta por:

- ✓ Director de Desarrollo Tecnológico e Informático UTN
- ✓ Jefe de Proyectos, DDTI UTN
- ✓ Jefe de Asistencia al Usuario, DDTI UTN
- ✓ Administrador de Redes y Comunicaciones DDTI UTN

El comité organizacional deberá revisar y actualizar una vez al año presentando las propuestas de corrección mediante oficio institucional al comité calificador.

3.5.4.- COMITÉ CALIFICADOR

La presente metodología para la seguridad informática debe ser aprobada por la máxima autoridad, el Honorable Consejo Universitario (HCU), para su implementación y difusión a la comunidad universitaria. El HCU se encuentra conformado por:

- ✓ Rector
- ✓ Vicerrectora Academica
- ✓ Vicerrector Administrativo
- ✓ Decano FICAYA
- ✓ Subdecano FICAYA
- ✓ Decano FICA
- ✓ Subdecano FICA
- ✓ Decano FACAE
- ✓ Subdecano FACAE
- ✓ Decano FECYT
- ✓ Subdecano FECYT
- ✓ Decano FCCSS
- ✓ Subdecana FCCSS
- ✓ Presidente Asociación General de Profesores
- ✓ Presidente Asociación Empleados y Trabajadores
- ✓ Director Financiero
- ✓ Director Planeamiento
- ✓ Procurador General
- ✓ Directora Bienestar Universitario
- ✓ Director DDTI
- ✓ Director CUIYT
- ✓ Director Postgrado
- ✓ Director Vinculación
- ✓ Directora Comunicación Organizacional

- ✓ Director CAI
- ✓ Directora Gestión Recursos Humanos
- ✓ Director CUDIC
- ✓ Coordinadora Relaciones Internacionales
- ✓ Director de Construcciones
- ✓ Representante Empleados y Trabajadores
- ✓ Presidente FEUE-I
- ✓ Representante Estudiantil FICAYA
- ✓ Representante Estudiantil FECYT
- ✓ Representante Estudiantil FACAE
- ✓ Representante Estudiantil FCCSS
- ✓ Representante Estudiantil FICA

3.5.5.- ALCANCE

Estas políticas de seguridad se aplicarán en cada una de las dependencias Universitarias, y a todo el personal Universitario, cualquiera que sea su situación contractual, la dependencia en la que trabaje y el nivel de tareas que realice. En caso del no cumplimiento de este documento, el HCU será quien tome las acciones pertinentes según la gravedad.

3.5.6.- OBJETIVOS

Los objetivos que se deben cumplir son:

- ✓ Administrar y proteger toda la Información de la Universidad Técnica del Norte, conjuntamente con los equipos tecnológicos utilizados para su procesamiento.
- ✓ Mantener las Políticas de Seguridad Perimetral actualizada y operativa de acorde a las necesidades que genere la red de datos institucional.
- ✓ Definir las acciones para la correcta valoración, análisis y evaluación de los resultados.

3.5.7.- POLITICAS

En el presente documento se determinan las políticas de seguridad perimetral, siendo este el resultado del análisis de los datos obtenidos en la auditoría de red y en base a los servicios que brinda la red universitaria, este es un primer paso para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Universidad Técnica del Norte.

3.5.7.1.- De la red de datos

- ✓ La red WAN tendrá un rango de direcciones IP de la siguiente subred: 190.95.196.192/27.
- ✓ La red DMZ tendrá un rango de direcciones IP de la siguiente subred: 10.24.8.0/24
- ✓ La red LAN se encuentra divida en dos subredes, una para los administrativos y otra para acceso de estudiantes y laboratorios.
- ✓ La subred LAN de administrativos tendrá un rango de direcciones IP de la siguiente subred: 172.16.0.0/16
- ✓ La subred LAN de estudiantes y laboratorios tendrá un rango de direcciones IP de la siguiente subred: 172.17.0.0/16

3.5.7.2.- De los cuartos de comunicaciones

El cuarto de comunicaciones es el principal componente de la red universitaria de datos.

- ✓ El acceso al cuarto de comunicaciones es restringido y solamente autorizado por el Administrador de Redes y Comunicaciones.
- ✓ Todos los equipos que posean servicios de red, deben encontrarse alojados en el cuarto de comunicaciones.
- ✓ En cada una de las facultades existen cuartos de comunicación, donde se alojan equipos de acceso a la red.
- ✓ El cuarto de comunicaciones deben poseer aire acondicionado de acorde a las dimensiones del mismo.
- ✓ El cuarto de comunicaciones debe poseer un sistema de ventilación acorde a las dimensiones del mismo.

3.5.7.3.- De los servidores

- ✓ Todos los servicios que presta la universidad a su personal administrativo y estudiantil, se encuentran alojados en servidores dentro del Cuarto de Comunicaciones.
- ✓ Cada servidor debe ser administrado por el personal capacitado de la Dirección de Desarrollo Tecnológico e Informático.
- ✓ El acceso a la administración de los servidores es restringido y exclusivo de quien lo administra.
- ✓ Se debe respaldar la información una vez al mes.

3.5.7.4.- De la seguridad informática

- ✓ Se asignará una cuenta de acceso a todos los usuarios de la red institucional, siempre y cuando se encuentre registrado en el sistema integrado de la Universidad.
- ✓ Se permitirá el uso de internet a todos los usuarios dentro de la red de datos universitaria.
- ✓ Se permitirá el acceso a los servidores de la red universitaria a todos los usuarios dentro y fuera de la red de datos universitaria.
- ✓ Se bloquearan las peticiones de acceso a puertos que no utilicen los servicios que presta la red de datos universitaria.
- ✓ Se monitoreará una vez al mes los puertos habilitados en cada uno de los servidores de la red universitaria.
- ✓ En caso de existir ataques a la red se bloquearán las IPs de origen del ataque.
- ✓ Se bloqueará el acceso a redes sociales dentro del campus universitario.
- ✓ Se habilitará el uso de redes sociales previa autorización del señor rector de la Universidad Técnica del Norte.
- ✓ La longitud minima de caracteres permitidos en una contraseña se establece en 6, los cuales tendrán una combinación alfanumérica entre mayúsculas y minúsculas.
- ✓ La longitud máxima de caracteres permisibles en una contraseña se establece en 12.

3.5.7.5.- De la red cableada

- ✓ Todos los puntos de acceso a la red de datos deben ser registrados y aprobados por el Administrador de Redes y Comunicaciones.
- ✓ Todos los equipos de red deben utilizar IP estática correspondiente a su respectiva VLAN.
- ✓ La IP de los equipos conectados a la red cableada serán registradas por el Administrador de Red.
- ✓ El cambio de dirección IP debe ser autorizada y realizada por el Administrador de Redes y Comunicaciones o su delegado.
- ✓ Se deben conectar equipos de red, previa autorización del Administrador de Redes y Comunicaciones.
- ✓ Los equipos conectatos a la red cableada pertenecen al lugar de trabajo, no al personal que desempeña en dicho lugar.
- ✓ El equipo del usuario conectado a la red cableada, está sujeto a monitoreo, pruebas de penetración y auditorías de seguridad.
- ✓ No visitar sitios web pornográficos o de contenido ilícito.

- ✓ Cualquier equipo que represente un riesgo de seguridad para la red de comunicaciones del campus universitario, podrá ser desconectado de la red y la persona que tenga registrado el equipo será notificado.
- ✓ Se debe respaldar la información de los equipos activos de red una vez al mes.
- ✓ Cualquier situación que no se pueda resolver con usuarios referente al sistema de red cableado, será referido al DDTI ubicado en el Edificio Central de la UTN específicamente al Área de Redes y Comunicaciones para tomar la decisión que sea necesaria.

3.5.7.6.- De la red inalámbrica[26]

- ✓ El mantenimiento de la seguridad de la red inalámbrica de la universidad requiere métodos que aseguren que sólo los usuarios autorizados puedan tener acceso al mismo. De tal manera, el equipo debe tener las seguridades físicas necesarias para evitar que se vean afectados los servicios de la red inalámbrica.
- ✓ Todos los puntos de acceso deben de ser registrados y aprobados por el administrador de la Red.
- ✓ La instalación, administración y uso de los dispositivos de la red inalámbrica debe estar de acuerdo con las especificaciones y normas de redes inalámbricas y con las políticas implantadas en la universidad.
- ✓ El SSID debe estar configurado para que sea identificado con la universidad.
- ✓ Ningún individuo debe conectar ni instalar cualquier equipo de comunicaciones a la red sin la previa autorización del administrador.
- ✓ Las comunicaciones inalámbricas no proveen codificación de los datos transmitidos. La protección de los datos es responsabilidad del usuario.
- ✓ No se debe permitir ni fomentar el uso de la red inalámbrica para utilizar los sistemas administrativos de la Universidad donde se transmiten o reciben datos confidenciales.
- ✓ El equipo del usuario conectado a la red inalámbrica, está sujeto a monitoreo, pruebas de penetración y auditorías de seguridad.
- ✓ Cualquier equipo que represente un riesgo de seguridad para la red de comunicaciones del campus universitario, podrá ser desconectado de la red y la persona que tenga registrado el equipo será notificado.
- ✓ Cualquier situación que no se pueda resolver con usuarios referente al sistema de red inalámbrica, será referido al DDTI ubicado en el Edificio Central de la UTN específicamente al Área de Redes y Comunicaciones para tomar la decisión que sea necesaria.

[26] Tomada de la Tesis “Implementación de la red inalámbrica que garantice la performance de administración mediante el acceso a los recursos de red en la Universidad Técnica del Norte” de Vinicio Guerra.

3.5.7.7.- de la red telefónica

- ✓ Los usuarios que poseen teléfonos IP, son responsables del buen uso del mismo.
- ✓ Existen 4 niveles de prioridad telefónica: General, Apoyo, Asesoría y Ejecutivo.
- ✓ Todos los usuarios tienen prioridad para llamadas en la categoría General.
- ✓ Para habilitar permisos superiores a la categoría General, debe ser autorizada por la máxima autoridad universitaria.
- ✓ El equipo telefónico pertenece al puesto de trabajo, no al personal que labora en el mismo.
- ✓ Los usuarios deben hacer buen uso del servicio telefónico.
- ✓ Los usuarios se hacen responsables de la clave de seguridad
- ✓ La clave de seguridad para llamadas esta compuesta de 4 dígitos seguidos de la tecla numeral.

3.5.7.8.- Del correo electronico

- ✓ El servicio de correo electrónico es un servicio gratuito para todo el personal administrativo, docente y estudiantil de la Universidad Técnica del Norte.
- ✓ El correo electrónico es de exclusivo uso académico y administrativo
- ✓ El Administrador de Correo Electrónico se reservará el derecho de monitorear las cuentas de usuario que presenten un comportamiento inadecuado.

3.5.7.9.- De la seguridad física

- ✓ El cableado estructurado de la Universidad Técnica del Norte debe estar certificado.
- ✓ El cableado estructurado de la Universidad Técnica del Norte debe estar etiquetado.
- ✓ Cada cuarto de equipos debe encontrarse cerrado y el acceso debe ser autorizado por el Administrador de redes y Comunicación.
- ✓ Cada cuarto de equipos debe poseer un sistema de aire acondicionado.
- ✓ Cada cuarto de equipos debe poseer alarmas de alerta de incendios.
- ✓ Cada cuarto de equipos debe poseer extintor contra incendios.
- ✓ Cada cuarto de equipos debe poseer sistema contra incendios.
- ✓ Cada cuarto de equipos debe poseer UPS.
- ✓ Cada cuarto de equipos debe poseer circuitos de energía eléctrica redundante.
- ✓ Cada cuarto frio debe tener cámaras de vigilancia.

3.5.7.10.- Del personal universitario

- ✓ El usuario es responsable de mantener sus contraseñas en secreto.

- ✓ El usuario es responsable del uso y acceso a los servicios de la red Universitaria.
- ✓ No proporcionar datos personales por medio de correo o teléfono.
- ✓ Se prohíbe la excesiva o abusiva navegación por Internet con fines extra laborales.
- ✓ Se prohíbe la transmisión de información confidencial a personal que no labore en la Universidad Técnica del Norte

CAPÍTULO IV

4. IMPLEMENTACIÓN DE LA SEGURIDAD PERIMETRAL EN EL ENTORNO DE RED

En este capítulo se detalla el proceso de instalación de las diferentes etapas que comprenden el Sistema de Seguridad Perimetral, la implementación de la nueva segmentación y direccionamiento de IP, así como la configuración del servidor en el cual se alberga el firewall y el IPS.

4.1. CONFIGURACIÓN DE LOS EQUIPOS ACTIVOS DE RED

Para la implementación de la nueva segmentación en la Red de Datos Universitaria se debe seguir una secuencia de procedimientos, los cuales permiten que el cambio lógico no altere las funcionalidades de la red. Estos pasos se los describe a continuación, y su configuración se encuentra detallada en el Anexo 02.

- **Respaldar la Información**

Antes de realizar cualquier cambio es recomendable sacar todas las configuraciones que se encuentren en los equipos activos de red lo cual permite que en el caso de existir inconvenientes al situar las nuevas configuraciones, se coloca las configuraciones anteriores y no existirá ningún problema.

- **Respaldar la configuración de interfaces.**

El presente proyecto presenta una nueva distribución lógica de red, más no física; es por ello que se debe respaldar la configuración de a que VLAN pertenece cada una de las Interfaces de los Switchs, y al momento de colocar las nuevas configuraciones en los equipos asignar cada uno de los puertos a su determinada y nueva VLAN. El listado de los puertos y sus respectivas VLANs lo puede ver en el Anexo 03.

- **Cambio de direccionamiento IP**

Posterior a respaldar la información de los equipos activos de red, se debe cambiar únicamente el direccionamiento IP al Chasis Blade y a los equipos de red activos tanto Switch de Core y Switchs de Acceso, este procedimiento se lo debe hacer en el siguiente orden: Chasis Blade, Switchs de Acceso y Switchs de Core, ya que si se lo realiza primero en el Switch de Core se pierde conectividad con los demás equipos y para poder realizar alguna configuración se debe ir al cuarto de equipos de cada uno de los Switchs y configurarlos mediante la consola.

- **Configuración Switch de Core Principal**

Luego de haber cambiado las IPs a todos los equipos de red se procede a eliminar la configuración actual e ingresar la nueva configuración al Switch de Core Principal, la cual incluye los siguientes campos:

- ✓ Configuración de Nombre
- ✓ Configuración de las contraseñas para ingreso de consola y telnet
- ✓ Configuración del Banner
- ✓ Configuración de VTP Server
- ✓ Configuración de las nuevas VLANs
- ✓ Configuración de la IP en las Interfaces de VLAN
- ✓ Configuración de los Enlaces de Trunk
- ✓ Configuración del Enrutamiento por defecto

- **Configuración de los Switchs de Acceso**

Luego de haber configurado al Switch de Core se procede a la configuración de los demás Switchs de Acceso, a los cuales se ingresa mediante la IP que se configuró anteriormente. En la nueva configuración consta:

- ✓ Configuración de Nombre
- ✓ Configuración de contraseñas para ingreso de Consola y Telnet
- ✓ Configuración del Banner
- ✓ Configuración de VTP Client
- ✓ Configuración de los enlaces Trunk

- **Configuración de las interfaces de los Switchs**

Finalmente se debe configurar cada uno de las interfaces del Switch, agregándolas a las respectivas VLANs

4.2. CONFIGURACIÓN DE LOS ELEMENTOS PRINCIPALES DEL FIREWALL

Para el funcionamiento del Firewall, los pasos de instalación se pueden observar en el Anexo 06, se deben configurar varios ficheros en los cuales se encuentran editadas las zonas de nuestra red, las interfaces del firewall y las reglas que permitirán o denegarán el acceso a los diferentes servicios. En la Imagen 32, se muestra la pantalla de Shoreline por el cual se accede a las diferentes configuraciones del Firewall.

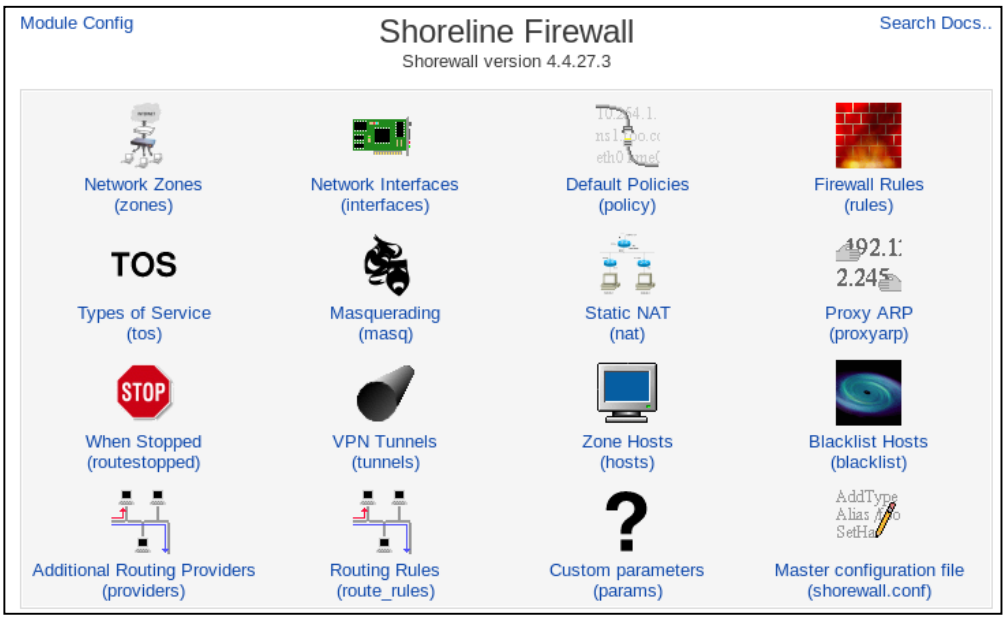


IMAGEN 32.- *Pantalla de configuración del Shoreline Firewall*

Fuente: *Servicio Shorewall*

Los archivos de configuración quue se deben editar para el funcionamiento del Firewall y que se los realiza mediante Shoreline Firewall son: Network Zones, Network Interfaces, Default Policies, Firewall Rules y Dinamic NAT.

4.2.1. NETWORK ZONES

Representan las redes que se conectarán al firewall, para la implementación de seguridad perimetral en la Universidad Técnica del Norte se establecen 4 zonas:

- ✓ fw.- Representa al sistema propio del firewall a implementar.
- ✓ dmz.- Representa a la DMZ donde se encuentran los servidores de la Universidad.
- ✓ local.- Representa la intranet de la Universidad.
- ✓ net.- Representa la salida a Internet.

En la Imagen 33, se muestra la configuración de las zonas en Shoreline.

Zone ID	Parent zone	Zone type	Comment
dmz		IPv4	Hacia la DMZ
local		IPv4	Hacia la Red Local
net		IPv4	Hacia Internet
fw		Firewall system	

IMAGEN 33.- *Zonas configuradas en Shoreline*

Fuente: *Servicio Shorewall*

4.2.2. NETWORK INTERFACES

Son todas las interfaces instaladas en el servidor y que se configurarán para la implementación de las reglas de seguridad, en el Firewall de la Universidad se necesita tres interfaces todas ellas Ethernet 10/100/1000 y se encuentran distribuidas de la siguiente manera, véase Imagen 34.

- ✓ eth0.- En esta interfaz se conecta el enlace hacia el internet.
- ✓ eth1.- En esta interfaz se conecta el enlace hacia la DMZ
- ✓ eth2 y eth3.- En estas interfaces se conectan los enlaces principales y backup hacia la intranet.

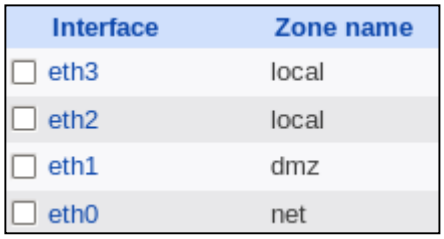


IMAGEN 34.- *Interfaces de red configuradas en Shoreline*
Fuente: *Servicio Shorewall*

Debido a que no existe enlace de backup en la red universitaria para la red local se configurará una sola interfaz de red.

4.2.3. DEFAULT POLICIES

Son políticas por defecto que se deben configurar en Firewall, debido a que se utiliza la política de todo lo que no es específicamente permitido se niega, se deben negar todas las transmisiones entre las diferentes zonas que se crean en el servidor Firewall, éstas políticas son las últimas en ser analizadas dentro de la configuración del Firewall, primero se analiza las Firewall rules y todo lo que no se encuentre permitido en dichas reglas será denegado por estas políticas. También existe una política por defecto que indica Negar el tráfico desde cualquier origen hacia cualquier destino que se analiza al finalizar todas las Firewall Rules y las Default Policies.

Para establecer las Default Policies se necesita analizar las zonas que se interconectarán mediante el firewall, en la Tabla 67, se indica el alcance que tiene cada una de las zonas y en la Imagen 35, se muestra las zonas de origen, las zonas de destino y la política seteada en DROP lo que indica que no se permiten las conexiones entre ellas.

TABLA 68.- *Default Policies establecidas para la red Universitaria*

N°	Zona Origen	Zona Destino	Descripción	Acción
1	Dmz	Net	Desde la DMZ hacia la red externa	Denegar (DROP)
2	Dmz	Local	Desde la DMZ hacia la intranet	Denegar (DROP)
3	Dmz	Firewall	Desde la DMZ hacia el servidor Firewall	Denegar (DROP)
4	Local	Dmz	Desde la intranet hacia la DMZ	Denegar (DROP)
5	Local	Net	Desde la intranet hacia la red externa	Denegar (DROP)
6	Local	Firewall	Desde la intranet hacia el servidor Firewall	Denegar (DROP)
7	Net	Dmz	Desde la red externa hacia la DMZ	Denegar (DROP)
8	Net	Local	Desde la red externa hacia la intranet	Denegar (DROP)
9	Net	Firewall	Desde la red externa hacia el servidor Firewall	Denegar (DROP)
10	Any	Any	Desde cualquier origen hacia cualquier destino	Denegar (DROP)

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Source zone	Destination zone	Policy
dmz	net	DROP
dmz	local	DROP
dmz	Firewall	DROP
net	dmz	DROP
net	local	DROP
net	Firewall	DROP
local	net	DROP
local	dmz	DROP
local	Firewall	DROP
Any	Any	DROP

IMAGEN 35.- *Configuración de Default Policies en el Shoreline*

Fuente: *Servicio Shorewall*

4.2.4. FIREWALL RULES

Mediante las Firewall Rules se crea las diferentes políticas de seguridad en donde se especifica el origen, el destino, el puerto de comunicación y se establece si se permite o no el acceso. Al momento de estar en marcha el servidor Firewall estas reglas son las primeras en ser analizadas y dado el caso que no exista una política se realizará lo que especifica las Default Policies es decir se negará todo.

Para la configuración de las Firewall Rules se tendrá en cuenta los puertos que necesita cada uno de los servicios que presta y necesita la red informática de la Universidad y se permitirá el acceso solo a dichos puertos. Por motivos de seguridad no se indican específicamente cuales son las políticas establecidas en el Firewall.

Las reglas de seguridad empleadas se las describe a continuación en forma general.

- ✓ Desde la Internet hacia la DMZ y hacia la Intranet solo se habilitarán los puertos necesarios por cada uno de los servicios.
- ✓ Desde la DMZ hacia la Internet y la Intranet sólo se habilitarán los puertos necesarios por cada uno de los servicios.
- ✓ Desde la Intranet hacia la DMZ y hacia la Internet sólo se habilitarán los puertos necesarios por cada uno de los servidores, y la misma configuración servirá para cada una de las interfaces de la zona local del firewall.
- ✓ Se habilitará solamente a determinados equipos de la Dirección de Desarrollo Tecnológico e Informático para el acceso hacia el Firewall.

4.2.5. DINAMIC NAT

El NAT ayuda a traducir las direcciones IPv4 Privadas a IPv4 Públicas es por ello que se debe configurar las reglas necesarias para que los diferentes segmentos de red interna de la Universidad Técnica del Norte salgan por el pull de direcciones IPv4 públicas que tiene asignado. Además se realiza un NATEO interno debido a la existencia de la DMZ y a que ésta tiene un direccionamiento IP diferente al resto de la red.

Para realizar el NATEO de los servidores que posee la red Universitaria se utilizara una IPv4 pública por cada uno, al existir dos subredes en la Intranet una para la parte Administrativa y otra para la parte de acceso de los estudiantes se utilizarán IPsv4 diferentes, esto se lo puede realizar ya que no se sobrepasa el número de IPsv4 públicas que tiene asignada la Universidad.

4.3. CONFIGURACIÓN DE LOS ARCHIVOS DE SURICATA

Luego de la instalación del IPS Suricata, la cual se indica en el Anexo 07, se debe proceder a la configuración de varios parámetros que se encuentran en el archivo de configuraciones de Suricata. Para acceder al archivo de configuraciones digite en la consola:

nano etc/suricata/surucata.yaml

Los valores que se deben configurar dentro de este archivo de configuración son los siguientes:

- **max-pending-packets**

Esto representa el número de paquetes que puede procesar al mismo tiempo, esto depende de las capacidades del equipo servidor donde se encuentra alojado el IDS/IPS Suricata.

max-pending-packets:2000

- **action-order**

Indica el orden de la acción que ocurre cuando se establece una coincidencia con una de las reglas establecidas, las acciones son: *pass*, *drop*, *reject* y *alert*; y vienen establecidas por defecto.

action-order:

-pass

-drop

-reect

-alert

- **outputs**

Antes de todo se debe configurar el directorio en donde se guardarán las salida de los eventos de alerta

default-log-dir: /var/log/suricata

s mediante:

Luego se procede a la configuración de la salida de alertas. Para el registro de las alertas basadas en línea; las cuales se guardan en un archivo donde cada alerta ocupa una línea del mismo mostrando una descripción breve de la alerta, la hora en la que se activó la alerta y las direcciones IPs de las que proviene; se debe habilitar mediante *enabled:yes*, se debe agregar un nombre *filename:fast.log*, se debe configurar para que al momento de reiniciar el IDS/IPS no se sobre-escriba el archivo mediante *append:yes* y se le da un tamaño en MB con *limit:32*, de la siguiente manera

-fast:

enabled:yes

filename:fast.log

append:yes

limit:32

La salida de alertas mediante barnyard2 que se lo realiza por medio de las alertas unified, es muy importante para cuando se desea enviar todas las alertas o eventos detectados por el IDS/IPS Suricata hacia una base de datos externa. Se habilita mediante *enabled:yes*, se le asigna un nombre *filename:unified2.alert* y se le da un tamaño al archivo en MB *limit:32*, como se muestra a continuación:

- unified2-alert:

enabled: yes

filename: snort.unified2

limit: 32

Las salidas de los eventos HTTP se graban en el archivo http.log en el cual se debe habilitarlo por medio de *enabled:yes* y verificar su nombre *filename:http.log*.

- http-log:

enabled: yes

filename: http.log

La salida a syslog, el cual es el estándar para envío de los registros que se generan en una red de datos se lo debe habilitar o deshabilitar de la siguiente manera.

– syslog:

enabled: no

facility: local5

format: “[%i] — “

level:info

- **stats**

Muestra las estadísticas que se generan en el motor del IDS/IPS Suricata, se las debe habilitar mediante *enabled:yes*, agregar un nombre al archivo *filename:estadísticas.log*, indicar el tiempo en el cual se refreseca la generación de las estadísticas en segundos *interval:5* y especificar si se desea sobreescribir el archivo o no *append:yes*.

- stats:

enabled: yes

filename: estadisticas.log

interval: 5

append: yes/no

- **Motor de Detección de Alertas**

El motor de detección de las alertas crea grupos internos de todas las firmas de seguridad, y tomando en cuenta que hay varias firmas de seguridad que no serán utilizadas para todo el tráfico de la red, es necesario crear los grupos de firmas para optimizar el rendimiento y procesamiento del motor de detección. La desventaja es que si se crean varios grupos baja el rendimiento de los procesadores, a menos que el servidor donde se encuentre alojado tenga grandes capacidades, según la OISF si se va a procesar un troughput superior a 200 MB y el servidor posee grandes prestaciones, es recomendable configurar varios grupos dando así un perfil alto en el performance del motor de detección de alertas, como por ejemplo:

detect-engine:

-profile:high

This is the default setting.

-custom-values:

toclient_src_groups:2

toclient_dst_groups:2

toclient_sp_groups:2

toclient_dp_groups:3

toserver_src_groups:2

toserver_dst_groups:4

toserver_sp_groups:2

- **Afinidad de los CPU**

Cuando se posee un servidor con varios procesadores, se debe aprovechar la característica de multi-threading, en la cual se permite asignar uno o varios procesadores a los diferentes hilos que ejecuta Suricata. Si se asigna varios procesadores para un hilo se pueden elegir el modo de trabajo de los mismos ya sean “balanced” para repartir el procesamiento entre todos los procesadores del hilo o “exclusive” para asignar un procesador específico al hilo. La configuración se lo hará de la siguiente manera.

Cpu_affinity:

-management_cpu_set:

cpu:[5-7]

-receive_cpu_set:

cpu:[all]

-decode_cpu_set:

cpu:[0, 1]

mode:”balanced”

- **Definición de la red**

Para que el motor del IDS/ISP Suricata comience a analizar el tráfico se debe agregar las redes a las cuales se encuentra conectado.

vars:

address-groups:

HOME_NET: "[192.168.1.0/24, 10.20.0.0/16, 172.20.0.0/16]"

EXTERNAL_NET:any

HTTP_SERVERS:"$HOME_NET"

SMTP_SERVERS:"$HOME_NET"

SQL_SERVERS:"$HOME_NET"

DNS_SERVERS:"$HOME_NET"

TELNET_SERVERS:"$HOME_NET"

Luego de haber realizado las configuraciones necesarias en el archivo suricata.yaml es necesario puentear las interfaces de red, ya que Suricata analizará el tráfico que pase por él.

brctl addbr br0

brctl addif br0 eth1

brctl addif br0 eth0

ip li set br0 up

ip li set eth1 up

ip li set eth0 up

También se debe agregar una regla en las IP-Tables para que se envié el tráfico a las colas que el motor IDS/IPS Suricata lee.

- A FORWARD -i eth0 –j NFQUEUE

Finalmente para ejecutar Suricata como IPS se debe ejecutar el comando

suricata –c /etc/suricata/suricata.yaml -q id_cola

CAPÍTULO V

5. PRUEBAS DE FUNCIONAMIENTO DE LA SEGURIDAD PERIMETRAL

En el presente capítulo se presenta las pruebas de funcionalidad del sistema de seguridad perimetral, donde se implementa las dos etapas: Segmentación de red y Seguridad de la Red.

5.1. PRUEBAS DE LA SEGMENTACIÓN DE LA RED.

La nueva segmentación de red y el nuevo direccionamiento IP realizado en la Red de Datos Universitaria se lo realizó en el Switch de Core y para ello se muestra las configuraciones efectuadas en dicho equipo.

En la Imagen 36 se muestra la configuración de VTP en el Switch de Core, el cual permite la propagación de las VLANs creadas en el mismo.

```
SW-ZEUS#show vtp status
VTP Version                     : 2
Configuration Revision          : 1390
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 45
VTP Operating Mode              : Server
VTP Domain Name                 : UTN2014
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x23 0x4B 0x5F 0x7E 0xD8 0xDF 0x94 0x40
Configuration last modified b  0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 172.16.1.2 on interface Vl1 (lowest numbered VLAN interface
found)
SW-ZEUS#
```

IMAGEN 36.- *Configuración de VTP en el Switch de Core*

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Se puede observar el número de VLANs creadas, el modo de operación VTP que para el Switch de Core es en modo server y el dominio del protocolo VTP en este caso UTN2014. También muestra la IP del equipo que por confidencialidad se ha borrado el último octeto; en la Imagen 37 se puede ver la configuración de un Switch cualesquiera de la red con la configuración de VTP en modo cliente.

```
SW-ARISTOTELES>ena
Password:
SW-ARISTOTELES#show vtp status
VTP Version                     : 2
Configuration Revision          : 1310
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 45
VTP Operating Mode              : Client
VTP Domain Name                 : UTN2014
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEB 0xEF 0x1E 0x35 0x27 0xE7 0xDA 0x3C
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
```

IMAGEN 37.- *Configuración de VTP en un Switch de la Red Universitaria.*

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

En la Imagen 38 se muestra todas las VLANs creadas en el Switch de Core y que por medio de VTP se propagarán hacia los demás Switchs.

VLAN	Name	Status
1	default	active
2	EQUIPOS_ACTIVOS	active
4	EDIFCENTRAL-FINANCIERO	active
5	EDIF-CENTRAL-AUTRIDADES-TESIS	active
6	EDIFCENTRAL-DEPTINFORMATICA	active
7	CECI	active
8	EDIFCENTRAL-AUTORIDADES	active
10	EDIFCENTRAL-ADMINISTRATIVOS	active
12	EDIFCENTRAL-COMUN.ORGANIZACIONAL	active
14	FICA-ADM	active
16	FICA-LAB	active
18	FICA-CISCO	active
20	FICAYA-ADM	active
22	FICAYA-LAB	active
24	CEC-UTN	active
26	POSTGRADO	active
28	CAI-ADM	active
30	CAI-LAB	active
32	FFCCSS-ADM	active
34	ESTUDIANTES.FFCCSS	active
36	BIBLIOTECA-ADM	active
37	VLAN0037	active
38	ESTUDIANTES.BIBLIOTECA	active
40	FECYT-ADM-ED.FISICA	active
42	FECYT-LAB	active
44	FACAE-ADM	active
46	FACAE-LAB	active
48	AUDITORIO	active
52	MILTONREYES-ADM	active
54	MILTONREYES-LAB	active
64	TELEFONIA-IP	active
66	COPIADORA	active
68	Wireless-FICA	active
70	WPRUEBA-DOCENTES	active
72	WPRUEBA-ADMINISTRATIVOS	active
74	WPRUEBA-ESTUDIANTES	active
96	WIRELESS-DOCENTES	active
112	WIRELESS-ADMINISTRATIVOS	active
120	NAT-DMZ-INTERNO	active
121	PUBLICAS	active
122	DMZ	active
123	INSIDE-SERVIDORES	active
128	WIRELESS-ESTUDIANTES	active
160	WIRELESS-EVENTOS	active
168	ENLACE_BANCO_DEL_PACIFICO	active

IMAGEN 38.- *VLANs creadas en el Switch de Core.*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Para cada una de las VLANs se ha creado un pool de direcciones IP para DHCP, además se excluye las IPs que son necesarias para la administración es decir las primeras 20 direcciones. En la Imagen 39 se muestra las configuraciones de DHCP y las IPs excluidas del mismo en una de las VLANs creadas.

```
ip dhcp excluded-address 172.16.5.1 172.16.5.20
ip dhcp pool EDIF-CENTRAL-AUTORIDADES-TESIS
   network 172.16.5.0 255.255.255.0
   default-router 172.16.5.1
   dns-server 172.16.1.158
```

IMAGEN 39.- *DHCP e IPs excluidas de la VLAN 5 configuradas en el Swich Core*
Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

En los equipos CISCO la información creada en el Switch de Core se propagará mediante VTP, en cambio en los equipos 3COM existentes en la Red Universitaria al no tener propagación de las VLANs por medio de VTP, es necesario crear manualmente las VLANs. En la Imagen 40 se muestra la creación de las VLANs en los Switch 3COM.

```
----------------------SW-HERACLES-ENLACES, Switch 2 - FECYT (1)---------
Select menu option (bridge/vlan): create
Select VLAN ID (2-4094)[3]: 5
Enter VLAN Name [VLAN 5]: EDIF-CENTRAL-AUTORIDADES-TESIS
```

IMAGEN 40.- *Creación de las VLANs en equipos 3COM*
Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Para poder observar las VLANs creadas se accede manualmente al menú *summary* y despliega todas las VLANs creadas en el equipo, en la Imagen 41 se muestra el detalle de las VLANs creadas en uno de los equipos 3COM.

```
----------------------SW-HERACLES-ENLACES, Switch 2 - FECYT (1)---------
Select menu option (bridge/vlan): summary
Select VLAN ID (1-2,5,10,12,14,22,32,40,52,56,60,64,all)[all] : all

VLAN ID   Name
----------------------------------------
1         Default VLAN
2         APs
5         EDIF-CENTRAL-AUTORIDADES-TESIS
10        Administrativos UTN
12        COMUNICACION ORGANIZACIONAL
```

IMAGEN 41.- *Resumen de las VLANs creadas en un equipo 3COM*
Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Luego de crear la VLAN es necesario agregar los puertos que pertenecerán a dicha VLAN. En la Imagen 42 se muestra la forma de agregar un puerto a determinada VLAN. Se debe

seleccionar la VLAN deseada, luego el puerto a asignarse y dependiendo si es trunk o acceso seleccionar tagged o untagged respectivamente.

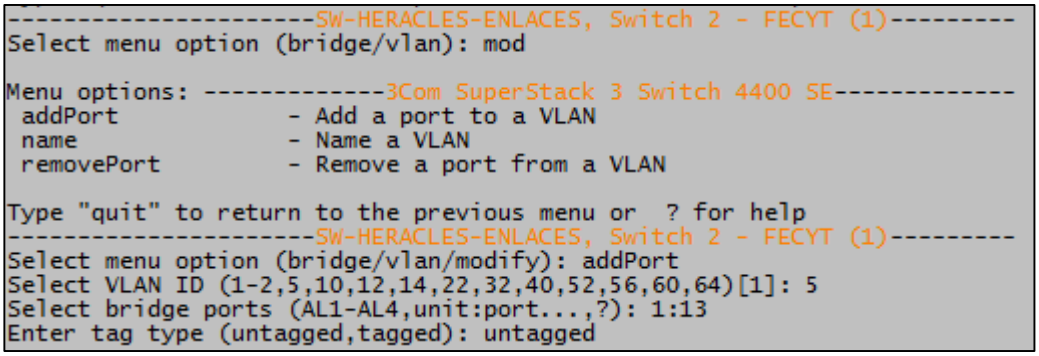


IMAGEN 42.- *Agregación de un puerto a la VLAN correspondiente*
Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

En la Red Universitaria existen equipos Cisco Small Business los cuales no poseen VTP es por ello que se debe configurar vía WEB donde se crea manualmente las VLANs y se agrega los puertos de red. En la Imagen 43 se indica la creación de las VLANs en los equipos Cisco Small Business.

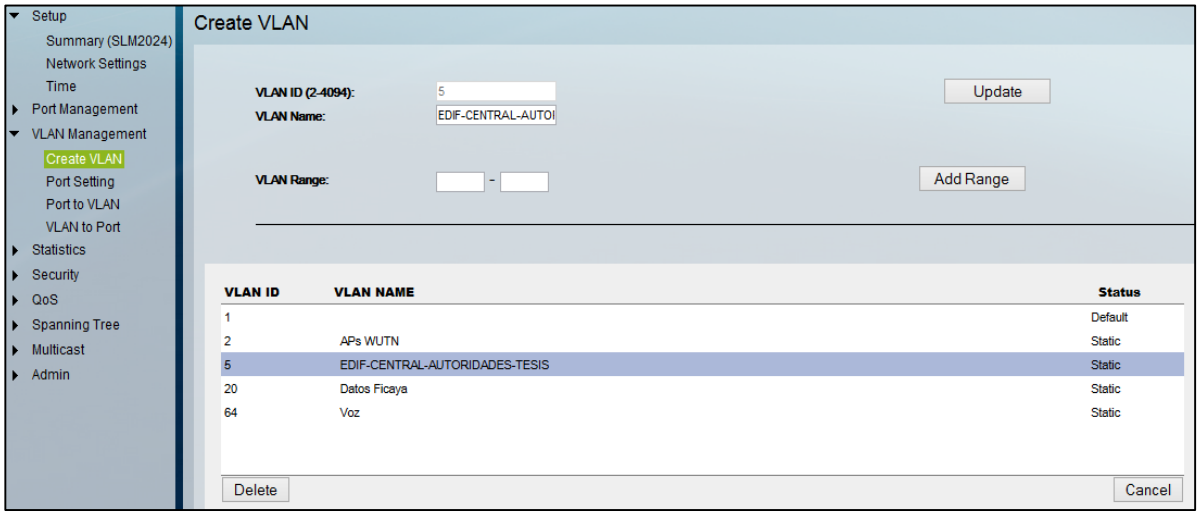


IMAGEN 43.- *Creación de VLANs en equipos Cisco Small Business*
Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

En la Imagen 44 se observa la configuración manual de los puertos, para agregarlos en la VLAN respectiva es necesario seleccionar la opción *untagged* en los puertos de acceso y la opción *tagged* en los puertos de trunk.

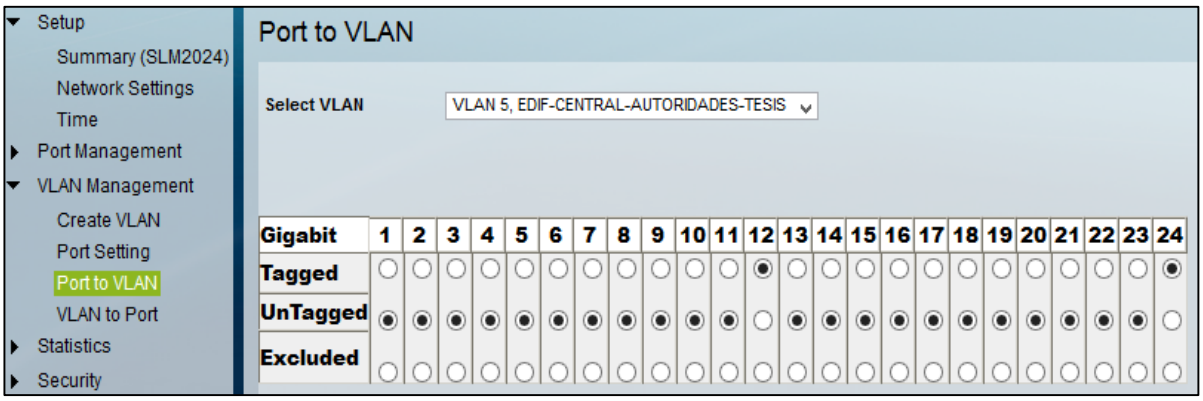


IMAGEN 44.- *Configuración de los puertos de los equipos Cisco Small Business*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Luego de haber realizado la configuración en los diferentes equipos de red es necesario comprobar la conectividad, es por ello que en la Imagen 45 se muestra la dirección IP de un computador conectado a la VLAN 5.

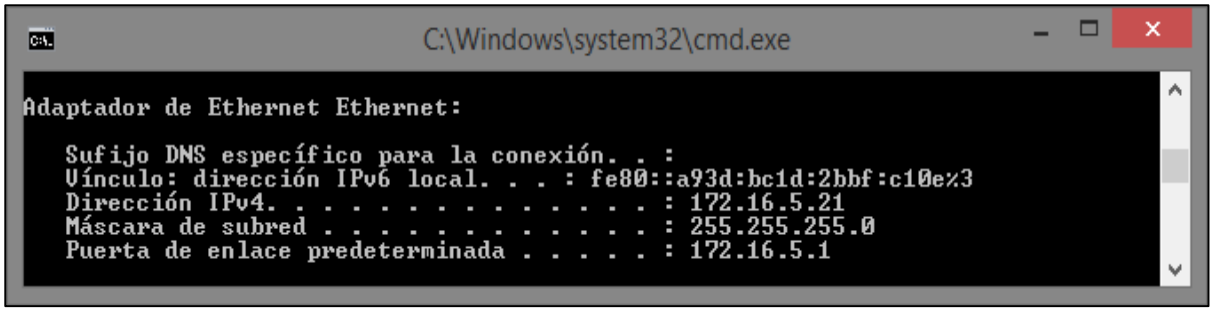


IMAGEN 45.- *IP del computador conectado a la VLAN 5*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Luego de revisar la configuración en la computadora se procede a revisar si tiene servicio de internet, en la Imagen 46 se observa el ping realizado a www.google.com.

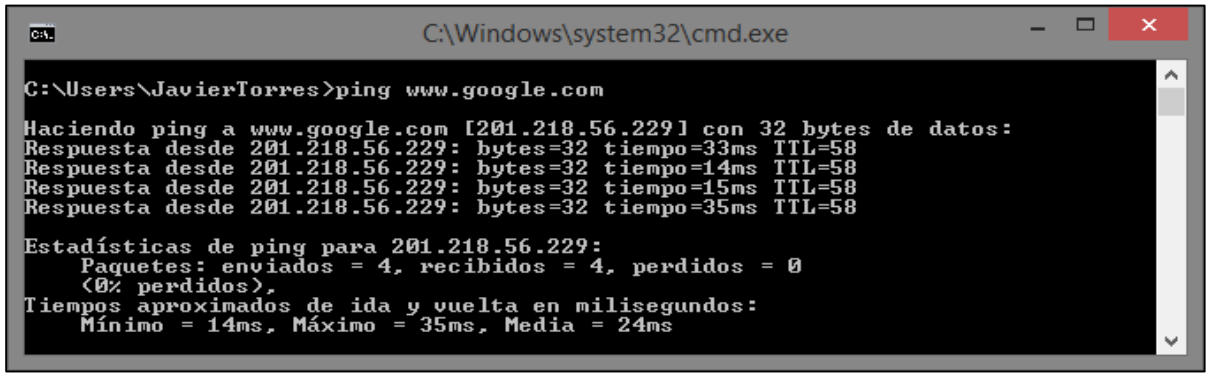


IMAGEN 46.- *Ping hacia www.google.com como prueba de acceso a internet*

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

5.2. PRUEBAS DE LA SEGURIDAD DE LA RED

En esta sección se colocó IPs aleatorias para su explicación, dichas IPs no concuerdan con las IPs configuradas en los servicios de la Universidad por motivos de seguridad, las IPs públicas son de conocimiento general y pertenecen a la red de la Universidad Técnica del Norte pero de igual manera no coinciden con las IPs de los servicios prestados.

Para la demostración de que el Firewall e IPS se realizarán pruebas que indiquen el funcionamiento de las diferentes configuraciones dentro de dichos equipos. Lo primero a comprobar es la salida hacia el internet, mediante NAT se traducen las IPs privadas a las IPs públicas que posee la Universidad. En la Imagen 47 se muestra el NATEO realizado en el equipo firewall donde todas las redes internas de la Universidad salen por la interfaz pública en este caso la WLAN0.

Outgoing interface	Network to masquerade
190.95.196.219 on wlan0	172.16.0.0/16
190.95.196.220 on wlan0	172.17.0.0/16
190.95.196.221 on wlan0	172.18.0.0/24

IMAGEN 47.- *Configuración de DNAT para salida a internet.*
Fuente: *Equipo Firewall, Dirección de Desarrollo Tecnológico e Informático – UTN*

La máquina en la que se realizó las pruebas tiene la IP 172.15.5.21 asignada mediante DHCP, quiere decir que la IP pública por la que tendrá salida hacia el internet es la IP 190.95.196.219, para comprobar es necesario visitar la página web: *http://www.whatismyip.com/es/*, la Imagen 48 muestra la IP pública a la cual se está realizando el NAT.

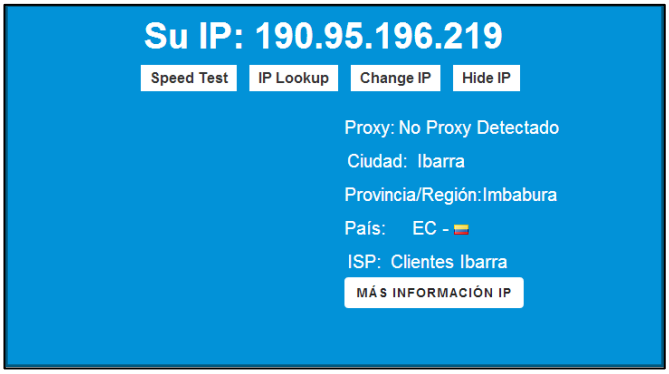


IMAGEN 48.- *Resultado de la consulta de la IP pública.*
Fuente: *http://www.whatismyip.com/es/*

También se debe configurar el NAT hacia la DMZ en este caso se lo debe realizar servicio por servicio, se lo realiza tanto para la red interna como para la red externa, en la Imagen 49 se muestra la configuración NAT para la DMZ.

External address	External interface	Internal address
172.16.5.10	eth0	10.24.8.10
172.16.5.11	eth0	10.24.8.11
172.16.5.12	eth0	10.24.8.12
172.16.5.13	eth0	10.24.8.13
172.16.5.14	eth0	10.24.8.14
10.24.8.10	eth1	172.16.5.10
10.24.8.11	eth1	172.16.5.11
10.24.8.12	eth1	172.16.5.12
10.24.8.13	eth1	172.16.5.13
10.24.8.14	eth1	172.16.5.14
10.24.8.198	wlan0	190.95.196.198
190.95.196.198	eth0	10.24.8.198

IMAGEN 49.- *Configuración de NAT para la DMZ*

Fuente: *Equipo Firewall, Dirección de Desarrollo Tecnológico e Informático – UTN*

La Universidad tiene su servidor web alojado en *www.utn.edu.ec* ubicado dentro de su la DMZ de la misma con una IP privada que pertenece a la VLAN de la misma, para comprobar si se encuentra realizado correctamente el NAT se debe usar el comando *nslookup* en la consola de Windows, el comando nslookup permite ver la dirección IP de determinado URL. En la Imagen 50 se muestra la IP pública de la Universidad mediante el comando nslookup.

```
C:\Users\karlita>nslookup www.utn.edu.ec
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  192.168.1.1

Respuesta no autoritativa:
DNS request timed out.
    timeout was 2 seconds.
Nombre:  www.utn.edu.ec
Address:  190.95.196.198
```

IMAGEN 50.- *Respuesta de nslookup de la URL www.utn.edu.ec*

Fuente: *PC externa a la red universitaria*

Los puertos que serán habilitados son solamente los que cada uno de los servicios necesite, en la Imagen 51 se observa ejemplos de la habilitación de puertos para cada una de las zonas que tiene la red, cabe indicar que solamente existirán configuraciones de permitir ya que la regla por defecto es denegar todo el tráfico.

Action	Source	Destination	Protocol	Source ports	Destination ports
ACCEPT	Zone net - Hacia el Internet	Host 190.95.194.211 in zone net - Hacia el Internet	TCP	222	222
ACCEPT	Zone net - Hacia el Internet	Host 190.95.194.211 in zone net - Hacia el Internet	TCP	3306	3306
ACCEPT	Zone net - Hacia el Internet	Host 190.95.194.211 in zone net - Hacia el Internet	TCP	4433	4433
ACCEPT	Zone net - Hacia el Internet	Host 190.95.194.211 in zone net - Hacia el Internet	TCP	465	465
ACCEPT	Zone net - Hacia el Internet	Host 190.95.194.211 in zone net - Hacia el Internet	TCP	10000	10000
ACCEPT	Zone local - Hacia la Intranet	Host 10.24.8.11 in zone dmz - Hacia la DMZ	ICMP	Any	
ACCEPT	Host 10.24.8.11 in zone dmz - Hacia la DMZ	Zone net - Hacia el Internet	Any		
ACCEPT	Zone local - Hacia la Intranet	Zone local - Hacia la Intranet	ICMP	Any	
ACCEPT	Host 172.20.6.204 in zone net - Hacia el Internet	Firewall	Any		

IMAGEN 51.- *Ejemplos de reglas de firewall.*

Fuente: *Equipo Firewall – Dirección de Desarrollo Tecnológico e Informático – UTN*

En el análisis realizado en la sección 2.6. del presente proyecto, se detectaron varios puertos destinados a servidores de juegos online y que se encontraban habilitados. Para comprobar que ya se encuentra bloqueado estos servicios online se seleccionó el servidor de juegos *Steam*, la cual es una plataforma de servicios multi-jugador. Los puertos de comunicación que utiliza Steam son diferentes a los que se han habilitado en el firewall de la red Universitaria, mirar Imagen 52, por ello no es posible la ejecución del software, tal como se muestra en la Imagen 53.

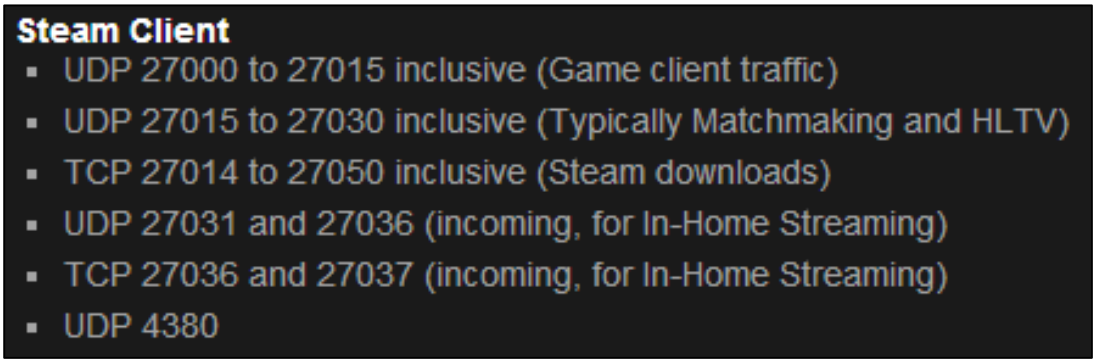


IMAGEN 52*.- Puertos de comunicación de la plataforma de juegos Steam*

Fuente: *https://support.steampowered.com/kb_article.php?ref=8571-GLVN-8711*

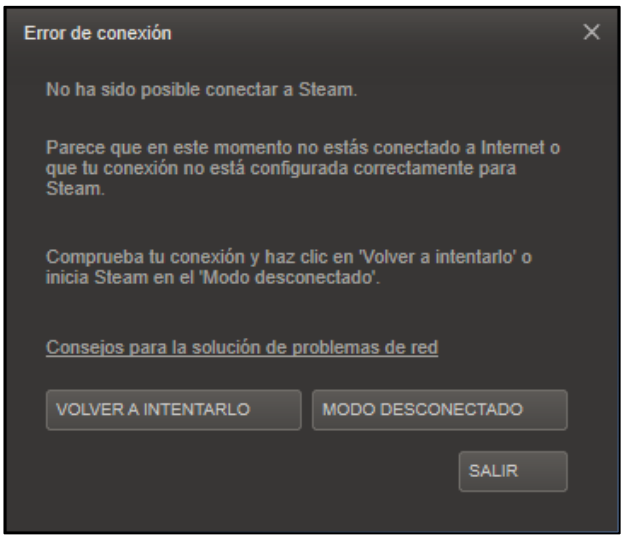


IMAGEN 53.- *Error de conexión de la plataforma de juegos online Steam*
Fuente: *Plataforma de juegos Steam*

Como resultado del análisis antes mencionado, existían varios puertos de comunicación pertenecientes a servidores de juegos on-line, con la implementación de las correctas políticas de seguridad implementadas donde se habilitan los puertos de comunicación exclusivos de cada uno de los servicios que presta la universidad, se logra bloquear el acceso a dichos servidores de juegos así como también impiden el paso de tráfico no deseado desde y hacia la red Universitaria.

CAPÍTULO VI

6. ANÁLISIS ECONÓMICO

En este último capítulo se realiza un análisis económico de los elementos utilizados en la implementación del Sistema de Seguridad Perimetral en comparación con los equipos que posee la red universitaria y soluciones propietarias.

Debido a que la nueva segmentación de red y nuevo direccionamiento IP se lo realiza en los equipos de red existentes, solo se analizará el software y hardware necesario para la implementación del Firewall e IPS.

6.1. PRESUPUESTO DE SOFTWARE Y HARDWARE UTILIZADO

Para la instalación del servidor de virtualización y las máquinas virtuales para el Firewall e IPS, se sugieren los equipos mostrados en la Tabla 68:

TABLA 69.- *Presupuesto de Hardware*

PRESUPUESTO DE HARDWARE SUGERIDO		
Cant.	Descripción	Valor
1	Servidor HP Proliant	$ 1120
1	Monitor LED 22”	$ 130
1	UPS CyberPower CP1500AVRLCD	$ 140
1	Teclado HP	$ 22
1	Mouse HP	$ 13
1	CPU HP Pavilion p2-1310 Desktop	$ 240
	TOTAL	$ 1665

Fuente: *Basado en cotizaciones de empresas de telecomunicaciones*

La Universidad dentro de sus activos fijos posee varios de los equipos mencionados en la anterior tabla, es por ello que los equipos necesarios para su adquisición se reducen al Servidor HP Proliant y al UPS, dando un total de $1260.

En el desarrollo de este proyecto también se utilizó diferente Software, los cuales son detallados en la Tabla 69.

TABLA 70.- *Presupuesto de Software*

PRESUPUESTO DE SOFTWARE UTILIZADO			
Cant.	Software	Descripción	Valor
1	ZOC	Software para conexiones a equipos de red.	$ 0
1	XenServer	Software para virtualización	$ 0
1	XenCenter	Software para administración de máquinas virtuales	$ 0
1	CentOS	Sistema Operativo bajo plataforma Open Source	$ 0
1	Shorewall	Software para administración de Firewall	$ 0
1	Webmin	Software para administración de Shorewall	$ 0
1	Suricata	Software para administración de IPS	$ 0
		TOTAL	$ 0

Fuente: *Basado en investigación Teórica Práctica*

Debido a que todos los Software que son utilizados en la implementación de este proyecto son bajo arquitecturas del Open Source y de descarga libre, no presenta algún costo para la Universidad. En la Tabla 70 se muestra el presupuesto total del proyecto.

TABLA 71.- *Presupuesto total del proyecto*

PRESUPUESTO TOTAL DEL PROYECTO		
Cant.	Descripción	Valor
1	Presupuesto de Hardware Sugerido	$ 1665
1	Presupuesto de Software Utilizado	$ 0
	TOTAL	$ 1665

Fuente: *Basado en Investigación Teórica Práctica*

6.2. PRESUPUESTO DE EQUIPOS EXISTENTES EN LA RED UNIVERSITARIA

En la red universitaria se encuentra instalado y funcionando un Firewall, más no un IPS. El equipo que se encuentra configurado como Firewall es el ASA 5520 el cual es propietario de la marca Cisco. El valor de este equipo se encuentra en los $2725, y viene con la licencia original Cisco como también el software de administración de los productos ASA llamado Cisco ASDM-IDM Launcher.

El equipo servidor donde en el cual se pretendía instalar los servicios de Firewall e IPS es un equipo IBM Power 710, el cuál con las características mencionadas en la sección 3.2.1, tiene un valor aproximado de $3800 y el respectivo software de virtualización IBM VIOS tiene un valor de $1000 dólares. En la tabla 71.

TABLA 72.- *Presupuesto de la solución con equipos existentes*

PRESUPUESTO DE LA SOLUCIÓN CON EQUIPOS EXISTENTES EN LA UNIVERSIDAD TÉCNICA DEL NORTE		
Cant.	Descripción	Valor
1	Cisco ASA 5520	$ 2725
1	Servidor IBM Power 710 Express	$ 3800
1	Software de Virtualización IBM VIOS	$ 1000
	TOTAL	$ 7525

Fuente: *Basado en cotizaciones de empresas de telecomunicaciones*

6.3. PRESUPUESTO DE UNA SOLUCIÓN PROPIETARIA

Dentro del mercado existen varias empresas orientadas a la seguridad informática, las cuales brindan a sus clientes la oportunidad de adquirir un appliance ya estructurados para la seguridad de la red como son IBM, HP, Cisco entre otros (observar imagen 33, Cuadrante de Gartner, sección 3.4.2 de este documento). En la Tabla 72 se muestran dos soluciones propietarias de seguridad perimetral

TABLA 73.- *Cotización de soluciones propietarias para seguridad perimetra l*

PRESUPUESTOS DE SOLUCIONES PROPIETARIAS		
Cant.	Descripción	Valor
1	Check Point 12400 Appliance Next Generation Threat Prevention	$ 61787,74
1	Licencia 2-Year NG TP Package for 12400 Appliance	$ 25276,18
1	Cisco ASA IPS Edition	$ 13393,99
	TOTAL	$ 100457,91

Fuente*: Basado en cotizaciones de empresas de telecomunicaciones*

Como se puede observar en la tabla anterior las soluciones propietarias para seguridad perimetral son verdaderamente costosas, ya que se debe adquirir tanto el equipo como la licencia de funcionamiento.

6.4. ANÁLISIS COSTO BENEFICIO

Carreño, U (2013) afirma que: “El análisis costo-beneficio, es una evaluación socioeconómica del programa o proyecto a nivel de prefactibilidad, y consistirá en determinar la conveniencia de un programa o proyecto de inversión mediante la valoración en términos monetarios de los costos y beneficios asociados directa e indirectamente, incluyendo externalidades, a la ejecución y operación de dicho programa o proyecto de inversión.”

Para el análisis costo beneficio es necesario elaborar dos listas donde se detallan los costos del proyecto y los beneficios que acarrea el mismo, agregando junto con los valores señalados en las secciones anteriores del este capítulo, finalmente sumarlos y obtener el valor total de los costos y beneficios. En la Tabla 73 se muestra los valores de los costos y en la Tabla 74 se muestra los valores de los beneficios del proyecto, la relación que se realiza es entre la solución presentada y una posible solución propietaria a adquirirse.

TABLA 74.- *Costos del proyecto presentado*

COSTOS			
N°		Descripción	Valor
1	Hardware	Servidor HP Proliant	$ 1120
2		Monitor LED 22”	$ 130
3		UPS CyberPower CP1500AVRLCD	$ 140
4		Teclado HP	$ 22
5		Mouse HP	$ 13
6		CPU HP Pavilion p2-1310 Desktop	$ 240
7	Software	ZOC	$ 0
8		XenServer	$ 0
9		XenCenter	$ 0
10		CentOS	$ 0
11		Shorewall	$ 0
12		Webmin	$ 0
13		Suricata	$ 0
		TOTAL COSTOS	**$ 1665**

Fuente: *Basado en cotizaciones de empresas de telecomunicaciones*

TABLA 75.- *Beneficios del proyecto presentado*

BENEFICIOS		
N°	Descripción	Valor
1	Compra de equipo dedicado para Firewall	$ 61787,74
2	Licencia para 2 años del equipo Firewall	$ 25276,18
3	Compra de equipo dedicado para IPS	$ 13393,99
	TOTAL BENEFICIOS	**$ 100457,91**

Fuente: *Basado en cotizaciones de empresas de telecomunicaciones*

Para el cálculo del análisis costo beneficio es necesario la utilización de la fórmula indicada en la Ecuación 1:

$$C/_B = \frac{BENEFICIOS}{COSTOS}$$

Ecuación 1.- *Fórmula del análisis costo beneficio*

Fuente: *Blank, Leland (2006). Ingeniería Económica. McGrawHill. México*

Si la relación C/B es cero o positivo, indica que el proyecto debe realizarse caso contrario si la relación C/B es negativa el proyecto debe rechazarse. En la Ecuación 2 se muestra la relación C/B del proyecto.

$$C/_B = \frac{\$\ 100457{,}91}{\$\ 1665} = 60{,}34$$

Ecuación 2.- *Relación C/B del proyecto*

Fuente: *Basado en los valores obtenidos en el proyecto*

El resultado de la relación Costo-Beneficio C/B es un valor positivo de 60,34 lo que quiere decir que el proyecto se debe aceptar al brindar mayores beneficios que los costos que se generarán. Con la implementación del proyecto y la utilización de software libre permite que por cada dólar de inversión en este proyecto en el transcurso de 2 años (tiempo de duración de la licencia del equipo firewall propietario) la Universidad Técnica del Norte se ahorrará USD 59,34 con respecto a la solución propietaria.

CONCLUSIONES

Al finalizar el presente proyecto de titulación se han obtenido las siguientes conclusiones:

- ✓ La seguridad informática es indispensable para las redes de datos de la actualidad, debido al crecimiento agigantado de las comunicaciones globales también crece la necesidad de cuidar toda la información que se genera y se transmite alrededor del mundo.
- ✓ La implementación de un sistema de seguridad perimetral ayuda a los administradores de red a proteger la información que circula por la red empresarial de una manera más eficiente, gracias a la combinación de diferentes funcionalidades que pertenecen a la misma como el Firewall, IDS e IPS.
- ✓ Para poder implementar un sistema de seguridad perimetral y que su funcionamiento sea el correcto, se debe segmentar la red de acuerdo a las necesidades y dependencias que posea la organización; así también establecer un correcto direccionamiento IP, el cual debe permitir la escalabilidad deseada a futuro por la organización en la que se implementará.
- ✓ Dentro de las diferentes plataformas de Software Libre existen aplicaciones que pueden ser utilizadas como sistemas de seguridad informática, y que gracias al open source el administrador de red puede configurarla y acoplarla a las necesidades y requerimientos que presente la red.
- ✓ La virtualización permite utilizar y aprovechar al máximo los recursos de determinado equipo, ya que al no virtualizar es necesario un equipo por cada uno de los servicios a implementar.
- ✓ En el presente trabajo de titulación se permitió unificar dos métodos de seguridad informática basados en software libre como son los Firewall y los IPS mediante Shorewall y Suricata respectivamente, para el monitoreo y detección de ataques a la red en la Red de Distribución de la Universidad Técnica del Norte.

RECOMENDACIONES

Al finalizar el presente proyecto de titulación se han obtenido las siguientes recomendaciones:

- ✓ En la red universitaria es urgente una administración adecuada de los diferentes segmentos y direcciones IP, debido a que no existe un registro de a quién pertenece cada una de las IPs y esto conlleva a que se vuelva dificultoso la gestión de las políticas de seguridad a nivel de IP.
- ✓ En el mercado existen varios software que permiten la virtualización de servicios para las empresas, utilizar XenServer permite al administrador de red utilizar todos los recursos del equipo servidor y además de explotar, según las necesidades de la organización, todas las características del servidor de virtualización.
- ✓ Las políticas de seguridad conlleva un trabajo en equipo tanto el administrador de red, trabajadores y estudiantes de la Universidad, es por ello que se recomienda la elaboración de un manual de procedimientos para el acceso y uso de los diferentes servicios de red Universitarios.
- ✓ La utilización de software libre permite al administrador de red utilizar los recursos necesarios y añadir las políticas que la red requiera, sin las limitaciones que un equipo propietario pueda generar.
- ✓ El IPS Suricata se encuentra en funcionamiento solamente por medio de la consola de administración, en un futuro se puede elaborar interfaces gráficas para su administración y permitiendo una interacción más sencilla entre el IPS Suricata y el Usuario.
- ✓ El presente proyecto da la pauta para su aplicación en redes IPv6, permitiendo el inicio para los estudios en Segmentación y Direccionamiento IPv6, Firewalls, IDS e IPS.
- ✓ Finalmente la recomendación más importante es optar por el uso de software libre y equipos no propietarios, lo que permite a la organización la reducción de costos en cada uno de los proyectos a desarrollarse.

BIBLIOGRAFÍA

LIBROS

ANGENENDT, R. & MEMBREY, P. & VERHOEVEN, T. (2009). *The Definitive Guide to CentOS.* New York: Springer-Verlag Inc.

BEAVER, K. (3era Ed.) (2010). *Hacking for Dummies.* Hoboken: Wiley Publishing Inc.

BORONCZYK, T. & NEGUS, C. (2009). *CentOS Bible*. Indianapolis: Wiley Publishing Inc.

BORKIN, M. & KRAUS, R. & PROWELL, S. (2010). *Seven Deadliest Network Atacks.* Burlington: Elsevier Inc.

CORLETTI, A. (2011). *Seguridad por Niveles.* Madrid: DarFE Learning Consulting, S.L.

ENAMORADO, L. & GARCÍA, A. & SANZ, J. (2011). *Servicios de red e Internet.* Madrid: Ibergarceta Publicaciones.

ESCRIVÁ, G. (2013). *Seguridad Informática.* Madrid: McMillan Iberia S.A.

GHEORGHE, L. (1era Ed.) (2006). *Designing and Implementing Linux Firewalls and QoS using netfilter, iproute2, NAT and L7-filter*. Birmingham: Packt Publishing Ltd.

HALLBERG, B. A. (5ta Ed.). (2009). *Networking a beginner's guide*. México: The McGraw Hill Companies.

HOBSON, J. (1era Ed.). (2013). *Centos 6 Linux Server.* Birmingham: Packt Publishing Ltd.

JORBA, J & SUPPI, R. (2da Ed.). (2007). *Sofware Libre: Proyecto en Administración de Redes y Sistemas Operativos basados en GNU/Linux*. Barcelona: Eureca Media.

KATZ, M. (2013). *Redes y Seguridad.* México: Alfaomega.

KURTZ, G. & McCLURE, S. & SCAMBRAY, J. (6ta Ed.) (2009). *Hacking Exposed: Network Security Secrets & Solutions.* The McGraw Hill Companies.

LONG, J. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.* Burlington: Syngress Publishing Inc.

MITNICK, K. & SIMON, W. (200). *Ther art of intrusión.* Indianapolis: Wilcy Publishing Inc.

ROA, J. (2da Ed.). (2013). *Seguridad Informática.* Madrid: McGraw Hill Interamericana.

STALLINGS, W. (7ma Ed.). (2008). *Comunicaciones y Redes de Computadores*. Madrid: Pearson Education S.A.

TORI, C. (1era Ed.). (2008). *Hacking Ético*. Rosario, Argentina.

TANENBAUM, A. (5ta Ed.). (2012). *Redes de Computadoras.* México: Pearson Education.

TANENBAUM, A. (3ra Ed.). (2009). *Sistemas Operativos Modernos.* México: Pearson Education.

REVISTAS

BERTHA, S. (2013). *Seguridad en el Servidor.* Revista User 256: Web Hacking, 10, 290-315.

LAWRENCE, R. (2009). *The Internet is broken.* Revista IEEE: Espectrum 07.09, 30-35.

LUCKY, R. (2012). *Wires and Wireless.* Revista IEEE: Espectrum 11.12, 24.

MARCHIONNI, E. (2011). *Configuraciones del Servidor.* Revista Users 210: Administrador de Servidores, 2, 34-71.

MARCHIONNI, E. (2011). *Seguridad Corporativa.* Revista Users 210: Administrador de Servidores, 3, 72-105.

MARCHIONNI, E. (2011). *Virtualización de Servidores.* Revista Users 210: Administrador de Servidores, 4, 106-151.

PEÑA, C. (2012). *Protección a la Red.* Revista Users 227: Redes la Guía Definitiva, 9, 210-237.

PEÑA, C. (2012). *GNU/Linux.* Revista Users 227: Redes la Guía Definitiva, Ap1, 256-269.

TESIS

Alulema Chiluisa, D. (2008). *Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors, utilizando tecnología UTM (Unified Threat Management)*. (Tesis inédita de Ingeniería). Escuela Politécnica Nacional, Quito, ECU.

Astudillo Herrera, J & Jiménez Macías, A. & Ortiz Flores, F. (2011). *Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial*. (Tesis inédita de Ingeniería). Escuela Superior Politécnica del Litoral, Guayaquil, ECU.

Giménez García, M. (2009). *Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral*. (Tesis inédita de Ingeniería). Universidad de Almería, Almería, ESP.

Plasencia Bedón, L. (2010). *Servidor AAA para validación y control de acceso de usuarios hacia la infraestructura de Networking de un ente del Ministerio de Defensa Nacional.* (Tesis inédita de Ingeniería). Disponible en el repositorio digital de la Universidad Técnica del Norte, Ibarra, ECU

Ramón Ibujés, N. (2010). *Reingeniería de la red de datos de un ente del Ministerio de Defensa Nacional (MIDENA)*. (Tesis inédita de Ingeniería). Disponible en el repositorio digital de la Universidad Técnica del Norte, Ibarra, ECU

Vinueza Jaramillo, T. (2012). *Honeynet virtual híbrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra*. (Tesis inédita de Ingeniería). Disponible en el repositorio digital de la Universidad Técnica del Norte, Ibarra, ECU.

URLS

Aguilar, A. & Francoise, J. & Solano, Y. (2010). *Que es un Firewall.* Recuperado de: http://www.slideshare.net/miriamfransua/qu-es-un-firewall

Altadill, P. (2010). *IPTABLES Manual Práctico*. Recuperado de: http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall.pdf

Alfonso, A. (2011). *IDS/IPS Suricata. Entendiendo y configurando Suricata. Parte I.* Recuperado de: http://seguridadyredes.wordpress.com/2011/02/22/ids-ips-suricata-entendiendo-y-configurando-suricata-parte-i/

Anval, A. (2013). *Snort vs Suricata.* Recuperado de: http://wiki.aanval.com/wiki/Snort_vs_Suricata

Araujo, C. (2012). *Historia de las Redes de Datos.* Recuperado de: http://pocateoriaelectronica.blogspot.com/2012/03/historia-de-las-redes-de-datos.html

Bastidas A. (2012). *Paravirtualización con Xen-Server*. Recuperado de: http://sysadmin.org.mx/contenidos/paravirtualizacion-con-xenserver.html

Barrios, J. (2011). *Introducción a las IPTABLES.* Recuperado de: http://www.alcancelibre.org/staticpages/index.php/introduccion-iptables

Barrios, J. (2013). *Cómo configurar un muro cortafuegos con Shorewall y tres interfaces de red.* Recuperado de: http://www.alcancelibre.org/staticpages/index.php/como-shorewall-3-interfaces-red

Borghello, C. (2009). *Detección de Intrusos en Tiempo Real*. Recuperado de: http://www.segu-info.com.ar/proteccion/deteccion.htm

Borghello, C. (2009). *Seguridad Lógica - Identificación y Autentificación*. Recuperado de: http://www.segu-info.com.ar/logica/identificacion.htm

Brachmann, S. (2012). *Las ventajas de CentOS.* Recuperado de: http://www.ehowenespanol.com/ventajas-centos-info_248710/

Caicedo, N. (2012). *Segmentación de Redes*. Recuperado de: http://es.scribd.com/doc/78439010/Segmentacion-de-Redes

Carreño, U. (2013). *Lineamientos para la elaboración y presentación de los análisis costo y beneficio de los programas y proyectos de inversión.* Recuperado de: http://www.shcp.gob.mx/LASHCP/MarcoJuridico/ProgramasYProyectosDeInversion/Lineamientos/costo_beneficio.pdf

Casco, M. (2009). *Iptables, el Firewall de Linux.* Recuperado de: http://elsoftwarelibre.wordpress.com/2009/07/19/iptables-el-firewall-de-linux/

Champ, C. (2012). *Snort vs Suricata vs Sagan.* Recuperado de: https://github.com/Snorby/snorby/wiki/Snort-vs-Suricata-vs-Sagan

ESPE-Q. (2012). *Comercio Electrónico - Seguridad Informática.* Recuperado de: http://www.slideshare.net/laqescobarq/comercio-elec-y-seguridad-informatica

Fernández, F (2012). *Historia de la Telegrafía.* Recuperado de: http://www.ea1uro.com/eb3emd/Telegrafia_hist/Telegrafia_hist.htm#02

Fitzsimmons, T. & Matthews, J. & White, J. (2011). *Quantitative analysis of Intrusion Detection Systems: Snort and Suricata.* Recuperado de: http://people.clarkson.edu/~jmatthew/publications/SPIE_SnortSuricata_2013.pdf

Gutiérrez, A. (2014). *Diferencia entre IP pública e IP privada.* Recuperado de: http://windowsespanol.about.com/od/RedesYDispositivos/f/IP-Publica-IP-Privada.htm

Holguín, L. (2012). *Sistema Operativo CentOS.* Recuperado de: http://luisa-holguin19.blogspot.com/

Journal, N. (2012). *Building an IDS/IPS on a Linux machine Part 1 - Preparation work.* Recuperado de: http://cyruslab.net/2012/10/10/building-an-idsips-on-a-linux-machine-part-1-preparation-work/

Kaspersky Lab (2014). *Amenazas de Seguridad en Internet.* Recuperado de: http://www.kaspersky.es/internet-security-center/threats

Lingenfelter, B. (2012). *Qué es el sistema operativo CentOS de Linux.* Recuperado de: http://www.ehowenespanol.com/sistema-operativo-centos-linux-info_323386/

Malambo, Y. (2010). *Clases de IP.* Recuperado de: http://circutronica.blogspot.com/p/clases-de-ip.html

Martínez, E. (2014). *Concepto de red y tipos de redes.* Recuperado de: http://www.eveliux.com/mx/Concepto-de-red-y-tipos-de-redes.html

Martínez, E. (2014). *Modelo de referencia OSI.* Recuperado de: http://www.eveliux.com/mx/Modelo-de-referencia-OSI.html

Martínez, K. (2013). *Segmentación y direccionamiento IP*. Recuperado de: http://redes1ti.blogspot.com/2013/02/segmentacion-y-direccionamiento-ip.html

Microsoft. (2014). *Que es un Firewall.* Recuperado de: http://windows.microsoft.com/es-xl/windows/what-is-firewall#1TC=windows-7

Mifsud, E. (2012). *Introducción a la seguridad informática - Políticas de seguridad*. Recuperado de: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=4

OISF. (2014). *Basic Setup.* Recuperado de: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Basic_Setup

OISF. (2014). *CentOS 6.5 Installation*. Recuperado de: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/CentOS_65_Installation

OISF. (2014). *Suricata all features.* Recuperado de: http://suricata-ids.org/features/all-features/

Pareja, E. (2008). *Las Redes: Comunicación del Mundo.* Recuperado de: http://lasredesmundiales.blogspot.com/2008/04/historia-de-las-redes-de-datos.html

Pérez, E. (2014). *IDS e IPS.* Recuperado de: http://www.ecualinux.com/soluciones/servicios-en-red/ids-e-ips/

Punina, C. (2011). *Virtualización vs Paravirtualización.* Recuperado de: http://prezi.com/uooqr3yql22u/virtualizacion-vs-paravirtualizacion/

Quinodóz, C. (2009). *Ventajas y desventajas de las estructuras de las redes físicas.* Recuperado de: http://profecarolinaquinodoz.com/principal/?tag=ventajas-y-desventajas-de-una-red

Ríos, R. (2012). *Switching: VLANs y VTP.* Recuperado de: http://www.slideshare.net/riosieiro/switching-vlans-y-vtp

Rilvera, R. (2012). *Diferencia entre Switch capa 2 y capa 3.* Recuperado de: http://es.scribd.com/doc/87087243/Diferencia-Entre-Switch-Capa-2-y-Capa-3

Robles, L. (2012). *Modelos de Seguridad de la Información.* Recuperado de: http://www.slideshare.net/luisrobles17/modelos-de-seguridad-de-la-informacin

Rusell, R. (2012). *Iptables (8) - Linux man page*. Recuperado de: http://linux.die.net/man/8/iptables

Saive, R. (2013). *Suricata 1.4.4 Released - A Network Intrusion Detection, Prevention and Security Monitoring System.* Recuperado de: http://www.tecmint.com/suricata-a-network-intrusion-detection-prevention-system/

Saive, R. (2014). *How to enable EPEL Repository for RHEL/CentOS 7.x/6.x/5.x.* Recuperado de: http://www.tecmint.com/how-to-enable-epel-repository-for-rhel-centos-6-5/

Salmun, A. (2012). *Forma de segmentación de Switchs capa 2, capa 3 y capa 4*. Recuperado de: http://www.teknobuilding.com/switches-capa-2-capa-3-y-capa-4/

Sawrkar, P. (2013). *Suricata 1.4.5 released! A Network Intrusion Detection, Prevention.* Recuperado de: http://prakashsawarkar.blogspot.com/2013/08/suricata-145-released-network-intrusion.html

Schar, K. (2010). *Snort 2.8.6 on CentOS 5.5 Installation and Configuration Guide.* Recuperado de: http://www.snort.org/assets/145/Install_Snort_2.8.6_on_CentOS_5.5.pdf

Silva, L (2011). *Comandos Básicos en GNU/Linux CentOS*. Recuperado de: http://www.centosni.net/comandos-basicos-en-gnulinux-centos/

Sullivan, D. (2009). *How to evaluate and manage UTM for network security*. Recuperado de: http://searchnetworking.techtarget.com/How-to-evaluate-and-manage-UTM-for-network-security

TP-LINK Technologies Co. Ltd. (2014). *Qué es DMZ.* Recuperado de: http://www.tp-link.es/article/?faqid=28

Vialfa, C. (2014). *Diferencias entre los protocolos TCP y UDP*. Recuperado de: http://es.kioskea.net/faq/1559-diferencias-entre-los-protocolos-tcp-y-udp

Vogelmann, E. (2008). *Políticas y modelos de seguridad.* Recuperado de: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonEste.pdf

ANEXO 1. - NOMENCLATURA DE EQUIPOS ACTIVOS DE RED

Los equipos activos de red que posee la Universidad tienen nombres comunes y similares en casi todas las dependencias, es decir si existen dos Switchs en un mismo rack en el primer piso de una facultad, un Switch tiene como nombre SwitchP1SW1 y el otro Switch SwitchP1SW2, la diferencia en algunos casos es solamente un número. Para ello se sugiere implementar una singular forma de nombrar a cada uno de los equipos de red, la cual consiste en utilizar nombres muy peculiares como por ejemplo: dioses del olimpo, súper héroes, anime, filósofos, entre otros. La idea principal es diferenciar a cada uno de los equipos entre todos.

A los equipos activos de red que existen en el edificio central se los identificará mediante nombres de los dioses de EL OLIMPO, tomando en cuenta que el Switch central de Core será llamado ZEUS. En la Tabla 75, se muestran los nombres que pueden ser utilizados en los Switch del Edificio Central, hay que tomar en cuenta que los equipos que se encuentran en el Edificio de Bienestar Estudiantil pertenecen a la nomenclatura y direccionamiento del Edificio Central.

TABLA 76.- *Nombres sugeridos para los equipos activos de red en el Edificio Central*

Edificio Central - EL OLIMPO	
N°	**Nombre**
1	Zeus (Switch central de core)
2	Afrodita
3	Apolo
4	Ares
5	Atenea
6	Cratos
7	Cronos
8	Eris
9	Eros
10	Hades
11	Hera
12	Heracles
13	Iris
14	Morfeo
15	Némesis
16	Nix
17	Odín
18	Perseo
19	Poseidón
20	Tritón

Fuente: Basado en Investigación Teórica y Práctica

En la Facultad de Ingeniería en Ciencias Aplicadas existen carreras en las cuales el área predominante es las Matemáticas, por ello todos los equipos activos de red que existan en la FICA llevarán como nombre el de los GRANDES MATEMÁTICOS DE LA HISTORIA. En la Tabla 76, se enlista nombres de matemáticos que pueden ser utilizados para nombrar los equipos activos de red de la FICA.

TABLA 77.- *Nombres sugeridos para los equipos activos de red en la FICA*

FICA - GRANDES MATEMÁTICOS	
N°	**Nombre**
1	Aristóteles
2	Arquímedes
3	Bernoulli
4	Copérnico
5	Coulomb
6	Descartes
7	Einstein
8	Euclides
9	Euler
10	Fourier
11	Galileo
12	Gauss
13	Laplace
14	Mileto
15	Newton
16	Pascal
17	Pitágoras
18	Poisson
19	Riemann
20	Ruffini

Fuente: *Basado en Investigación Teórica y Práctica*

Debido la complejidad de los nombres de varios ecologistas y ambientalistas reconocidos históricamente como por ejemplo Gro Harlem Brundtland, en la Facultad de Ingeniería en Ciencias Agropecuarias y Agronómicas se empleará nombres más sencillos y fáciles de recordar es por ello que se ha optado por utilizar los nombres de los SÚPER HÉROES DE LOS COMICS. En la Tabla 77, se muestran los nombres de súper héroes que pueden ser utilizados para nombrar a los equipos de red de la FICAYA

TABLA 78.- *Nombres sugeridos para los equipos activos de red en la FICAYA*

FICAYA - SUPERHEROES	
N°	**Nombre**
1	Batman
2	Cíclope
3	Colosus
4	Daredevil
5	Elektra
6	Falcon
7	Ghost-Rider
8	Hulk
9	Iron-Man
10	Loki
11	Nebula
12	Punisher
13	Rogue
14	Silver-Surfer
15	Spiderman
16	Storm
17	Thanos
18	Thor
19	Venom
20	Wolverine

Fuente: *Basado en Investigación Teórica y Práctica*

En la Faculta de Educación Ciencia y Tecnología los equipos activos de red serán representados por *GRUPOS MUSICALE*, representando el arte y cultura que se enseña en las aulas de la facultad, en la Tabla 78, se indican los nombres de grupos musicales para nombrar a los equipos activos de red.

TABLA 79.- *Nombres sugeridos para los equipos activos de red en la FECYT*

FECYT - GRUPOS MUSICALES	
N°	**Nombre**
1	AC-DC
2	Aerosmith
3	Beatles
4	Chicago
5	Cinderella
6	Europe
7	Jackson
8	Kiss
9	Metallica
10	Nirvana
11	Pink-Floy
12	Poison
13	Queen
14	R-E-M
15	Scorpions
16	The-Cure
17	The-Doors
18	The-Police
19	Toto
20	U2

Fuente: *Basado en Investigación Teórica y Práctica*

La predominación de la mujer en las aulas de la Facultad de Ciencias Administrativas y Económicas inspira a que los equipos de activos de esta facultad lleven el nombre de MUJERES haciendo un pequeño homenaje hacia ellas, en la Tabla 79, se muestran algunos de los nombres que se pueden utilizar para nombrar los equipos activos de red.

TABLA 80.- *Nombres sugeridos para los equipos activos de red en la FACAE*

FACAE - MUJERES	
N°	**Nombre**
1	Alexandra
2	Andrea
3	Carolina
4	Catalina
5	Diana
6	Eduarda
7	Elizabeth
8	Emilia
9	Estefanía
10	Isabel
11	Karen
12	María
13	Marisol
14	Martha
15	Milene
16	Nicole
17	Nohemí
18	Sarahí
19	Tamia
20	Yadira

Fuente: *Basado en Investigación Teórica y Práctica*

Los equipos activos de red de la Facultad de Ciencias de la Salud llevarán los nombres de GRANDES MÉDICOS de la historia y se los muestra en la Tabla 80.

TABLA 81.- Nombres sugeridos para los equipos activos de red en la FCCSS

FCCSS - GRANDES MÉDICOS	
N°	**Nombre**
1	Alexander-Fleming
2	Anton-Van
3	Edward-Jenner
4	Eskola
5	Francis-Peabody
6	Gregor-Mendel
7	Hipócrates
8	Karl-Koller
9	Luis-Pasteur
10	Paracelso
11	Pedro-Lain
12	Philippe-Pinel
13	Rene-Favaloro
14	Sabin
15	San-Lucas
16	Sigmund-Freud
17	Theiler
18	Viktor-Frankl
19	Weller
20	William-Harvey

Fuente: *Basado en Investigación Teórica y Práctica*

Para un fácil reconocimiento de los equipos activos de red de Postgrado se utilizará nombres de varios personajes de ANIMES, los cuales se pueden observar en la Tabla 81.

TABLA 82.- *Nombres sugeridos para los equipos activos de red en Postgrado*

POSTGRADO - ANIMES	
N°	**Nombre**
1	Goku
2	Bills
3	Boo
4	Broly
5	Bulma
6	Cell
7	Dabura
8	Freezer
9	Gohan
10	Gothen
11	Janemba
12	Krillin
13	Milk
14	Nappa
15	Piccolo
16	Tapion
17	Trunks
18	Vegueta
19	Wiss
20	Yamcha

Fuente: *Basado en Investigación Teórica y Práctica*

Para nombrar los equipos de red activos que pertenecen al edificio del Centro Académico de Idiomas se optará por los diferentes IDIOMAS que existen en el mundo, los cuales se muestran a continuación en la Tabla 82.

TABLA 83.- *Nombres sugeridos para los equipos activos de red en el CAI*

CAI - EXTRANJERO	
N°	**Nombre**
1	Alemán
2	Árabe
3	Búlgaro
4	Chino
5	Coreano
6	Finlandés
7	Francés
8	Griego
9	Húngaro
10	Inglés
11	Irlandés
12	Italiano
13	Japonés
14	Mongol
15	Persa
16	Polaco
17	Portugués
18	Ruso
19	Turco
20	Ucraniano

Fuente: *Basado en Investigación Teórica y Práctica*

Los equipos de red que pertenecen a la Biblioteca Universitaria llevarán los nombres de GRANDES LITERATOS, en alusión a dicha dependencia. Los nombres a utilizarse se muestran en la Tabla 83.

TABLA 84.- *Nombres sugeridos para los equipos activos de red de la Biblioteca*

BIBLIOTECA – GRANDES LITERATOS	
N°	Nombre
1	Alan-Poe
2	Almagro
3	Benedetti
4	Berne
5	Borges
6	Cervantes
7	Cohello
8	Dotoievski
9	García-Lorca
10	García-Márquez
11	Gillen
12	Homero
13	Mistral
14	Neruda
15	Octavio-Paz
16	Shakespeare
17	Shevchenko
18	Tagore
19	Torcuato
20	Vargas-Llosa

Fuente: *Basado en Investigación Teórica y Práctica*

Para nombrar los equipos activos de red que posee el colegio universitario se utilizarán los nombres de los GRANDES ECUATORIANOS que han destacado por sus diferentes desempeños, en la Tabla 84 se muestra varios de los nombres que se emplearán.

TABLA 85.- *Nombres sugeridos para los equipos activos de red en el Colegio Universitario*

COLEGIO UNIVERSITARIO - GRANDES ECUATORIANOS	
N°	Nombre
1	Abdón Calderón
2	Antonio J. de Sucre
3	Eloy Alfaro
4	Eugenio Espejo
5	García Moreno
6	Guayasamin
7	Iván Vallejo
8	Jaime Hurtado
9	Jefferson Pérez
10	Jorge Icaza
11	Juan Montalvo
12	Julio Jaramillo
13	Leónidas Proaño
14	Mejía Lequerica
15	Manuela Sáenz
16	Matilde Hidalgo
17	Roldós Aguilera
18	Rosalía Arteaga
19	Tránsito
20	Velasco Ibarra

Fuente: *Basado en Investigación Teórica y Práctica*

ANEXO 02

SIMULACIÓN DE LA RED UNIVERSITARIA

Para la demostración de un correcto funcionamiento de la nueva segmentación y nuevo direccionamiento IP de la Red Universitaria, se ha realizado una simulación de toda la red en Cisco Packet Tracer.

Cisco Packet Tracer, véase la Imagen 54, es una herramienta interactiva de simulación de redes para el aprendizaje de configuración de equipos, interconectados en diferentes topologías sin la necesidad de adquirir físicamente los equipos de red.

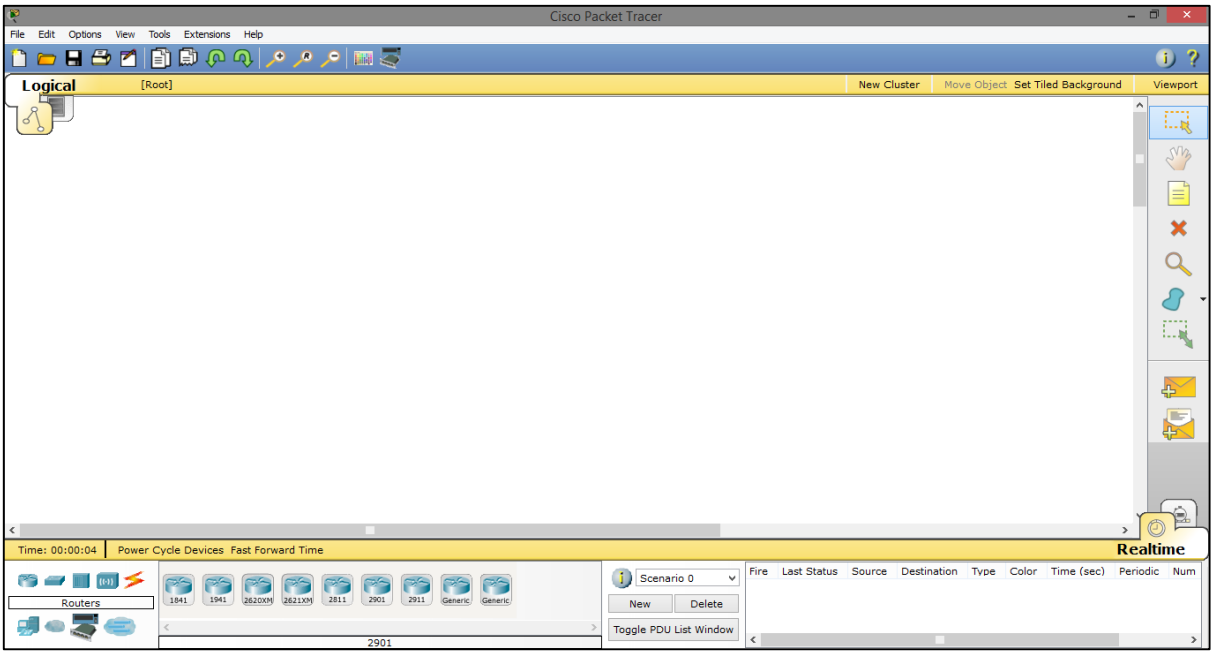


IMAGEN 54.- *Pantalla inicial de Cisco Packet Tracer*

Fuente: *Simulador de redes Cisco Packet Tracer V6.0.1.001*

Cisco Packet Tracer puede simular diferentes equipos de red como Switch, Routers, Hubs, Clouds, Modems, APs, dispositivos Wireless, Equipos finales y de usuario además de los diferentes tipos de cables de conexión Par Trenzado, Coaxial, Fibra Óptica, etc. Además Cisco Packet Tracer permite realizar las dos topologías de red tanto la lógica como la física.

Para la simulación de la red de la Universidad Técnica del Norte se ha empleado los Switch 3560 como Switch de Core ya que tiene funcionalidades de capa 3; y el Switch 2960 como Switchs de acceso en toda la red universitaria.

En la Imagen 55, se observa cómo debería ser la estructura lógica de la red de la Universidad Técnica del Norte la cual, en la cual se identifica el enlace principal desde el Switch de Core ubicado en el edificio central hacia el firewall y el enlace de backup desde el Switch de Core secundario que se encuentra en la FICA hacia el firewall y por medio del firewall se accede al internet y hacia la DMZ.

Para cada una de las facultades se ha configurado un clúster en el cual, dentro del clúster se realizara las diferentes topologías lógicas que tienen cada una, en caso de que las facultades tengan varios racks, cada uno se lo representará con un nuevo clúster dentro del clúster principal de la facultad.

En la Imagen 56, se muestra la topología física de la red universitaria, la cual mediante la utilización de edificios se ha realizado un bosquejo de la ubicación de cada una de las facultades y dependencias universitarias, los vínculos de color verde representan los enlaces de radio que tiene la universidad, los de color rojo son los enlaces principales hacia el Core principal y los de color azul representan los enlaces secundarios hacia el Core secundario.

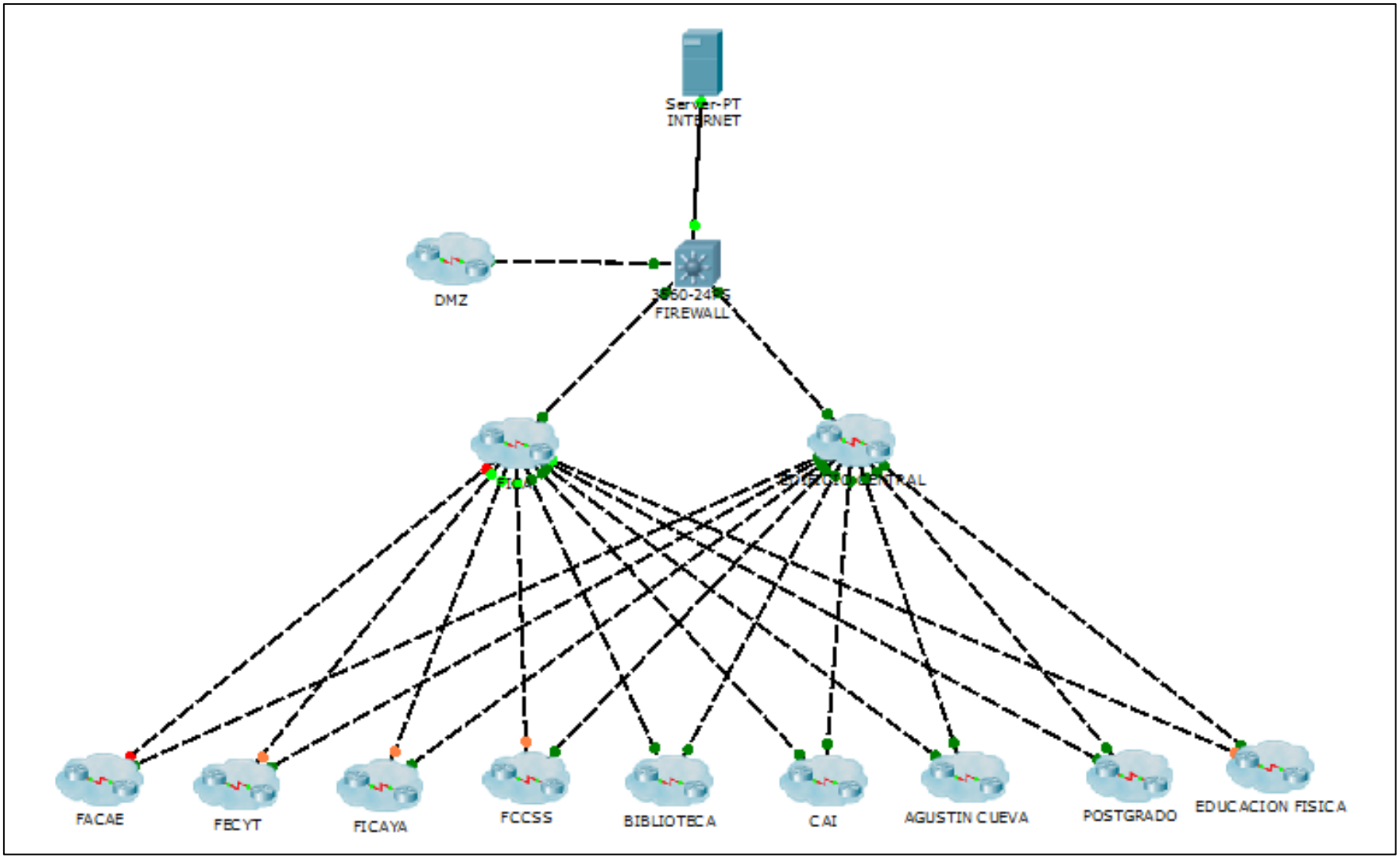


IMAGEN 55.- *Simulación de la Topología Lógica de la Red Universitaria*

Fuente: *Simulador de redes Cisco Packet Tracer V6.0.1.001*

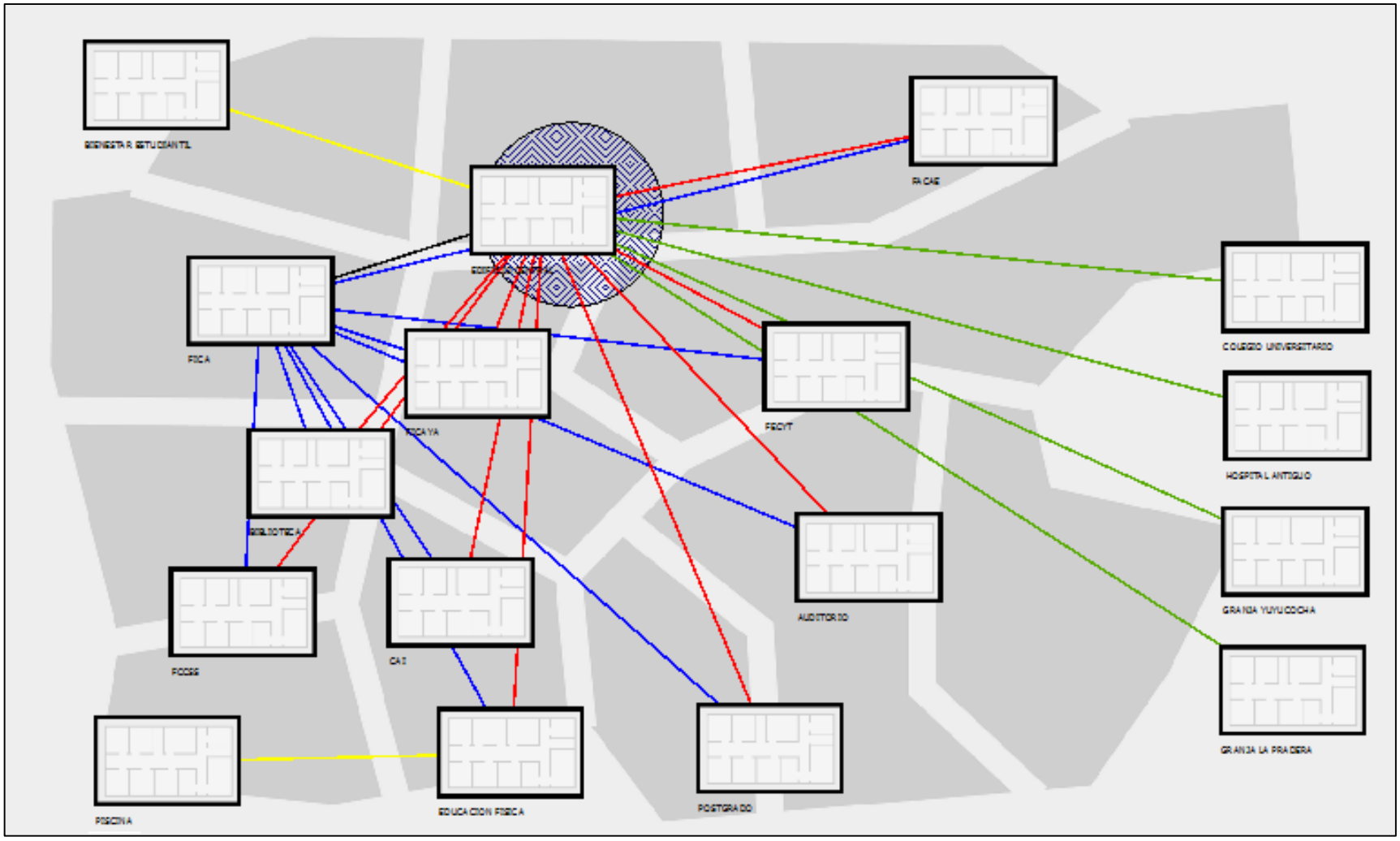


IMAGEN 56.- *Simulación de la Topología Física de la red Universitaria*

Fuente: *Simulador de redes Cisco Packet Tracer V6.0.1.001*

La Universidad cuenta con Wireless en todo su campus y para su simulación se empleó Access Point, utilizando un AP por cada una de las Wireless que posee la red universitaria. En la Imagen 57 se puede observar la simulación de la red Wireless Universitaria.

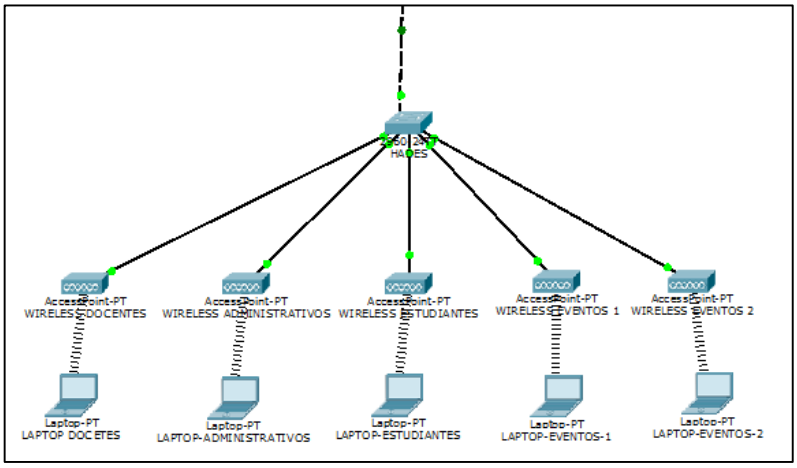


IMAGEN 57.- *Simulación de la red Wireless de la Universidad Técnica del Norte*
Fuente: *Simulador de redes Cisco Packet Tracer V6.0.1.001*

Al realizar la simulación se determina que la nueva distribución de IPs y la segmentación de red están correctamente distribuidos, y para la configuración de todos los equipos de red se ha utilizado los diferentes comandos explicados a continuación.

- **Respaldar la configuración del Switch**

Antes de realizar cualquier cambio en las configuraciones de los equipos, es indispensable respaldar toda la información que éste contenga, y se lo realiza con el siguiente comando:

Switch#copy running-config tftp

Address or name of remote host []? A.A.A.A

Destination filename [router01-confg]? router01-config-20120730.bak

!!830 bytes copied in 0.489 secs (1022 bytes/sec)

Donde A.A.A.A es la IP del equipo donde se respaldará las configuraciones del equipo.

- **Configurar el nombre en cada uno de los Switchs**

Se deben nombrar a todos los equipos activos de red existentes para ello se utilizarán los nombres sugeridos en el Anexo 01.

Switch>enable

Switch#configure terminal

Switch(config)#hostname NOMBRE

NOMBRE(config)#

- **Configurar Contraseñas**

En cada uno de los equipos activos de red se deben configurar las contraseñas para el enable, telnet y secret.

Switch(config)#enable password PASSWORD-ENABLE

Switch(config)#enable secret PASSWORD-SECRET

Switch(config)#line console 0

Switch(config-line)#password PASSWORD

Switch(config-line)#login

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password PASSWORD

Switch(config-line)#login

Switch(config-line)#exit

- **Configurar VTP server y VTP client**

En toda la red se debe configurar un Switch que cumpla la funcionalidad de ser el VTP server mientras que los demás equipos de red deben ser los VTP clients.

Switch#vlan database

Switch(vlan)#vtp server ó Switch(vlan)#vtp client

Switch(vlan)#vtp domain DOMINIO-VTP

Switch(vlan)#vlan password PASSWORD-VLAN

Switch(vlan)#exit

- **Creación de VLANs**

En el equipo que se ha configurado como VTP server, se deben crear las VLANs para que se propaguen hacia el resto de equipos clientes.

Switch#vlan database

Switch(vlan)#vlan NUMERO-DE-VLAN name NOMBRE-DE-LA-VLAN

Switch(vlan)#exit

- **Configuración de los Enlaces Troncales**

Los enlaces troncales son aquellos por los cuales se comunican los diferentes equipos activos de red, y se debe configurar en cada uno de los puertos del enlace en los Switchs.

Switch(config)#interface fastethernet #/#

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk native vlan #-VLAN-NATIVA

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#escription NOMBRE-DEL-ENLACE

Switch(config-if)#no shutdown

Switch(config-if)#exit

- **Agregar puertos a determinada VLAN**

Dependiendo a la dependencia que pertenezca un determinado puerto es necesario colocarlo en su correspondiente VLAN.

Switch(config)#interface fastethernet #/#

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan #

Switch(config-if)#switchport voice vlan #

Switch(config-if)#description DESCRIPCION-DEL-PUERTO

Switch(config-if)#no shutdown

Switch(config-if)#exit

En caso de tener una VLAN específicamente para el tráfico de voz se debe colocar el número de dicha VLAN en el comando

Switch(config-if)#switchport voice vlan #

En caso de que sea más de un puerto consecutivo el que se debe agregar a una determinada VLAN, se puede utilizar el siguiente comando.

Switch(config)#interface range fastethernet #/# - #

en lugar de

Switch(config)#interface fastethernet #/#

- **Configuración de IPs en cada una de las VLANs**

Se debe configurar la IP del interface VLAN perteneciente a cada una de las VLANs ya que por esta será el Gateway de cada una de las subredes, esto solo se lo debe realizar en el Switch de core principal y el Switch de Core secundario.

Switch(config)#interface vlan #

Switch(config-if)#ip address A.A.A.A B.B.B.B

Switch(config-if)#no shutdown

Switch(config-if)#exit

A.A.A.A representa la dirección IP y B.B.B.B representa la máscara de red.

- **Configuración de HSRP**

HSRP es un protocolo propietario de cisco en el cual permite la creación de enlaces backups, es por ello que se deben configurar en el Switch de Core principal como en el secundario.

Switch(config)#interface vlan #

Switch(config-if)#standby #-NUMERO-DEL-GRUPO ip A.A.A.A

Switch(config-if)#standby #-NUMERO-DEL-GRUPO priority 200

Switch(config-if)#standby #-NUMERO-DEL-GRUPO preempt

Switch(config-if)#exit

El #-NUMERO-DEL-GRUPO, es un nombre que se le da al conjunto de enlaces que pertenecerán al grupo HSRP, la IP debe pertenecer al mismo rango de IPs que se configure en cada una de las VLANs, si no se configura la prioridad el equipo reconoce el valor 100 por default pero el enlace principal será el que tenga la prioridad mayor. Un ejemplo de configuración de HSRP en una VLAN es el siguiente:

CorePrincipal(config)#interface vlan 52

CorePrincipal(config-if)#ip address 172.20.52.2 255.255.255.0

CorePrincipal(config-if)#standby 1 ip 172.20.52.1

CorePrincipal(config-if)#standby 1 priority 200

CorePrincipal(config-if)#standby 1 preempt

CorePrincipal(config-if)#exit

CoreSecundario(config)#interface vlan 52

CoreSecundario(config-if)#ip address 172.20.52.3 255.255.255.0

CoreSecundario(config-if)#standby 1 ip 172.20.52.1

CoreSecundario(config-if)#standby 1 priority 150

CoreSecundario(config-if)#standby 1 preempt

CoreSecundario(config-if)#exit

El funcionamiento de HSRP consiste en que a todos los equipos que se conecten a la VLAN 52 (en el ejemplo) se colocará como Gateway la IP 172.20.52.1, y el protocolo HSRP será el encargado de enrutar por el Switch con mayor prioridad y cuando el Switch principal tenga fallas, se apague o deje de funcionar por alguna razón, automáticamente el protocolo HSRP enrutará por el Switch con la siguiente prioridad.

- **Habilitar las funcionalidades de capa 3 en el Switch**

Debido a que los equipos utilizados son capa 3, se debe habilitar todas las funcionalidades de Router mediante el comando

Switch(config)#ip routing

- **Configuración de STP en los equipos**

Cuando en una red se tiene enlaces redundantes es indispensable la configuración del protocolo STP, ya que permite configurar cual es el enlace principal y cuál es el secundario.

SwitchPrincipal(config)#spanning-tree vlan 1 root primary

SwitchPrincipal(config)#exit

SwitchSecundario(config)#spanning-tree vlan 1 root secundary

SwitchSecundario(config)#exit

La prioridad por defecto de STP es 32769 y mientras más baja sea la prioridad será el enlace principal. Otra manera de configurar es mediante:

SwitchPrincipal(config)#spanning-tree vlan 1 prority <0-61440>

SwitchPrincipal(config)#exit

SwitchSecundario(config)#spanning-tree vlan 1 prority <0-6144>

SwitchSecundario(config)#exit

Tomando en cuenta que la prioridad del Switch Principal debe ser menor a la prioridad del Switch Secundario.

- **Configuración del default Gateway**

El Switch de Core principal está conectado directamente a la red LAN pero para salir hacia el exterior es decir la internet, es necesario configurar el default Gateway, que en este caso es la IP del Firewall.

Switch(config)#ip default Gateway A.A.A.A

Donde A.A.A.A es la IP del firewall o salida hacia el internet.

- **Configuración del servidor DHCP[27]**

Para activar la funcionalidad del servidor DHCP del Switch de Core se debe ingresar el siguiente comando.

Switch(config)#ip dhcp pool NOMBRE-DEL-POOL

Switch(dhcp-config)#network A.A.A.A B.B.B.B

Switch(dhcp-config)#default-router A.A.A.C

Switch(dhcp-config)#dns-server D.D.D.D

Switch(dhcp-config)#exit

Para poder excluir IPs y que estas no sean tomadas en cuenta en el servidor DHCP

Switch(config)#ip dhcp excluded-address A.A.A.A A.A.A.X

Donde A.A.A.A y A.A.A.X representan el rango de IPs que se van a excluir del servidor DHCP.

- **Configurar SSH**

Se deben configurar varios campos para quienes accedan mediante SSH hacia los Switchs, el cual es la versión de SSH, el timeput y el número de intentos de ingreso.

Switch(config)#ip ssh authentication-retries #

Switch(config)#ip ssh time-out #

[27] DHCP = Dynamic Host Configuration Protocol, Es el protocolo encargado de asignar direcciones IP a los equipos conectados a él.

Switch(config)#ip shh versión #

Switch(config)#line vyt 0 4

Switch(config-line)#transport input ssh telnet

Switch(config-line)#exit

- **Configurar ruteo en el Switch**

El Switch de Core también cumple con las funcionalidades de un Router es por ello que se deben emplear rutas estáticas.

Switch(config)#ip route A.A.A.A B.B.B.B C.C.C.C

Donde A.A.A.A es la dirección o pull de direcciones que se desea alcanzar, B.B.B.B es la máscara de la red a la cual deseamos alcanzar y C.C.C.C es la IP del siguiente salto.

- **Configurar el MOTD[28]**

El MOTD es el mensaje que aparece al momento de iniciar sesión en el equipo, este texto distingue entre mayúsculas y minúsculas.

Switch(config)#banner motd &MENSAJE-A-DESPLEGAR&

Swtich(config)#exit

- **Encriptación de contraseñas**

Luego de realizar las configuraciones es recomendable encriptar todas las contraseñas que hemos colocado y así cuando sean mostradas no aparezcan en texto plano.

Switch(config)#service password-encryption

- **Guardar las configuraciones**

Luego de haber realizado todas las configuraciones es necesario guardar el contenido del archivo de configuración en ejecución en la RAM no volátil.

Switch#copy running-config startup-config

Una aplicación rápida de este comando es escribir el código *do wr* en cualquier ubicación que se encuentre.

- **Borrar contenido del Switch**

Para borra las configuraciones del equipo se deben seguir los siguientes pasos, primero borrar el archivo que contiene las VLAN.

[28] MOTD = Message of the day, es el mensaje que se observa al momento de ingresar a un equipo de red.

Switch#delete flash:vlan.dat

Delete filename [vlan.dat]?[Enter]

Delete flash:vlan.dat? [confirm][Intro]

Luego se debe borrar la configuración actual del equipo

Switch#erase startup-config

Y por último reiniciar al equipo

Switch#reloaded

System configuration has been modified. Save? [yes/no]:no

Proceed with reload? [confirm][Intro]

Would you like to enter the initial configuration dialog? [yes/no]:no

Press RETURN to get started! [Intro]

- **Comandos para ver información del equipo**

Ver la información IOS del equipo Cisco

Switch>show versión

Ver el archivo de configuración activa actual del equipo Cisco

Switch#show running-config

Ver la configuración actual de la NVRAM

Switch#show startup-config

Ver la configuración de un determinado puerto

Switch#show interface fastethernet #/#

Ver la configuración de una determinada VLAN

Switch#show interface vlan #

Ver contenido de la tabla MAC

Switch#show mac-address-table

Eliminar las direcciones MAC de la tabla

Switch#clear mac-address-table dynamic

Ver los enlaces troncales

Switch#show interface trunk

Ver el listado de los comandos que se han ingresado

Switch#show history

ANEXO 03

PUERTOS DE LOS SWITCHS CON SU RESPECTIVA VLAN

El presente proyecto presenta una solución con una nueva distribución lógica de la red como también un nuevo direccionamiento IP, pero no se modificará en la topología física. Por ello es necesario respaldar la información de las diferentes interfaces de los equipos de red.

Equipos de red del Edificio Central

En el Edificio Central existen varios Racks que se encuentran distribuidos en todo el inmueble, los cuales se los indica a continuación.

- **Data Center**

En el Data Center se encuentran el Switch de Core Principal, los Chasis Blades donde se encuentran los Servidores y el Switch Concentrador, en la Tabla 85 se detalla las configuraciones sobre el modo de trabajo, las VLANs y la descripción de cada una de las interfaces del Switch de Core, en la Tabla 86 y la Tabla 87 las configuraciones de los dos Chasis Blade y en la Tabla 88 las configuraciones de las interfaces del Switch Concentrador.

TABLA 86.- *Descripción de las interfaces del Switch de Core del Data Center*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH CORE PRINCIPAL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	TenFastEthernet 1/1	Trunk	-	-	-
2	TenFastEthernet 1/2	Trunk	-	-	-
3	GigabitEthernet 1/3	Access	121	3	Hacia Router Telconet
4	GigabitEthernet 1/4	Trunk	-	-	Enlace Chasis Blade
5	GigabitEthernet 1/5	Trunk	-	-	Enlace Hacia WLC
6	GigabitEthernet 1/6	Trunk	-	-	Fibra a Terraza
7	GigabitEthernet 2/1	Trunk	-	-	Fibra a FICA
8	GigabitEthernet 2/2	Trunk	-	-	Fibra a Biblioteca
9	GigabitEthernet 2/3	Trunk	-	-	Fibra a FICAYA
10	GigabitEthernet 2/4	Trunk	-	-	Fibra a FACAE
11	GigabitEthernet 2/5	Trunk	-	-	Fibra a Derecho
12	GigabitEthernet 2/6	Trunk	-	-	Fibra a FCCSS

13	GigabitEthernet 3/1	Trunk	-	-	Fibra a FECYT
14	GigabitEthernet 3/2	Trunk	-	-	Fibra a Bienestar
15	GigabitEthernet 3/3	Trunk	-	-	Fibra a Auditorio A.C.
16	GigabitEthernet 3/4	Trunk	-	-	Fibra a Educación F.
17	GigabitEthernet 3/5	Trunk	-	-	Fibra a Segundo Piso
18	GigabitEthernet 3/6	Trunk	-	-	Fibra a Auditorio J.M.
19	FastEthernet 4/1	Access	4	16	Financiero
20	FastEthernet 4/2	Access	4	16	Financiero
21	FastEthernet 4/3	Access	4	16	Financiero
22	FastEthernet 4/4	Access	4	16	Financiero
23	FastEthernet 4/5	Access	4	16	Financiero
24	FastEthernet 4/6	Access	4	16	Financiero
25	FastEthernet 4/7	Access	4	16	Financiero
26	FastEthernet 4/8	Access	4	16	Financiero
27	FastEthernet 4/9	Access	4	16	Financiero
28	FastEthernet 4/10	Access	4	16	Financiero
29	FastEthernet 4/11	Access	4	16	Financiero
30	FastEthernet 4/12	Access	4	16	Financiero
31	FastEthernet 4/13	Access	4	16	Financiero
32	FastEthernet 4/14	Access	4	16	Financiero
33	FastEthernet 4/15	Access	4	16	Financiero
34	FastEthernet 4/16	Access	4	16	Financiero
35	FastEthernet 4/17	Access	4	16	Financiero
36	FastEthernet 4/18	Access	4	16	Financiero
37	FastEthernet 4/19	Access	4	16	Financiero
38	FastEthernet 4/20	Access	4	16	Financiero
39	FastEthernet 4/21	Access	4	16	Financiero
40	FastEthernet 4/22	Access	4	16	Financiero
41	FastEthernet 4/23	Access	4	16	Financiero
42	FastEthernet 4/24	Access	4	16	Financiero
43	FastEthernet 4/25	Access	4	16	Financiero
44	FastEthernet 4/26	Access	4	16	Financiero
45	FastEthernet 4/27	Access	4	16	Financiero
46	FastEthernet 4/28	Access	4	16	Financiero
47	FastEthernet 4/29	Access	4	16	Financiero

48	FastEthernet 4/30	Access	4	16	Financiero
49	FastEthernet 4/31	Access	4	16	Financiero
50	FastEthernet 4/32	Access	4	16	Financiero
51	FastEthernet 4/33	Access	4	16	Financiero
52	FastEthernet 4/34	Access	4	16	Financiero
53	FastEthernet 4/35	Access	4	16	Financiero
54	FastEthernet 4/36	Access	10	20	Ed. Central Admins
55	FastEthernet 4/37	Access	10	20	Ed. Central Admins
56	FastEthernet 4/38	Access	10	20	Ed. Central Admins
57	FastEthernet 4/39	Access	10	20	Ed. Central Admins
58	FastEthernet 4/40	Access	10	20	Ed. Central Admins
59	FastEthernet 4/41	Access	10	20	Ed. Central Admins
60	FastEthernet 4/42	Access	10	20	Ed. Central Admins
61	FastEthernet 4/43	Access	10	20	Ed. Central Admins
62	FastEthernet 4/44	Access	10	20	Ed. Central Admins
63	FastEthernet 4/45	Access	10	20	Ed. Central Admins
64	FastEthernet 4/46	Access	10	20	Ed. Central Admins
65	FastEthernet 4/47	Access	10	20	Ed. Central Admins
66	FastEthernet 4/48	Access	10	20	Ed. Central Admins
67	FastEthernet 5/1	Access	6	12	Informática
68	FastEthernet 5/2	Access	6	12	Informática
69	FastEthernet 5/3	Access	6	12	Informática
70	FastEthernet 5/4	Access	6	12	Informática
71	FastEthernet 5/5	Access	6	12	Informática
72	FastEthernet 5/6	Access	6	12	Informática
73	FastEthernet 5/7	Access	122	4	DMZ-SVRAPP2
74	FastEthernet 5/8	Access	1	1	Jubilaciones
75	FastEthernet 5/9	Access	122	4	DMZ-CONNECT
76	FastEthernet 5/10	Access	1	1	Antivirus
77	FastEthernet 5/11	Access	121	3	Servidor Quipux
78	FastEthernet 5/12	Access	6	12	Informática
79	FastEthernet 5/13	Access	122	4	DMZ
80	FastEthernet 5/14	Access	122	4	DMZ
81	FastEthernet 5/15	Access	122	4	Presidencia
82	FastEthernet 5/16	Access	202	1	Presidencia

83	FastEthernet 5/17	Access	122	4	Streaming TV
84	FastEthernet 5/18	Access	122	4	Streaming TV
85	FastEthernet 5/19	Access	122	4	DMZ-Share-Point
86	FastEthernet 5/20	Access	1	1	Servidor CUICYT
87	FastEthernet 5/21	Access	14	44	Servidor Aula Virtual
88	FastEthernet 5/22	Trunk	-	-	Enlace a la Garita
89	FastEthernet 5/23	Access	64	8	Telefonía
90	FastEthernet 5/24	Access	64	8	Telefonía
91	FastEthernet 5/25	Access	64	8	Telefonía
92	FastEthernet 5/26	Access	64	8	Telefonía
93	FastEthernet 5/27	Access	64	8	Telefonía
94	FastEthernet 5/28	Access	64	8	Telefonía
95	FastEthernet 5/29	Access	64	8	Telefonía
96	FastEthernet 5/30	Access	64	8	Telefonía
97	FastEthernet 5/31	Access	64	8	Telefonía
98	FastEthernet 5/32	Access	64	8	Telefonía
99	FastEthernet 5/33	Access	1	1	Cámara
100	FastEthernet 5/34	Access	1	1	Cámara
101	FastEthernet 5/35	Access	1	1	Aire
102	FastEthernet 5/36	Access	1	1	Aire
103	FastEthernet 5/37	Access	1	1	Aire
104	FastEthernet 5/38	Access	64	8	Telefonía
105	FastEthernet 5/39	Access	1	1	Libre
106	FastEthernet 5/40	Access	1	1	Libre
107	FastEthernet 5/41	Trunk	-	-	PortChannel Sw-C2
108	FastEthernet 5/42	Trunk	-	-	PortChannel Sw-C2
109	FastEthernet 5/43	Trunk	-	-	PortChannel Sw-C2
110	FastEthernet 5/44	Trunk	-	-	PortChannel Sw-C2
111	FastEthernet 5/45	Trunk	-	-	PortChannel Sw-C2
112	FastEthernet 5/46	Trunk	-	-	PortChannel Sw-C2
113	FastEthernet 5/47	Trunk	-	-	PortChannel Sw-C2
114	FastEthernet 5/48	Trunk	-	-	PortChannel Sw-C2
115	FastEthernet 6/1	Access	6	12	Informática
116	FastEthernet 6/2	Access	6	12	Informática
117	FastEthernet 6/3	Access	6	12	Informática

118	FastEthernet 6/4	Access	6	12	Informática
119	FastEthernet 6/5	Access	6	12	Informática
120	FastEthernet 6/6	Access	6	12	Informática
121	FastEthernet 6/7	Access	6	12	Informática
122	FastEthernet 6/8	Access	6	12	Informática
123	FastEthernet 6/9	Access	6	12	Informática
124	FastEthernet 6/10	Access	6	12	Informática
125	FastEthernet 6/11	Access	6	12	Informática
126	FastEthernet 6/12	Access	6	12	Informática
127	FastEthernet 6/13	Access	6	12	Informática
128	FastEthernet 6/14	Access	6	12	Informática
129	FastEthernet 6/15	Access	6	12	Informática
130	FastEthernet 6/16	Access	6	12	Informática
131	FastEthernet 6/17	Access	6	12	Informática
132	FastEthernet 6/18	Access	6	12	Informática
133	FastEthernet 6/19	Access	6	12	Informática
134	FastEthernet 6/20	Access	6	12	Informática
135	FastEthernet 6/21	Trunk	-	-	McOrtega - IP-Local
136	FastEthernet 6/22	Access	121	3	McOrtega - IP-Publica
137	FastEthernet 6/23	Access	6	12	Informática - AP
138	FastEthernet 6/24	Access	1	1	Control de Acceso
139	FastEthernet 6/25	Access	6	12	Informática
140	FastEthernet 6/26	Access	6	12	Informática
141	FastEthernet 6/27	Access	6	12	Informática
142	FastEthernet 6/28	Access	6	12	Informática
143	FastEthernet 6/29	Access	6	12	Informática
144	FastEthernet 6/30	Access	6	12	Informática
145	FastEthernet 6/31	Access	6	12	Informática
146	FastEthernet 6/32	Access	6	12	Informática
147	FastEthernet 6/33	Access	6	12	Informática
148	FastEthernet 6/34	Access	6	12	Informática
149	FastEthernet 6/35	Access	6	12	Informática
150	FastEthernet 6/36	Access	6	12	Informática
151	FastEthernet 6/37	Access	6	12	Informática
152	FastEthernet 6/38	Access	6	12	Informática

153	FastEthernet 6/39	Access	6	12	Informática
154	FastEthernet 6/40	Access	6	12	Informática
155	FastEthernet 6/41	Access	6	12	Informática
156	FastEthernet 6/42	Access	16	40	Monitoreo Diego P.
157	FastEthernet 6/43	Access	68	1	Wireless-FICA
158	FastEthernet 6/44	Access	1	1	Firewall-Wireless
159	FastEthernet 6/45	Access	6	12	Informática
160	FastEthernet 6/46	Access	68	1	Wireless-FICA
161	FastEthernet 6/47	Access	6	12	Informática
162	FastEthernet 6/48	Access	6	12	Informática

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 87.- *Descripción de las interfaces del Chasis Blade 01 del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL CHASIS BLADE 01					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	122	4	DMZ - BDD
2	GigabitEthernet 0/2	Access	122	4	DMZ
3	GigabitEthernet 0/3	Access	122	4	DMZ
4	GigabitEthernet 0/4	Access	1	1	Servidor DNS
5	GigabitEthernet 0/5	Access	122	4	DMZ
6	GigabitEthernet 0/6	Access	122	4	DMZ
7	GigabitEthernet 0/7	Access	122	4	DMZ
8	GigabitEthernet 0/8	Access	122	4	DMZ
9	GigabitEthernet 0/9	Access	122	4	DMZ
10	GigabitEthernet 0/10	Access	122	4	DMZ
11	GigabitEthernet 0/11	Access	122	4	DMZ - WEB
12	GigabitEthernet 0/12	Access	122	4	DMZ
13	GigabitEthernet 0/13	Access	122	4	DMZ

14	GigabitEthernet 0/14	Access	122	4	DMZ
15	GigabitEthernet 0/15	Access	122	4	DMZ
16	GigabitEthernet 0/16	Access	122	4	DMZ
17	GigabitEthernet 0/17	Trunk	-	-	
18	GigabitEthernet 0/18	Trunk	-	-	
19	GigabitEthernet 0/19	Access	1	1	Libre
20	GigabitEthernet 0/20	Access	1	1	Libre
21	GigabitEthernet 0/21	Access	1	1	Libre
22	GigabitEthernet 0/22	Access	1	1	Libre
23	GigabitEthernet 0/23	Access	1	1	Libre
24	GigabitEthernet 0/24	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 88.- *Descripción de las interfaces del Chasis Blade 02 del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL CHASIS BLADE 02					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	122	4	DMZ
2	GigabitEthernet 0/2	Access	122	4	DMZ
3	GigabitEthernet 0/3	Access	122	4	DMZ - ServerAPP
4	GigabitEthernet 0/4	Access	1	1	Servidor DNS
5	GigabitEthernet 0/5	Access	122	4	DMZ
6	GigabitEthernet 0/6	Access	122	4	DMZ - Geoportal
7	GigabitEthernet 0/7	Access	122	4	DMZ
8	GigabitEthernet 0/8	Access	122	4	DMZ
9	GigabitEthernet 0/9	Access	122	4	DMZ
10	GigabitEthernet 0/10	Access	122	4	DMZ
11	GigabitEthernet 0/11	Access	122	4	DMZ
12	GigabitEthernet 0/12	Access	122	4	DMZ - AulaVirtual
13	GigabitEthernet 0/13	Access	122	4	DMZ
14	GigabitEthernet 0/14	Access	122	4	DMZ
15	GigabitEthernet 0/15	Access	122	4	DMZ

16	GigabitEthernet 0/16	Access	122	4	DMZ
17	GigabitEthernet 0/17	Access	1	1	Libre
18	GigabitEthernet 0/18	Trunk	-	-	
19	GigabitEthernet 0/19	Access	1	1	Libre
20	GigabitEthernet 0/20	Access	1	1	Libre
21	GigabitEthernet 0/21	Access	1	1	Libre
22	GigabitEthernet 0/22	Access	1	1	Libre
23	GigabitEthernet 0/23	Access	1	1	Libre
24	GigabitEthernet 0/24	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 89.- *Descripción de las interfaces del Switch Concentrador del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH CONCENTRADOR					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1/0/1	Access	122	4	DMZ-Servidores
2	GigabitEthernet 1/0/2	Access	121	3	ASA-Outside
3	GigabitEthernet 1/0/3	Access	1	1	Inside-PacketSH
4	GigabitEthernet 1/0/4	Access	1	1	ILO-Blade
5	GigabitEthernet 1/0/5	Access	168	202	Banco Pichincha
6	GigabitEthernet 1/0/6	Access	64	8	GW de Voz
7	GigabitEthernet 1/0/7	Access	64	8	Call Manager
8	GigabitEthernet 1/0/8	Access	64	8	IVR VoIP
9	GigabitEthernet 1/0/9	Access	64	8	Servidor – Karlita
10	GigabitEthernet 1/0/10	Access	6	12	Informática
11	GigabitEthernet 1/0/11	Access	1	1	Libre
12	GigabitEthernet 1/0/12	Access	121	3	IP-McOrtega-Publica
13	GigabitEthernet 1/0/13	Access	1	1	Firewall Proxy UTN
14	GigabitEthernet 1/0/14	Access	1	1	Portal Cautivo UTN
15	GigabitEthernet 1/0/15	Access	1	1	Libre
16	GigabitEthernet 1/0/16	Access	1	1	Libre
17	GigabitEthernet 1/0/17	Trunk	-	-	Portchanel Core
18	GigabitEthernet 1/0/18	Trunk	-	-	Portchanel Core
19	GigabitEthernet 1/0/19	Trunk	-	-	Portchanel Core

20	GigabitEthernet 1/0/20	Trunk	-	-	Portchanel Core
21	GigabitEthernet 1/0/21	Trunk	-	-	Portchanel Core
22	GigabitEthernet 1/0/22	Trunk	-	-	Portchanel Core
23	GigabitEthernet 1/0/23	Trunk	-	-	Portchanel Core
24	GigabitEthernet 1/0/24	Trunk	-	-	Portchanel Core

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Planta Baja**

En la planta baja del Edificio Central existe un solo Switch y en la Tabla 89 se muestra la descripción de las interfaces del mismo.

TABLA 90.- *Descripción de las interfaces del Switch de la Planta Baja del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL RACK DERECHO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	4	16	Financiero
2	FastEthernet 0/2	Access	4	16	Financiero
3	FastEthernet 0/3	Access	4	16	Financiero
4	FastEthernet 0/4	Access	4	16	Financiero
5	FastEthernet 0/5	Access	4	16	Financiero
6	FastEthernet 0/6	Access	4	16	Financiero
7	FastEthernet 0/7	Access	4	16	Financiero
8	FastEthernet 0/8	Access	4	16	Financiero
9	FastEthernet 0/9	Access	4	16	Financiero
10	FastEthernet 0/10	Access	4	16	Financiero
11	FastEthernet 0/11	Access	4	16	Financiero
12	FastEthernet 0/12	Access	4	16	Financiero
13	FastEthernet 0/13	Access	4	16	Financiero
14	FastEthernet 0/14	Access	4	16	Financiero
15	FastEthernet 0/15	Access	10	20	Ed. Central Admins
16	FastEthernet 0/16	Access	10	20	Ed. Central Admins
17	FastEthernet 0/17	Access	4	16	Financiero
18	FastEthernet 0/18	Access	4	16	Financiero
19	FastEthernet 0/19	Access	4	16	Financiero
20	FastEthernet 0/20	Access	4	16	Financiero

21	FastEthernet 0/21	Access	4	16	Financiero
22	FastEthernet 0/22	Access	4	16	Financiero
23	FastEthernet 0/23	Access	4	16	Financiero
24	FastEthernet 0/24	Access	4	16	Financiero
25	FastEthernet 0/25	Access	4	16	Financiero
26	FastEthernet 0/26	Access	4	16	Financiero
27	FastEthernet 0/27	Access	10	20	Ed. Central Admins
28	FastEthernet 0/28	Access	10	20	Ed. Central Admins
29	FastEthernet 0/29	Access	10	20	Ed. Central Admins
30	FastEthernet 0/30	Access	10	20	Ed. Central Admins
31	FastEthernet 0/31	Access	10	20	Ed. Central Admins
32	FastEthernet 0/32	Access	10	20	Ed. Central Admins
33	FastEthernet 0/33	Access	10	20	Ed. Central Admins
34	FastEthernet 0/34	Access	10	20	Ed. Central Admins
35	FastEthernet 0/35	Access	10	20	Ed. Central Admins
36	FastEthernet 0/36	Access	10	20	Ed. Central Admins
37	FastEthernet 0/37	Access	10	20	Ed. Central Admins
38	FastEthernet 0/38	Access	10	20	Ed. Central Admins
39	FastEthernet 0/39	Access	10	20	Ed. Central Admins
40	FastEthernet 0/40	Access	10	20	Ed. Central Admins
41	FastEthernet 0/41	Access	10	20	Ed. Central Admins
42	FastEthernet 0/42	Access	10	20	Ed. Central Admins
43	FastEthernet 0/43	Access	10	20	Ed. Central Admins
44	FastEthernet 0/44	Access	10	20	Ed. Central Admins
45	FastEthernet 0/45	Access	10	20	Ed. Central Admins
46	FastEthernet 0/46	Access	10	20	Ed. Central Admins
47	FastEthernet 0/47	Access	2	6	AP - UTN
48	FastEthernet 0/48	Access	66	201	Copiadora
49	GigabitEthernet 0/1	Trunk	-	-	Core Principal
50	GigabitEthernet 0/2	Access	1	1	Libre

- **Segundo Piso**

En el segundo piso del Edificio Central existe un Rack de equipos de red con dos Switchs de Acceso, en la Tabla 90 y en la Tabla 91 se muestran la descripción de las interfaces de los Switchs.

TABLA 91.- *Descripción de las interfaces del Switch 01 del segundo piso del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL SEGUNDO PISO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	8	14	Autoridades
2	FastEthernet 0/2	Access	8	14	Autoridades
3	FastEthernet 0/3	Access	8	14	Autoridades
4	FastEthernet 0/4	Access	8	14	Autoridades
5	FastEthernet 0/5	Access	10	20	Ed. Central Admins
6	FastEthernet 0/6	Access	10	20	Ed. Central Admins
7	FastEthernet 0/7	Access	8	14	Autoridades
8	FastEthernet 0/8	Access	8	14	Autoridades
9	FastEthernet 0/9	Access	10	20	Ed. Central Admins
10	FastEthernet 0/10	Access	10	20	Ed. Central Admins
11	FastEthernet 0/11	Access	10	20	Ed. Central Admins
12	FastEthernet 0/12	Access	10	20	Ed. Central Admins
13	FastEthernet 0/13	Access	10	20	Ed. Central Admins
14	FastEthernet 0/14	Access	10	20	Ed. Central Admins
15	FastEthernet 0/15	Access	8	14	Autoridades
16	FastEthernet 0/16	Access	8	14	Autoridades
17	FastEthernet 0/17	Access	8	14	Autoridades
18	FastEthernet 0/18	Access	8	14	Autoridades
19	FastEthernet 0/19	Access	8	14	Autoridades
20	FastEthernet 0/20	Access	8	14	Autoridades
21	FastEthernet 0/21	Access	8	14	Autoridades
22	FastEthernet 0/22	Access	8	14	Autoridades
23	FastEthernet 0/23	Access	8	14	Autoridades
24	FastEthernet 0/24	Access	8	14	Autoridades
25	FastEthernet 0/25	Access	8	14	Autoridades
26	FastEthernet 0/26	Access	8	14	Autoridades
27	FastEthernet 0/27	Access	8	14	Autoridades
28	FastEthernet 0/28	Access	8	14	Autoridades
29	FastEthernet 0/29	Access	8	14	Autoridades
30	FastEthernet 0/30	Access	8	14	Autoridades

31	FastEthernet 0/31	Access	10	20	Ed. Central Admins
32	FastEthernet 0/32	Access	10	20	Ed. Central Admins
33	FastEthernet 0/33	Access	10	20	Ed. Central Admins
34	FastEthernet 0/34	Access	10	20	Ed. Central Admins
35	FastEthernet 0/35	Access	10	20	Ed. Central Admins
36	FastEthernet 0/36	Access	10	20	Ed. Central Admins
37	FastEthernet 0/37	Access	10	20	Ed. Central Admins
38	FastEthernet 0/38	Access	10	20	Ed. Central Admins
39	FastEthernet 0/39	Access	10	20	Ed. Central Admins
40	FastEthernet 0/40	Access	10	20	Ed. Central Admins
41	FastEthernet 0/41	Access	10	20	Ed. Central Admins
42	FastEthernet 0/42	Access	8	14	Autoridades
43	FastEthernet 0/43	Access	8	14	Autoridades
44	FastEthernet 0/44	Access	8	14	Autoridades
45	FastEthernet 0/45	Access	8	14	Autoridades
46	FastEthernet 0/46	Access	8	14	Autoridades
47	FastEthernet 0/47	Access	8	14	Autoridades
48	FastEthernet 0/48	Access	8	14	Autoridades
49	GigabitEthernet 0/1	Trunk	-	-	Core Principal
50	GigabitEthernet 0/2	Trunk	-	-	Rack-Piso02

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 92.- *Descripción de las interfaces del Switch 02 del segundo piso del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL SEGUNDO PISO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	8	14	Autoridades
2	FastEthernet 0/2	Access	8	14	Autoridades
3	FastEthernet 0/3	Access	8	14	Autoridades
4	FastEthernet 0/4	Access	121	3	Públicas
5	FastEthernet 0/5	Access	8	14	Autoridades
6	FastEthernet 0/6	Access	8	14	Autoridades
7	FastEthernet 0/7	Access	8	14	Autoridades

8	FastEthernet 0/8	Access	8	14	Autoridades
9	FastEthernet 0/9	Access	8	14	Autoridades
10	FastEthernet 0/10	Access	8	14	Autoridades
11	FastEthernet 0/11	Access	2	6	AP - UTN
12	FastEthernet 0/12	Access	8	14	Autoridades
13	FastEthernet 0/13	Access	8	14	Autoridades
14	FastEthernet 0/14	Access	8	14	Autoridades
15	FastEthernet 0/15	Access	8	14	Autoridades
16	FastEthernet 0/16	Access	8	14	Autoridades
17	FastEthernet 0/17	Access	8	14	Autoridades
18	FastEthernet 0/18	Access	8	14	Autoridades
19	FastEthernet 0/19	Access	8	14	Autoridades
20	FastEthernet 0/20	Access	8	14	Autoridades
21	FastEthernet 0/21	Access	8	14	Autoridades
22	FastEthernet 0/22	Access	8	14	Autoridades
23	FastEthernet 0/23	Access	8	14	Autoridades
24	FastEthernet 0/24	Access	8	14	Autoridades
25	GigabitEthernet 0/1	Trunk	-	-	Rack Piso2
26	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Auditorio José Martí**

En el Auditorio José Martí del Edificio Central existe un Rack de equipos de red con dos Switchs de Acceso, en la Tabla 92 y en la Tabla 93 se muestran la descripción de las interfaces de los Switchs.

TABLA 93.- *Descripción de las interfaces del Switch 01 del Auditorio José Martí del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL AUDITORIO JOSÉ MARTÍ					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	10	20	Ed. Central Admins

2	FastEthernet 0/2	Access	10	20	Ed. Central Admins
3	FastEthernet 0/3	Access	10	20	Ed. Central Admins
4	FastEthernet 0/4	Access	10	20	Ed. Central Admins
5	FastEthernet 0/5	Access	10	20	Ed. Central Admins
6	FastEthernet 0/6	Access	10	20	Ed. Central Admins
7	FastEthernet 0/7	Access	10	20	Ed. Central Admins
8	FastEthernet 0/8	Access	10	20	Ed. Central Admins
9	FastEthernet 0/9	Access	10	20	Ed. Central Admins
10	FastEthernet 0/10	Access	10	20	Ed. Central Admins
11	FastEthernet 0/11	Access	10	20	Ed. Central Admins
12	FastEthernet 0/12	Access	10	20	Ed. Central Admins
13	FastEthernet 0/13	Access	10	20	Ed. Central Admins
14	FastEthernet 0/14	Access	10	20	Ed. Central Admins
15	FastEthernet 0/15	Access	10	20	Ed. Central Admins
16	FastEthernet 0/16	Access	10	20	Ed. Central Admins
17	FastEthernet 0/17	Access	10	20	Ed. Central Admins
18	FastEthernet 0/18	Access	10	20	Ed. Central Admins
19	FastEthernet 0/19	Access	10	20	Ed. Central Admins
20	FastEthernet 0/20	Access	10	20	Ed. Central Admins
21	FastEthernet 0/21	Access	10	20	Ed. Central Admins
22	FastEthernet 0/22	Access	10	20	Ed. Central Admins
23	FastEthernet 0/23	Access	10	20	Ed. Central Admins
24	FastEthernet 0/24	Access	10	20	Ed. Central Admins
25	FastEthernet 0/25	Access	10	20	Ed. Central Admins
26	FastEthernet 0/26	Access	10	20	Ed. Central Admins
27	FastEthernet 0/27	Access	10	20	Ed. Central Admins
28	FastEthernet 0/28	Access	10	20	Ed. Central Admins
29	FastEthernet 0/29	Access	10	20	Ed. Central Admins
30	FastEthernet 0/30	Access	10	20	Ed. Central Admins
31	FastEthernet 0/31	Access	10	20	Ed. Central Admins
32	FastEthernet 0/32	Access	10	20	Ed. Central Admins
33	FastEthernet 0/33	Access	10	20	Ed. Central Admins
34	FastEthernet 0/34	Access	10	20	Ed. Central Admins

35	FastEthernet 0/35	Access	10	20	Ed. Central Admins
36	FastEthernet 0/36	Access	10	20	Ed. Central Admins
37	FastEthernet 0/37	Access	10	20	Ed. Central Admins
38	FastEthernet 0/38	Access	10	20	Ed. Central Admins
39	FastEthernet 0/39	Access	10	20	Ed. Central Admins
40	FastEthernet 0/40	Access	10	20	Ed. Central Admins
41	FastEthernet 0/41	Access	10	20	Ed. Central Admins
42	FastEthernet 0/42	Access	10	20	Ed. Central Admins
43	FastEthernet 0/43	Access	10	20	Ed. Central Admins
44	FastEthernet 0/44	Access	10	20	Ed. Central Admins
45	FastEthernet 0/45	Access	10	20	Ed. Central Admins
46	FastEthernet 0/46	Access	10	20	Ed. Central Admins
47	FastEthernet 0/47	Access	10	20	Ed. Central Admins
48	FastEthernet 0/48	Access	10	20	Ed. Central Admins
49	GigabitEthernet 0/1	Trunk	-	-	Core Central
50	GigabitEthernet 0/2	Trunk	-	-	José Martí 02

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 94.- *Descripción de las interfaces del Switch 02 del Auditorio José Martí del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL AUDITORIO JOSÉ MARTÍ					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	10	20	Ed. Central Admins
2	FastEthernet 0/2	Access	10	20	Ed. Central Admins
3	FastEthernet 0/3	Access	10	20	Ed. Central Admins
4	FastEthernet 0/4	Access	10	20	Ed. Central Admins
5	FastEthernet 0/5	Access	10	20	Ed. Central Admins
6	FastEthernet 0/6	Access	10	20	Ed. Central Admins

7	FastEthernet 0/7	Access	10	20	Ed. Central Admins
8	FastEthernet 0/8	Access	10	20	Ed. Central Admins
9	FastEthernet 0/9	Access	10	20	Ed. Central Admins
10	FastEthernet 0/10	Access	10	20	Ed. Central Admins
11	FastEthernet 0/11	Access	10	20	Ed. Central Admins
12	FastEthernet 0/12	Access	10	20	Ed. Central Admins
13	FastEthernet 0/13	Access	10	20	Ed. Central Admins
14	FastEthernet 0/14	Access	10	20	Ed. Central Admins
15	FastEthernet 0/15	Access	10	20	Ed. Central Admins
16	FastEthernet 0/16	Access	10	20	Ed. Central Admins
17	FastEthernet 0/17	Access	10	20	Ed. Central Admins
18	FastEthernet 0/18	Access	10	20	Ed. Central Admins
19	FastEthernet 0/19	Access	10	20	Ed. Central Admins
20	FastEthernet 0/20	Access	10	20	Ed. Central Admins
21	FastEthernet 0/21	Access	10	20	Ed. Central Admins
22	FastEthernet 0/22	Access	10	20	Ed. Central Admins
23	FastEthernet 0/23	Access	10	20	Ed. Central Admins
24	FastEthernet 0/24	Access	10	20	Ed. Central Admins
25	FastEthernet 0/25	Access	10	20	Ed. Central Admins
26	FastEthernet 0/26	Access	10	20	Ed. Central Admins
27	FastEthernet 0/27	Access	10	20	Ed. Central Admins
28	FastEthernet 0/28	Access	10	20	Ed. Central Admins
29	FastEthernet 0/29	Access	10	20	Ed. Central Admins
30	FastEthernet 0/30	Access	10	20	Ed. Central Admins
31	FastEthernet 0/31	Access	10	20	Ed. Central Admins
32	FastEthernet 0/32	Access	10	20	Ed. Central Admins
33	FastEthernet 0/33	Access	10	20	Ed. Central Admins
34	FastEthernet 0/34	Access	10	20	Ed. Central Admins
35	FastEthernet 0/35	Access	10	20	Ed. Central Admins
36	FastEthernet 0/36	Access	10	20	Ed. Central Admins
37	FastEthernet 0/37	Access	10	20	Ed. Central Admins
38	FastEthernet 0/38	Access	10	20	Ed. Central Admins
39	FastEthernet 0/39	Access	10	20	Ed. Central Admins
40	FastEthernet 0/40	Access	10	20	Ed. Central Admins
41	FastEthernet 0/41	Access	10	20	Ed. Central Admins

42	FastEthernet 0/42	Access	10	20	Ed. Central Admins
43	FastEthernet 0/43	Access	10	20	Ed. Central Admins
44	FastEthernet 0/44	Access	10	20	Ed. Central Admins
45	FastEthernet 0/45	Access	10	20	Ed. Central Admins
46	FastEthernet 0/46	Access	10	20	Ed. Central Admins
47	FastEthernet 0/47	Access	2	6	AP - UTN
48	FastEthernet 0/48	Access	10	20	Ed. Central Admins
49	GigabitEthernet 0/1	Trunk	-	-	José Martí 01
50	GigabitEthernet 0/2	Access	1	-	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Canal Universitario**

En el Canal Universitario del Edificio Central existe un solo Switch y en la Tabla 94 se muestra la descripción de las interfaces del mismo.

TABLA 95.- *Descripción de las interfaces del Switch del Canal Universitario en el Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL CANAL UNIVERSITARIO UTV					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	12	18	Comun. Organizacional
2	FastEthernet 0/2	Access	12	18	Comun. Organizacional
3	FastEthernet 0/3	Access	12	18	Comun. Organizacional
4	FastEthernet 0/4	Access	12	18	Comun. Organizacional
5	FastEthernet 0/5	Access	12	18	Comun. Organizacional
6	FastEthernet 0/6	Access	12	18	Comun. Organizacional
7	FastEthernet 0/7	Access	12	18	Comun. Organizacional
8	FastEthernet 0/8	Access	12	18	Comun. Organizacional
9	FastEthernet 0/9	Access	12	18	Comun. Organizacional
10	FastEthernet 0/10	Access	12	18	Comun. Organizacional
11	FastEthernet 0/11	Access	12	18	Comun. Organizacional
12	FastEthernet 0/12	Access	12	18	Comun. Organizacional
13	FastEthernet 0/13	Access	12	18	Comun. Organizacional
14	FastEthernet 0/14	Access	12	18	Comun. Organizacional
15	FastEthernet 0/15	Access	12	18	Comun. Organizacional
16	FastEthernet 0/16	Access	12	18	Comun. Organizacional

17	FastEthernet 0/17	Access	12	18	Comun. Organizacional
18	FastEthernet 0/18	Access	12	18	Comun. Organizacional
19	FastEthernet 0/19	Access	12	18	Comun. Organizacional
20	FastEthernet 0/20	Access	12	18	Comun. Organizacional
21	FastEthernet 0/21	Access	12	18	Comun. Organizacional
22	FastEthernet 0/22	Access	12	18	Comun. Organizacional
23	FastEthernet 0/23	Access	12	18	Comun. Organizacional
24	FastEthernet 0/24	Access	12	18	Comun. Organizacional
25	FastEthernet 0/25	Access	12	18	Comun. Organizacional
26	FastEthernet 0/26	Access	12	18	Comun. Organizacional
27	FastEthernet 0/27	Access	12	18	Comun. Organizacional
28	FastEthernet 0/28	Access	12	18	Comun. Organizacional
29	FastEthernet 0/29	Access	12	18	Comun. Organizacional
30	FastEthernet 0/30	Access	122	4	DMZ
31	FastEthernet 0/31	Access	12	18	Comun. Organizacional
32	FastEthernet 0/32	Access	12	18	Comun. Organizacional
33	FastEthernet 0/33	Access	12	18	Comun. Organizacional
34	FastEthernet 0/34	Access	12	18	Comun. Organizacional
35	FastEthernet 0/35	Access	12	18	Comun. Organizacional
36	FastEthernet 0/36	Access	12	18	Comun. Organizacional
37	FastEthernet 0/37	Access	12	18	Comun. Organizacional
38	FastEthernet 0/38	Access	12	18	Comun. Organizacional
39	FastEthernet 0/39	Access	12	18	Comun. Organizacional
40	FastEthernet 0/40	Access	12	18	Comun. Organizacional
41	FastEthernet 0/41	Access	12	18	Comun. Organizacional
42	FastEthernet 0/42	Access	12	18	Comun. Organizacional
43	FastEthernet 0/43	Access	12	18	Comun. Organizacional
44	FastEthernet 0/44	Access	12	18	Comun. Organizacional
45	FastEthernet 0/45	Access	12	18	Comun. Organizacional
46	FastEthernet 0/46	Access	12	18	Comun. Organizacional
47	FastEthernet 0/47	Access	122	4	Streaming UTV
48	FastEthernet 0/48	Access	122	4	Streaming UTV
49	GigabitEthernet 0/1	Trunk	-	-	Terraza
50	GigabitEthernet 0/2	Access	1	1	Libre

***Fuente**: Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Terraza**

En la terraza del Edificio Central existe un Rack con dos Switchs de Acceso, en la Tabla 95 y en la Tabla 96 se muestra la descripción de las interfaces de los Switchs.

TABLA 96.- *Descripción de las interfaces del Switch 01 de la Terraza del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DE LA TERRAZA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	12	18	Comun. Organizacional
2	FastEthernet 0/2	Access	12	18	Comun. Organizacional
3	FastEthernet 0/3	Access	12	18	Comun. Organizacional
4	FastEthernet 0/4	Access	12	18	Comun. Organizacional
5	FastEthernet 0/5	Access	12	18	Comun. Organizacional
6	FastEthernet 0/6	Access	12	18	Comun. Organizacional
7	FastEthernet 0/7	Access	12	18	Comun. Organizacional
8	FastEthernet 0/8	Access	12	18	Comun. Organizacional
9	FastEthernet 0/9	Access	12	18	Comun. Organizacional
10	FastEthernet 0/10	Access	12	18	Comun. Organizacional
11	FastEthernet 0/11	Access	12	18	Comun. Organizacional
12	FastEthernet 0/12	Access	12	18	Comun. Organizacional
13	FastEthernet 0/13	Access	10	20	Ed. Central Admins
14	FastEthernet 0/14	Access	10	20	Ed. Central Admins
15	FastEthernet 0/15	Access	10	20	Ed. Central Admins
16	FastEthernet 0/16	Access	10	20	Ed. Central Admins
17	FastEthernet 0/17	Access	10	20	Ed. Central Admins
18	FastEthernet 0/18	Access	10	20	Ed. Central Admins
19	FastEthernet 0/19	Access	10	20	Ed. Central Admins
20	FastEthernet 0/20	Access	10	20	Ed. Central Admins
21	FastEthernet 0/21	Access	10	20	Ed. Central Admins
22	FastEthernet 0/22	Access	10	20	Ed. Central Admins
23	FastEthernet 0/23	Access	10	20	Ed. Central Admins
24	FastEthernet 0/24	Access	10	20	Ed. Central Admins
25	FastEthernet 0/25	Access	10	20	Ed. Central Admins
26	FastEthernet 0/26	Access	10	20	Ed. Central Admins

27	FastEthernet 0/27	Access	10	20	Ed. Central Admins
28	FastEthernet 0/28	Access	10	20	Ed. Central Admins
29	FastEthernet 0/29	Access	10	20	Ed. Central Admins
30	FastEthernet 0/30	Access	10	20	Ed. Central Admins
31	FastEthernet 0/31	Access	10	20	Ed. Central Admins
32	FastEthernet 0/32	Access	10	20	Ed. Central Admins
33	FastEthernet 0/33	Access	10	20	Ed. Central Admins
34	FastEthernet 0/34	Access	10	20	Ed. Central Admins
35	FastEthernet 0/35	Access	10	20	Ed. Central Admins
36	FastEthernet 0/36	Access	10	20	Ed. Central Admins
37	FastEthernet 0/37	Access	10	20	Ed. Central Admins
38	FastEthernet 0/38	Access	10	20	Ed. Central Admins
39	FastEthernet 0/39	Access	10	20	Ed. Central Admins
40	FastEthernet 0/40	Access	10	20	Ed. Central Admins
41	FastEthernet 0/41	Access	10	20	Ed. Central Admins
42	FastEthernet 0/42	Access	10	20	Ed. Central Admins
43	FastEthernet 0/43	Access	10	20	Ed. Central Admins
44	FastEthernet 0/44	Access	10	20	Ed. Central Admins
45	FastEthernet 0/45	Access	12	18	Comun. Organizacional
46	FastEthernet 0/46	Access	12	18	Comun. Organizacional
47	FastEthernet 0/47	Access	122	4	Streaming UTV
48	FastEthernet 0/48	Trunk	-	-	SW Radio Enlaces
49	GigabitEthernet 0/1	Trunk	-	-	Core Central
50	GigabitEthernet 0/2	Trunk	-	-	Rack-UTV

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 97.- *Descripción de las interfaces del Switch 02 de la Terraza del Edificio Central*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DE LA TERRAZA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Access	12	18	Comun. Organizacional
2	FastEthernet 1/2	Access	12	18	Comun. Organizacional
3	FastEthernet 1/3	Access	12	18	Comun. Organizacional
4	FastEthernet 1/4	Access	12	18	Comun. Organizacional

5	FastEthernet 1/5	Access	14	44	FICA-Administrativos
6	FastEthernet 1/6	Access	14	44	FICA-Administrativos
7	FastEthernet 1/7	Access	10	20	Ed. Central Admins
8	FastEthernet 1/8	Access	10	20	Ed. Central Admins
9	FastEthernet 1/9	Access	2	6	AP-UTN
10	FastEthernet 1/10	Access	2	6	AP-UTN
11	FastEthernet 1/11	Access	60	1	No Existe
12	FastEthernet 1/12	Access	60	1	No Existe
13	FastEthernet 1/13	Trunk	-	-	Enlace de Radio
14	FastEthernet 1/14	Trunk	-	-	Enlace de Radio
15	FastEthernet 1/15	Trunk	-	-	Enlace de Radio
16	FastEthernet 1/16	Trunk	-	-	Enlace de Radio
17	FastEthernet 1/17	Trunk	-	-	Enlace de Radio
18	FastEthernet 1/18	Trunk	-	-	Enlace de Radio
19	FastEthernet 1/19	Trunk	-	-	Enlace de Radio
20	FastEthernet 1/20	Trunk	-	-	Enlace de Radio
21	FastEthernet 1/21	Trunk	-	-	Enlace de Radio
22	FastEthernet 1/22	Trunk	-	-	Enlace de Radio
23	FastEthernet 1/23	Access	10	20	Ed. Central Admins
24	FastEthernet 1/24	Trunk	-	-	Enlace de Radio

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Garita**

En la Garita que se encuentra un Switch de Acceso y en la Tabla 97, se indica la descripción de todas sus in

TABLA 98.- *Descripción de las interfaces del Switch de la Garita*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA GARITA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Trunk	-	-	
2	FastEthernet 1/2	Access	10	20	Ed. Central Admins
3	FastEthernet 1/3	Trunk	-	-	
4	FastEthernet 1/4	Trunk	-	-	
5	FastEthernet 1/5	Trunk	-	-	
6	FastEthernet 1/6	Trunk	-	-	

7	FastEthernet 1/7	Trunk	-	-	
8	FastEthernet 1/8	Trunk	-	-	
9	FastEthernet 1/9	Trunk	-	-	
10	FastEthernet 1/10	Trunk	-	-	
11	FastEthernet 1/11	Trunk	-	-	
12	FastEthernet 1/12	Trunk	-	-	
13	FastEthernet 1/13	Trunk	-	-	
14	FastEthernet 1/14	Trunk	-	-	
15	FastEthernet 1/15	Trunk	-	-	
16	FastEthernet 1/16	Trunk	-	-	
17	FastEthernet 1/17	Trunk	-	-	
18	FastEthernet 1/18	Trunk	-	-	
19	FastEthernet 1/19	Access	2	6	AP - UTN
20	FastEthernet 1/20	Access	2	6	AP – UTN
21	FastEthernet 1/21	Access	2	6	AP – UTN
22	FastEthernet 1/22	Access	2	6	AP – UTN
23	FastEthernet 1/23	Access	2	6	AP – UTN
24	FastEthernet 1/24	Access	2	6	AP – UTN
25	FastEthernet 1/26	Trunk	-	-	
26	FastEthernet 1/26	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red de la FICA

En la Facultad de Ingeniería en Ciencias Aplicadas existen varios Racks donde se alojan el Switch de Core Secundario (Backup) y varios Switchs de Acceso.

- **Cuarto de Equipos**

En el cuarto de equipos de la FICA se encuentra solamente el Switch de Core, y en la Tabla 98 se muestra las configuraciones de las interfaces del Switch

TABLA 99.- *Descripción de las interfaces del Switch de Core de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH CORE SECUNDARIO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	TenFastEthernet 1/1	Access	1	1	-

2	TenFastEthernet 1/2	Access	1	1	-
3	GigabitEthernet 1/3	Access	1	1	-
4	GigabitEthernet 1/4	Access	1	1	-
5	GigabitEthernet 1/5	Access	1	1	-
6	GigabitEthernet 1/6	Access	1	1	-
7	GigabitEthernet 2/1	Trunk	-	-	Fibra FICA-Ed. Central
8	GigabitEthernet 2/2	Trunk	-	-	Fibra FICA-Biblioteca
9	GigabitEthernet 2/3	Trunk	-	-	Fibra FICA-FICAYA
10	GigabitEthernet 2/4	Trunk	-	-	Fibra FICA-FACAE
11	GigabitEthernet 2/5	Trunk	-	-	Fibra FICA-Ed. Central
12	GigabitEthernet 2/6	Trunk	-	-	Fibra FICA-FCCSS
13	GigabitEthernet 3/1	Trunk	-	-	Fibra FICA-FECYT
14	GigabitEthernet 3/2	Trunk	-	-	Fibra FICA-Postgrado
15	GigabitEthernet 3/3	Trunk	-	-	Sw-FICA-LAB-1
16	GigabitEthernet ¾	Access	1	1	Libre
17	GigabitEthernet 3/5	Access	1	1	Libre
18	GigabitEthernet 3/6	Access	1	1	Libre
19	FastEthernet 4/1	Access	14	44	FICA-Administrativos
20	FastEthernet 4/2	Access	14	44	FICA-Administrativos
21	FastEthernet 4/3	Access	14	44	FICA-Administrativos
22	FastEthernet 4/4	Access	14	44	FICA-Administrativos
23	FastEthernet 4/5	Access	14	44	FICA-Administrativos
24	FastEthernet 4/6	Access	14	44	FICA-Administrativos
25	FastEthernet 4/7	Access	121	3	IP públicas
26	FastEthernet 4/8	Access	14	44	FICA-Administrativos
27	FastEthernet 4/9	Access	14	44	FICA-Administrativos
28	FastEthernet 4/10	Access	2	6	AP - UTN
29	FastEthernet 4/11	Access	14	44	FICA-Administrativos
30	FastEthernet 4/12	Access	14	44	FICA-Administrativos
31	FastEthernet 4/13	Access	14	44	FICA-Administrativos
32	FastEthernet 4/14	Access	2	6	AP - UTN
33	FastEthernet 4/15	Access	14	44	FICA-Administrativos
34	FastEthernet 4/16	Access	14	44	FICA-Administrativos
35	FastEthernet 4/17	Access	1	1	Servidor de Monitoreo
36	FastEthernet 4/18	Access	14	44	FICA-Administrativos

37	FastEthernet 4/19	Access	14	44	FICA-Administrativos
38	FastEthernet 4/20	Access	14	44	FICA-Administrativos
39	FastEthernet 4/21	Access	14	44	FICA-Administrativos
40	FastEthernet 4/22	Access	14	44	FICA-Administrativos
41	FastEthernet 4/23	Access	14	44	FICA-Administrativos
42	FastEthernet 4/24	Access	14	44	FICA-Administrativos
43	FastEthernet 4/25	Access	14	44	FICA-Administrativos
44	FastEthernet 4/26	Access	14	44	FICA-Administrativos
45	FastEthernet 4/27	Access	14	44	FICA-Administrativos
46	FastEthernet 4/28	Access	14	44	FICA-Administrativos
47	FastEthernet 4/29	Access	1	1	Servidor Opina
48	FastEthernet 4/30	Access	1	1	Servidor Moodle
49	FastEthernet 4/31	Access	16	40	FICA-Laboratorios
50	FastEthernet 4/32	Access	16	40	FICA-Laboratorios
51	FastEthernet 4/33	Access	16	40	FICA-Laboratorios
52	FastEthernet 4/34	Access	16	40	FICA-Laboratorios
53	FastEthernet 4/35	Access	16	40	FICA-Laboratorios
54	FastEthernet 4/36	Access	16	40	FICA-Laboratorios
55	FastEthernet 4/37	Access	2	6	AP-UTN
56	FastEthernet 4/38	Access	16	40	FICA-Laboratorios
57	FastEthernet 4/39	Access	2	6	AP-UTN
58	FastEthernet 4/40	Access	2	6	AP-UTN
59	FastEthernet 4/41	Access	16	40	FICA-Laboratorios
60	FastEthernet 4/42	Access	16	40	FICA-Laboratorios
61	FastEthernet 4/43	Trunk	-	-	Sw-FICA-LAB-1
62	FastEthernet 4/44	Trunk	-	-	Sw-FICA-LAB-2
63	FastEthernet 4/45	Trunk	-	-	Sw-FICA-LAB-3
64	FastEthernet 4/46	Trunk	-	-	Sw-FICA-LAB-4
65	FastEthernet 4/47	Trunk	-	-	Sw-FICA-ASO-PROF
66	FastEthernet 4/48	Trunk	-	-	Sw-FICA-SALA
67	FastEthernet 5/1	Access	14	44	FICA-Administrativos
68	FastEthernet 5/2	Access	14	44	FICA-Administrativos
69	FastEthernet 5/3	Access	14	44	FICA-Administrativos
70	FastEthernet 5/4	Access	14	44	FICA-Administrativos
71	FastEthernet 5/5	Access	14	44	FICA-Administrativos

72	FastEthernet 5/6	Access	14	44	FICA-Administrativos
73	FastEthernet 5/7	Access	14	44	FICA-Administrativos
74	FastEthernet 5/8	Access	14	44	FICA-Administrativos
75	FastEthernet 5/9	Access	14	44	FICA-Administrativos
76	FastEthernet 5/10	Access	14	44	FICA-Administrativos
77	FastEthernet 5/11	Access	14	44	FICA-Administrativos
78	FastEthernet 5/12	Access	14	44	FICA-Administrativos
79	FastEthernet 5/13	Access	14	44	FICA-Administrativos
80	FastEthernet 5/14	Access	14	44	FICA-Administrativos
81	FastEthernet 5/15	Access	14	44	FICA-Administrativos
82	FastEthernet 5/16	Access	14	44	FICA-Administrativos
83	FastEthernet 5/17	Access	14	44	FICA-Administrativos
84	FastEthernet 5/18	Access	14	44	FICA-Administrativos
85	FastEthernet 5/19	Access	14	44	FICA-Administrativos
86	FastEthernet 5/20	Access	14	44	FICA-Administrativos
87	FastEthernet 5/21	Access	14	44	FICA-Administrativos
88	FastEthernet 5/22	Access	14	44	FICA-Administrativos
89	FastEthernet 5/23	Access	2	6	AP-UTN
90	FastEthernet 5/24	Access	14	44	FICA-Administrativos
91	FastEthernet 5/25	Access	14	44	FICA-Administrativos
92	FastEthernet 5/26	Access	14	44	FICA-Administrativos
93	FastEthernet 5/27	Access	14	44	FICA-Administrativos
94	FastEthernet 5/28	Access	14	44	FICA-Administrativos
95	FastEthernet 5/29	Access	14	44	FICA-Administrativos
96	FastEthernet 5/30	Access	14	44	FICA-Administrativos
97	FastEthernet 5/31	Access	14	44	FICA-Administrativos
98	FastEthernet 5/32	Access	14	44	FICA-Administrativos
99	FastEthernet 5/33	Access	14	44	FICA-Administrativos
100	FastEthernet 5/34	Access	14	44	FICA-Administrativos
101	FastEthernet 5/35	Access	16	40	Servidor Proxy FICA
102	FastEthernet 5/36	Access	14	44	FICA-Administrativos
103	FastEthernet 5/37	Access	14	44	FICA-Administrativos
104	FastEthernet 5/38	Access	14	44	FICA-Administrativos
105	FastEthernet 5/39	Access	122	4	DMZ-FICA
106	FastEthernet 5/40	Access	14	44	FICA-Administrativos

107	FastEthernet 5/41	Access	14	44	FICA-Administrativos
108	FastEthernet 5/42	Access	16	40	Servidor Proxy FICA
109	FastEthernet 5/43	Access	14	44	FICA-Administrativos
110	FastEthernet 5/44	Access	14	44	FICA-Administrativos
111	FastEthernet 5/45	Access	14	44	FICA-Administrativos
112	FastEthernet 5/46	Access	14	44	FICA-Administrativos
113	FastEthernet 5/47	Access	14	44	FICA-Administrativos
114	FastEthernet 5/48	Access	14	44	FICA-Administrativos
115	FastEthernet 6/1	Access	14	44	FICA-Administrativos
116	FastEthernet 6/2	Access	14	44	FICA-Administrativos
117	FastEthernet 6/3	Access	14	44	FICA-Administrativos
118	FastEthernet 6/4	Access	14	44	FICA-Administrativos
119	FastEthernet 6/5	Access	14	44	FICA-Administrativos
120	FastEthernet 6/6	Access	14	44	FICA-Administrativos
121	FastEthernet 6/7	Access	14	44	FICA-Administrativos
122	FastEthernet 6/8	Access	14	44	FICA-Administrativos
123	FastEthernet 6/9	Access	14	44	FICA-Administrativos
124	FastEthernet 6/10	Access	14	44	FICA-Administrativos
125	FastEthernet 6/11	Access	14	44	FICA-Administrativos
126	FastEthernet 6/12	Access	14	44	FICA-Administrativos
127	FastEthernet 6/13	Access	14	44	FICA-Administrativos
128	FastEthernet 6/14	Access	14	44	FICA-Administrativos
129	FastEthernet 6/15	Access	14	44	FICA-Administrativos
130	FastEthernet 6/16	Access	14	44	FICA-Administrativos
131	FastEthernet 6/17	Access	14	44	FICA-Administrativos
132	FastEthernet 6/18	Access	14	44	FICA-Administrativos
133	FastEthernet 6/19	Access	14	44	FICA-Administrativos
134	FastEthernet 6/20	Access	14	44	FICA-Administrativos
135	FastEthernet 6/21	Access	14	44	FICA-Administrativos
136	FastEthernet 6/22	Access	14	44	FICA-Administrativos
137	FastEthernet 6/23	Access	14	44	FICA-Administrativos
138	FastEthernet 6/24	Access	14	44	FICA-Administrativos
139	FastEthernet 6/25	Access	14	44	FICA-Administrativos
140	FastEthernet 6/26	Access	14	44	FICA-Administrativos
141	FastEthernet 6/27	Access	14	44	FICA-Administrativos

142	FastEthernet 6/28	Access	14	44	FICA-Administrativos
143	FastEthernet 6/29	Access	14	44	FICA-Administrativos
144	FastEthernet 6/30	Access	14	44	FICA-Administrativos
145	FastEthernet 6/31	Access	14	44	FICA-Administrativos
146	FastEthernet 6/32	Access	14	44	FICA-Administrativos
147	FastEthernet 6/33	Access	14	44	FICA-Administrativos
148	FastEthernet 6/34	Access	14	44	FICA-Administrativos
149	FastEthernet 6/35	Access	14	44	FICA-Administrativos
150	FastEthernet 6/36	Access	14	44	FICA-Administrativos
151	FastEthernet 6/37	Access	14	44	FICA-Administrativos
152	FastEthernet 6/38	Access	14	44	FICA-Administrativos
153	FastEthernet 6/39	Access	14	44	FICA-Administrativos
154	FastEthernet 6/40	Access	14	44	FICA-Administrativos
155	FastEthernet 6/41	Access	14	44	FICA-Administrativos
156	FastEthernet 6/42	Access	14	44	FICA-Administrativos
157	FastEthernet 6/43	Access	1	1	Sub Decano FICA
158	FastEthernet 6/44	Access	14	44	FICA-Administrativos
159	FastEthernet 6/45	Access	14	44	FICA-Administrativos
160	FastEthernet 6/46	Access	4	16	FICA-Financiero
161	FastEthernet 6/47	Access	14	44	FICA-Administrativos
162	FastEthernet 6/48	Access	14	44	FICA-Administrativos

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio I**

En el Laboratorio I existe un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 99 se muestra la descripción de las interfaces de dicho Switch.

TABLA 100.- *Descripción de las interfaces del Switch del Laboratorio I de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL LABORATORIO I DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios
3	FastEthernet 0/3	Access	16	40	FICA Laboratorios

4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios
7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios
35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios

37	FastEthernet 0/37	Access	16	40	FICA Laboratorios
38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios
41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios
47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	16	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio II**

En el Laboratorio II existe un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 100 se muestra la descripción de las interfaces de dicho Switch.

TABLA 101.- *Descripción de las interfaces del Switch del Laboratorio II de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL LABORATORIO II DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios
3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios

6	FastEthernet 0/6	Access	16	40	FICA Laboratorios
7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios
35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios
37	FastEthernet 0/37	Access	16	40	FICA Laboratorios

38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios
41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios
47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	16	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: Dirección de Desarrollo Tecnológico e Informático - UTN

- **Laboratorio III**

En el Laboratorio III existen dos Switchs de acceso para todos los equipos que existen en el mismo, en la Tabla 101 y en la Tabla 102 se muestra la descripción de las interfaces de ambos Switchs.

TABLA 102.- *Descripción de las interfaces del Switch 01 del Laboratorio III de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL LABORATORIO III DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios

3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios
7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios

35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios
37	FastEthernet 0/37	Access	16	40	FICA Laboratorios
38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios
41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios
47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	16	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Trunk	-	-	Distribución FICA

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 103.- *Descripción de las interfaces del Switch 02 del Laboratorio III de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL LABORATORIO III DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios
3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios

7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	GigabitEthernet 0/1	Trunk	-	-	FICA Lab3-01
26	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio IV**

En el Laboratorio IV existen dos Switchs de acceso para todos los equipos que existen en el mismo, en la Tabla 103 y en la Tabla 104 se muestra la descripción de las interfaces de ambos Switchs.

TABLA 104.- *Descripción de las interfaces del Switch 01 del Laboratorio IV de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL LABORATORIO IV DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios

3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios
7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios

35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios
37	FastEthernet 0/37	Access	16	40	FICA Laboratorios
38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios
41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios
47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	16	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Trunk	-	-	FICA Lab 4-02

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 105.- *Descripción de las interfaces del Switch 02 del Laboratorio IV de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL LABORATORIO IV DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios
3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios

7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios
35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios
37	FastEthernet 0/37	Access	16	40	FICA Laboratorios
38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios

41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios
47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	16	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	FICA Lab 4-01
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Laboratorio Cisco**

En el Laboratorio Cisco existen dos Switchs de acceso para todos los equipos que existen en el mismo, en la Tabla 105 y en la Tabla 106 se muestra la descripción de las interfaces de ambos Switchs.

TABLA 106.- *Descripción de las interfaces del Switch 01 del Laboratorio Cisco de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 D EL LABORATORIO CISCO DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios
3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios
7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios

12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios
25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios
35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios
37	FastEthernet 0/37	Access	16	40	FICA Laboratorios
38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios
41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios

47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	16	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Trunk	-	-	Cisco 02

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 107.- *Descripción de las interfaces del Switch 02 del Laboratorio Cisco de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL LABORATORIO CISCO DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	16	40	FICA Laboratorios
2	FastEthernet 0/2	Access	16	40	FICA Laboratorios
3	FastEthernet 0/3	Access	16	40	FICA Laboratorios
4	FastEthernet 0/4	Access	16	40	FICA Laboratorios
5	FastEthernet 0/5	Access	16	40	FICA Laboratorios
6	FastEthernet 0/6	Access	16	40	FICA Laboratorios
7	FastEthernet 0/7	Access	16	40	FICA Laboratorios
8	FastEthernet 0/8	Access	16	40	FICA Laboratorios
9	FastEthernet 0/9	Access	16	40	FICA Laboratorios
10	FastEthernet 0/10	Access	16	40	FICA Laboratorios
11	FastEthernet 0/11	Access	16	40	FICA Laboratorios
12	FastEthernet 0/12	Access	16	40	FICA Laboratorios
13	FastEthernet 0/13	Access	16	40	FICA Laboratorios
14	FastEthernet 0/14	Access	16	40	FICA Laboratorios
15	FastEthernet 0/15	Access	16	40	FICA Laboratorios
16	FastEthernet 0/16	Access	16	40	FICA Laboratorios
17	FastEthernet 0/17	Access	16	40	FICA Laboratorios
18	FastEthernet 0/18	Access	16	40	FICA Laboratorios
19	FastEthernet 0/19	Access	16	40	FICA Laboratorios
20	FastEthernet 0/20	Access	16	40	FICA Laboratorios
21	FastEthernet 0/21	Access	16	40	FICA Laboratorios
22	FastEthernet 0/22	Access	16	40	FICA Laboratorios
23	FastEthernet 0/23	Access	16	40	FICA Laboratorios
24	FastEthernet 0/24	Access	16	40	FICA Laboratorios

25	FastEthernet 0/25	Access	16	40	FICA Laboratorios
26	FastEthernet 0/26	Access	16	40	FICA Laboratorios
27	FastEthernet 0/27	Access	16	40	FICA Laboratorios
28	FastEthernet 0/28	Access	16	40	FICA Laboratorios
29	FastEthernet 0/29	Access	16	40	FICA Laboratorios
30	FastEthernet 0/30	Access	16	40	FICA Laboratorios
31	FastEthernet 0/31	Access	16	40	FICA Laboratorios
32	FastEthernet 0/32	Access	16	40	FICA Laboratorios
33	FastEthernet 0/33	Access	16	40	FICA Laboratorios
34	FastEthernet 0/34	Access	16	40	FICA Laboratorios
35	FastEthernet 0/35	Access	16	40	FICA Laboratorios
36	FastEthernet 0/36	Access	16	40	FICA Laboratorios
37	FastEthernet 0/37	Access	16	40	FICA Laboratorios
38	FastEthernet 0/38	Access	16	40	FICA Laboratorios
39	FastEthernet 0/39	Access	16	40	FICA Laboratorios
40	FastEthernet 0/40	Access	16	40	FICA Laboratorios
41	FastEthernet 0/41	Access	16	40	FICA Laboratorios
42	FastEthernet 0/42	Access	16	40	FICA Laboratorios
43	FastEthernet 0/43	Access	16	40	FICA Laboratorios
44	FastEthernet 0/44	Access	16	40	FICA Laboratorios
45	FastEthernet 0/45	Access	16	40	FICA Laboratorios
46	FastEthernet 0/46	Access	16	40	FICA Laboratorios
47	FastEthernet 0/47	Access	16	40	FICA Laboratorios
48	FastEthernet 0/48	Access	18	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Cisco 01
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático -. UTN*

- **Sala de Investigación**

En la Sala de Investigación existe un Switch de acceso para todos los equipos que existen en la misma, en la Tabla 107 se muestra la descripción de las interfaces de dicho Switch.

TABLA 108.- *Descripción de las interfaces del Switch de la Sala de Investigación de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA SALA DE INVESTIGACIÓN DE LA FICA					
N°	Interfaz	SwitchPort	Vlan	Vlan	Descripción

		Mode	Actual	Nueva	
1	FastEthernet 0/1	Access	18	40	FICA Laboratorios
2	FastEthernet 0/2	Access	18	40	FICA Laboratorios
3	FastEthernet 0/3	Access	18	40	FICA Laboratorios
4	FastEthernet 0/4	Access	18	40	FICA Laboratorios
5	FastEthernet 0/5	Access	18	40	FICA Laboratorios
6	FastEthernet 0/6	Access	18	40	FICA Laboratorios
7	FastEthernet 0/7	Access	18	40	FICA Laboratorios
8	FastEthernet 0/8	Access	18	40	FICA Laboratorios
9	FastEthernet 0/9	Access	18	40	FICA Laboratorios
10	FastEthernet 0/10	Access	18	40	FICA Laboratorios
11	FastEthernet 0/11	Access	18	40	FICA Laboratorios
12	FastEthernet 0/12	Access	18	40	FICA Laboratorios
13	FastEthernet 0/13	Access	18	40	FICA Laboratorios
14	FastEthernet 0/14	Access	18	40	FICA Laboratorios
15	FastEthernet 0/15	Access	18	40	FICA Laboratorios
16	FastEthernet 0/16	Access	18	40	FICA Laboratorios
17	FastEthernet 0/17	Access	18	40	FICA Laboratorios
18	FastEthernet 0/18	Access	18	40	FICA Laboratorios
19	FastEthernet 0/19	Access	18	40	FICA Laboratorios
20	FastEthernet 0/20	Access	18	40	FICA Laboratorios
21	FastEthernet 0/21	Access	68	40	FICA Laboratorios
22	FastEthernet 0/22	Access	18	40	FICA Laboratorios
23	FastEthernet 0/23	Access	18	40	FICA Laboratorios
24	FastEthernet 0/24	Access	18	40	FICA Laboratorios
25	FastEthernet 0/25	Access	18	40	FICA Laboratorios
26	FastEthernet 0/26	Access	18	40	FICA Laboratorios
27	FastEthernet 0/27	Access	18	40	FICA Laboratorios
28	FastEthernet 0/28	Access	18	40	FICA Laboratorios
29	FastEthernet 0/29	Access	18	40	FICA Laboratorios
30	FastEthernet 0/30	Access	18	40	FICA Laboratorios
31	FastEthernet 0/31	Access	18	40	FICA Laboratorios
32	FastEthernet 0/32	Access	18	40	FICA Laboratorios
33	FastEthernet 0/33	Access	18	40	FICA Laboratorios
34	FastEthernet 0/34	Access	18	40	FICA Laboratorios

35	FastEthernet 0/35	Access	18	40	FICA Laboratorios
36	FastEthernet 0/36	Access	18	40	FICA Laboratorios
37	FastEthernet 0/37	Access	18	40	FICA Laboratorios
38	FastEthernet 0/38	Access	18	40	FICA Laboratorios
39	FastEthernet 0/39	Access	18	40	FICA Laboratorios
40	FastEthernet 0/40	Access	18	40	FICA Laboratorios
41	FastEthernet 0/41	Access	18	40	FICA Laboratorios
42	FastEthernet 0/42	Access	18	40	FICA Laboratorios
43	FastEthernet 0/43	Access	18	40	FICA Laboratorios
44	FastEthernet 0/44	Access	18	40	FICA Laboratorios
45	FastEthernet 0/45	Access	18	40	FICA Laboratorios
46	FastEthernet 0/46	Access	18	40	FICA Laboratorios
47	FastEthernet 0/47	Access	18	40	FICA Laboratorios
48	FastEthernet 0/48	Access	18	40	FICA Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Sala de Profesores**

En la Sala de Profesores existe un Switch de acceso para todos los equipos que existen en la misma, en la Tabla 108 se muestra la descripción de las interfaces de dicho Switch.

TABLA 109.- *Descripción de las interfaces del Switch de la Sala de Profesores de la FICA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA SALA DE PROFESORES DE LA FICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	14	44	FICA Administrativos
2	FastEthernet 0/2	Access	14	44	FICA Administrativos
3	FastEthernet 0/3	Access	14	44	FICA Administrativos
4	FastEthernet 0/4	Access	14	44	FICA Administrativos
5	FastEthernet 0/5	Access	14	44	FICA Administrativos
6	FastEthernet 0/6	Access	14	44	FICA Administrativos
7	FastEthernet 0/7	Access	14	44	FICA Administrativos
8	FastEthernet 0/8	Access	14	44	FICA Administrativos
9	FastEthernet 0/9	Access	14	44	FICA Administrativos
10	FastEthernet 0/10	Access	14	44	FICA Administrativos

11	FastEthernet 0/11	Access	14	44	FICA Administrativos
12	FastEthernet 0/12	Access	14	44	FICA Administrativos
13	FastEthernet 0/13	Access	14	44	FICA Administrativos
14	FastEthernet 0/14	Access	14	44	FICA Administrativos
15	FastEthernet 0/15	Access	14	44	FICA Administrativos
16	FastEthernet 0/16	Access	14	44	FICA Administrativos
17	FastEthernet 0/17	Access	14	44	FICA Administrativos
18	FastEthernet 0/18	Access	14	44	FICA Administrativos
19	FastEthernet 0/19	Access	2	6	AP - UTN
20	FastEthernet 0/20	Access	2	6	AP - UTN
21	FastEthernet 0/21	Access	14	44	FICA Administrativos
22	FastEthernet 0/22	Access	14	44	FICA Administrativos
23	FastEthernet 0/23	Access	14	44	FICA Administrativos
24	FastEthernet 0/24	Access	14	44	FICA Administrativos
25	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
26	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Equipos de red de la FICAYA

En la Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales existe un Racks donde se alojan varios Switchs de Acceso, además en las granjas La Pradera y Yuyucocha también existen Switchs de Acceso.

- **Cuarto de Equipos**

En el cuarto de equipos de la FICAYA se encuentran varios Switchs de Acceso, y en las Tablas 109, 110, 111 y 112 se muestra las configuraciones de las interfaces de los Switchs. El Switch Linksys SR224 es un Switch capa 2 no administrable.

TABLA 110.- *Descripción de las interfaces del Switch 01 del cuarto de equipos de la FICAYA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL CUARTO DE EQUIPOS DE LA FICAYA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
2	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
3	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
4	GigabitEthernet 1	Access	20	52	FICAYA - Admin.

5	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
6	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
7	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
8	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
9	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
10	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
11	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
12	GigabitEthernet 1	Trunk	-	-	
13	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
14	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
15	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
16	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
17	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
18	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
19	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
20	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
21	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
22	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
23	GigabitEthernet 1	Trunk	-	-	
24	GigabitEthernet 1	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 111.- *Descripción de las interfaces del Switch 02 del cuarto de equipos de la FICAYA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL CUARTO DE EQUIPOS DE LA FICAYA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
2	GigabitEthernet 2	Access	20	52	FICAYA - Admin.
3	GigabitEthernet 3	Access	20	52	FICAYA - Admin.
4	GigabitEthernet 4	Access	20	52	FICAYA - Admin.
5	GigabitEthernet 5	Access	20	52	FICAYA - Admin.
6	GigabitEthernet 6	Access	20	52	FICAYA - Admin.
7	GigabitEthernet 7	Access	20	52	FICAYA - Admin.

8	GigabitEthernet 8	Access	20	52	FICAYA - Admin.
9	GigabitEthernet 9	Access	20	52	FICAYA - Admin.
10	GigabitEthernet 10	Access	20	52	FICAYA - Admin.
11	GigabitEthernet 11	Access	20	52	FICAYA - Admin.
12	GigabitEthernet 12	Trunk	-	-	
13	GigabitEthernet 13	Access	20	52	FICAYA - Admin.
14	GigabitEthernet 14	Access	20	52	FICAYA - Admin.
15	GigabitEthernet 15	Access	20	52	FICAYA - Admin.
16	GigabitEthernet 16	Access	20	52	FICAYA - Admin.
17	GigabitEthernet 17	Access	20	52	FICAYA - Admin.
18	GigabitEthernet 18	Access	20	52	FICAYA - Admin.
19	GigabitEthernet 19	Access	20	52	FICAYA - Admin.
20	GigabitEthernet 20	Access	20	52	FICAYA - Admin.
21	GigabitEthernet 21	Access	20	52	FICAYA - Admin.
22	GigabitEthernet 22	Access	20	52	FICAYA - Admin.
23	GigabitEthernet 23	Access	20	52	FICAYA - Admin.
24	GigabitEthernet 24	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 112.- *Descripción de las interfaces del Switch 03 del cuarto de equipos de la FICAYA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL CUARTO DE EQUIPOS DE LA FICAYA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Access	20	52	FICAYA - Admin.
2	FastEthernet 1/2	Access	20	52	FICAYA - Admin.
3	FastEthernet 1/3	Access	20	52	FICAYA - Admin.
4	FastEthernet 1/4	Access	20	52	FICAYA - Admin.
5	FastEthernet 1/5	Access	20	52	FICAYA - Admin.
6	FastEthernet 1/6	Access	20	52	FICAYA - Admin.
7	FastEthernet 1/7	Access	20	52	FICAYA - Admin.
8	FastEthernet 1/8	Access	20	52	FICAYA - Admin.
9	FastEthernet 1/9	Access	20	52	FICAYA - Admin.
10	FastEthernet 1/10	Access	20	52	FICAYA - Admin.

11	FastEthernet 1/11	Access	20	52	FICAYA - Admin.
12	FastEthernet 1/12	Access	20	52	FICAYA - Admin.
13	FastEthernet 1/13	Access	20	52	FICAYA - Admin.
14	FastEthernet 1/14	Access	20	52	FICAYA - Admin.
15	FastEthernet 1/15	Access	20	52	FICAYA - Admin.
16	FastEthernet 1/16	Access	20	52	FICAYA - Admin.
17	FastEthernet 1/17	Access	20	52	FICAYA - Admin.
18	FastEthernet 1/18	Access	20	52	FICAYA - Admin.
19	FastEthernet 1/19	Access	20	52	FICAYA - Admin.
20	FastEthernet 1/20	Access	20	52	FICAYA - Admin.
21	FastEthernet 1/21	Access	20	52	FICAYA - Admin.
22	FastEthernet 1/22	Access	20	52	FICAYA - Admin.
23	FastEthernet 1/23	Access	20	52	FICAYA - Admin.
24	FastEthernet 1/24	Access	20	52	FICAYA - Admin.
25	GigabitEthernet 1/25	Trunk	-	-	
26	GigabitEthernet 1/26	Trunk	-	-	

***Fuente**: Dirección de Desarrollo Tecnológico e Informático – UTN*

***TABLA 113.-** Descripción de las interfaces del Switch 04 del cuarto de equipos de la FICAYA*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 04 DEL CUARTO DE EQUIPOS DE LA FICAYA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Trunk	-	-	-
2	FastEthernet 1/2	Access	20	52	FICAYA - Admin.
3	FastEthernet 1/3	Access	20	52	FICAYA - Admin.
4	FastEthernet 1/4	Access	20	52	FICAYA - Admin.
5	FastEthernet 1/5	Access	20	52	FICAYA - Admin.
6	FastEthernet 1/6	Access	20	52	FICAYA - Admin.
7	FastEthernet 1/7	Access	20	52	FICAYA - Admin.
8	FastEthernet 1/8	Access	20	52	FICAYA - Admin.
9	FastEthernet 1/9	Access	20	52	FICAYA - Admin.
10	FastEthernet 1/10	Access	20	52	FICAYA - Admin.

11	FastEthernet 1/11	Access	20	52	FICAYA - Admin.
12	FastEthernet 1/12	Access	20	52	FICAYA - Admin.
13	FastEthernet 1/13	Access	20	52	FICAYA - Admin.
14	FastEthernet 1/14	Access	20	52	FICAYA - Admin.
15	FastEthernet 1/15	Access	20	52	FICAYA - Admin.
16	FastEthernet 1/16	Access	20	52	FICAYA - Admin.
17	FastEthernet 1/17	Access	20	52	FICAYA - Admin.
18	FastEthernet 1/18	Access	20	52	FICAYA - Admin.
19	FastEthernet 1/19	Access	20	52	FICAYA - Admin.
20	FastEthernet 1/20	Access	20	52	FICAYA - Admin.
21	FastEthernet 1/21	Access	20	52	FICAYA - Admin.
22	FastEthernet 1/22	Access	2	2	AP – UTN
23	FastEthernet 1/23	Access	2	2	AP – UTN
24	FastEthernet 1/24	Access	2	2	AP – UTN

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Granja La Pradera**

En la granja La Pradera existe un solo Switch del cual se indica la descripción de cada una de las interfaces en la Tabla 113

TABLA 114.- *Descripción de las interfaces del Switch de la Granja la Pradera*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA GRANJA LA PRADERA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1	Access	22	48	FICAYA - Laboratorios
2	FastEthernet 2	Access	22	48	FICAYA - Laboratorios
3	FastEthernet 3	Access	22	48	FICAYA - Laboratorios
4	FastEthernet 4	Access	22	48	FICAYA - Laboratorios
5	FastEthernet 5	Access	22	48	FICAYA - Laboratorios
6	FastEthernet 6	Access	22	48	FICAYA - Laboratorios
7	FastEthernet 7	Access	22	48	FICAYA - Laboratorios
8	FastEthernet 8	Access	22	48	FICAYA - Laboratorios
9	FastEthernet 9	Access	22	48	FICAYA - Laboratorios

10	FastEthernet 10	Access	22	48	FICAYA - Laboratorios
11	FastEthernet 11	Access	22	48	FICAYA - Laboratorios
12	FastEthernet 12	Access	22	48	FICAYA - Laboratorios
13	FastEthernet 13	Access	22	48	FICAYA - Laboratorios
14	FastEthernet 14	Access	22	48	FICAYA - Laboratorios
15	FastEthernet 15	Access	22	48	FICAYA - Laboratorios
16	FastEthernet 16	Access	22	48	FICAYA - Laboratorios
17	FastEthernet 17	Access	22	48	FICAYA - Laboratorios
18	FastEthernet 18	Access	22	48	FICAYA - Laboratorios
19	FastEthernet 19	Access	22	48	FICAYA - Laboratorios
20	FastEthernet 20	Access	22	48	FICAYA - Laboratorios
21	FastEthernet 21	Access	22	48	FICAYA - Laboratorios
22	FastEthernet 22	Access	22	48	FICAYA - Laboratorios
23	FastEthernet 23	Access	22	48	FICAYA - Laboratorios
24	FastEthernet 24	Access	22	48	FICAYA - Laboratorios
25	FastEthernet 25	Access	22	48	FICAYA - Laboratorios
26	FastEthernet 26	Access	22	48	FICAYA - Laboratorios
27	FastEthernet 27	Access	22	48	FICAYA - Laboratorios
28	FastEthernet 28	Access	22	48	FICAYA - Laboratorios
29	FastEthernet 29	Access	22	48	FICAYA - Laboratorios
30	FastEthernet 30	Access	22	48	FICAYA - Laboratorios
31	FastEthernet 31	Access	22	48	FICAYA - Laboratorios
32	FastEthernet 32	Access	22	48	FICAYA - Laboratorios
33	FastEthernet 33	Access	22	48	FICAYA - Laboratorios
34	FastEthernet 34	Access	22	48	FICAYA - Laboratorios
35	FastEthernet 35	Access	22	48	FICAYA - Laboratorios
36	FastEthernet 36	Access	22	48	FICAYA - Laboratorios
37	FastEthernet 37	Access	22	48	FICAYA - Laboratorios
38	FastEthernet 38	Access	22	48	FICAYA - Laboratorios
39	FastEthernet 39	Access	22	48	FICAYA - Laboratorios
40	FastEthernet 40	Access	22	48	FICAYA - Laboratorios
41	FastEthernet 41	Access	22	48	FICAYA - Laboratorios
42	FastEthernet 42	Access	22	48	FICAYA - Laboratorios
43	FastEthernet 43	Access	22	48	FICAYA - Laboratorios
44	FastEthernet 44	Access	22	48	FICAYA - Laboratorios

45	FastEthernet 45	Access	22	48	FICAYA - Laboratorios
46	FastEthernet 46	Access	22	48	FICAYA - Laboratorios
47	FastEthernet 47	Access	22	48	FICAYA - Laboratorios
48	FastEthernet 48	Access	22	48	FICAYA - Laboratorios
49	GigabitEthernet 1	Trunk	-	-	
50	GigabitEthernet 2	Trunk	-	-	
51	GigabitEthernet 3	Trunk	-	-	
52	GigabitEthernet 4	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Granja Yuyucocha**

En la granja La Pradera existe un solo Switch del cual se indica la descripción de cada una de las interfaces en la Tabla 114

TABLA 115.- *Descripción de las interfaces del Switch de la Granja Yuyucocha*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA GRANJA YUYUCOCHA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	20	52	FICAYA - Admin.
2	GigabitEthernet 2	Access	20	52	FICAYA - Admin.
3	GigabitEthernet 3	Access	20	52	FICAYA - Admin.
4	GigabitEthernet 4	Access	20	52	FICAYA - Admin.
5	GigabitEthernet 5	Access	20	52	FICAYA - Admin.
6	GigabitEthernet 6	Access	20	52	FICAYA - Admin.
7	GigabitEthernet 7	Access	20	52	FICAYA - Admin.
8	GigabitEthernet 8	Access	20	52	FICAYA - Admin.
9	GigabitEthernet 9	Access	20	52	FICAYA - Admin.
10	GigabitEthernet 10	Access	20	52	FICAYA - Admin.
11	GigabitEthernet 11	Access	20	52	FICAYA - Admin.
12	GigabitEthernet 12	Access	20	52	FICAYA - Admin.
13	GigabitEthernet 13	Access	20	52	FICAYA - Admin.
14	GigabitEthernet 14	Access	20	52	FICAYA - Admin.
15	GigabitEthernet 15	Access	20	52	FICAYA - Admin.
16	GigabitEthernet 16	Access	20	52	FICAYA - Admin.

17	GigabitEthernet 17	Access	20	52	FICAYA - Admin.
18	GigabitEthernet 18	Access	20	52	FICAYA - Admin.
19	GigabitEthernet 19	Access	20	52	FICAYA - Admin.
20	GigabitEthernet 20	Access	20	52	FICAYA - Admin.
21	GigabitEthernet 21	Access	20	52	FICAYA - Admin.
22	GigabitEthernet 22	Access	20	52	FICAYA - Admin.
23	GigabitEthernet 23	Access	20	52	FICAYA - Admin.
24	GigabitEthernet 24	Access	20	52	FICAYA - Admin.
25	GigabitEthernet 25	Trunk	-	-	
26	GigabitEthernet 26	Trunk	-	-	
27	GigabitEthernet 27	Trunk	-	-	
28	GigabitEthernet 28	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red de la FECYT

En la Facultad de Educación Ciencia y Tecnología existen varios Racks donde se alojan varios Switchs de Acceso, además los Racks que se encuentran en Educación Física y la Piscina pertenecen a la FECYT.

- **Cuarto de equipos.**

En el cuarto de equipos de la Facultad de Educación Ciencia y Tecnología existen tres Switchs de Acceso, y la descripción de cada una de las interfaces de los mismos se muestran en las Tablas 115, 116, 117.

TABLA 116.- *Descripción de las interfaces del Switch 01 del cuarto de equipos de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL CUARTO DE EQUIPOS DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	40	60	FECYT Admin.
2	FastEthernet 0/2	Access	40	60	FECYT Admin.
3	FastEthernet 0/3	Access	40	60	FECYT Admin.
4	FastEthernet 0/4	Access	40	60	FECYT Admin.
5	FastEthernet 0/5	Access	40	60	FECYT Admin.
6	FastEthernet 0/6	Access	40	60	FECYT Admin.
7	FastEthernet 0/7	Access	40	60	FECYT Admin.

8	FastEthernet 0/8	Access	40	60	FECYT Admin.
9	FastEthernet 0/9	Access	40	60	FECYT Admin.
10	FastEthernet 0/10	Access	40	60	FECYT Admin.
11	FastEthernet 0/11	Access	40	60	FECYT Admin.
12	FastEthernet 0/12	Access	40	60	FECYT Admin.
13	FastEthernet 0/13	Access	40	60	FECYT Admin.
14	FastEthernet 0/14	Access	40	60	FECYT Admin.
15	FastEthernet 0/15	Access	40	60	FECYT Admin.
16	FastEthernet 0/16	Access	40	60	FECYT Admin.
17	FastEthernet 0/17	Access	40	60	FECYT Admin.
18	FastEthernet 0/18	Access	40	60	FECYT Admin.
19	FastEthernet 0/19	Access	40	60	FECYT Admin.
20	FastEthernet 0/20	Access	40	60	FECYT Admin.
21	FastEthernet 0/21	Access	40	60	FECYT Admin.
22	FastEthernet 0/22	Access	40	60	FECYT Admin.
23	FastEthernet 0/23	Access	40	60	FECYT Admin.
24	FastEthernet 0/24	Access	40	60	FECYT Admin.
25	FastEthernet 0/25	Access	40	60	FECYT Admin.
26	FastEthernet 0/26	Access	40	60	FECYT Admin.
27	FastEthernet 0/27	Access	40	60	FECYT Admin.
28	FastEthernet 0/28	Access	40	60	FECYT Admin.
29	FastEthernet 0/29	Access	40	60	FECYT Admin.
30	FastEthernet 0/30	Access	40	60	FECYT Admin.
31	FastEthernet 0/31	Access	40	60	FECYT Admin.
32	FastEthernet 0/32	Access	40	60	FECYT Admin.
33	FastEthernet 0/33	Access	40	60	FECYT Admin.
34	FastEthernet 0/34	Access	40	60	FECYT Admin.
35	FastEthernet 0/35	Access	40	60	FECYT Admin.
36	FastEthernet 0/36	Access	40	60	FECYT Admin.
37	FastEthernet 0/37	Access	40	60	FECYT Admin.
38	FastEthernet 0/38	Access	40	60	FECYT Admin.
39	FastEthernet 0/39	Access	40	60	FECYT Admin.
40	FastEthernet 0/40	Access	40	60	FECYT Admin.
41	FastEthernet 0/41	Access	40	60	FECYT Admin.
42	FastEthernet 0/42	Access	40	60	FECYT Admin.

43	FastEthernet 0/43	Trunk	-	-	Rack Prin. 02
44	FastEthernet 0/44	Trunk	-	-	Rack Prin. 03
45	FastEthernet 0/45	Trunk	-	-	Lab 2
46	FastEthernet 0/46	Trunk	-	-	Lab 1
47	FastEthernet 0/47	Trunk	-	-	Lab Mac
48	FastEthernet 0/48	Trunk	-	-	Coordinación
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Access	1	1	Libre

***Fuente**: Dirección de Desarrollo Tecnológico e Informático – UTN*

***TABLA 117.-** Descripción de las interfaces del Switch 02 del cuarto de equipos de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL CUARTO DE EQUIPOS DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	42	56	FECYT Laboratorios
2	FastEthernet 0/2	Access	42	56	FECYT Laboratorios
3	FastEthernet 0/3	Access	42	56	FECYT Laboratorios
4	FastEthernet 0/4	Access	42	56	FECYT Laboratorios
5	FastEthernet 0/5	Access	42	56	FECYT Laboratorios
6	FastEthernet 0/6	Access	42	56	FECYT Laboratorios
7	FastEthernet 0/7	Access	42	56	FECYT Laboratorios
8	FastEthernet 0/8	Access	42	56	FECYT Laboratorios
9	FastEthernet 0/9	Access	42	56	FECYT Laboratorios
10	FastEthernet 0/10	Access	42	56	FECYT Laboratorios
11	FastEthernet 0/11	Access	42	56	FECYT Laboratorios
12	FastEthernet 0/12	Access	42	56	FECYT Laboratorios
13	FastEthernet 0/13	Access	42	56	FECYT Laboratorios
14	FastEthernet 0/14	Access	42	56	FECYT Laboratorios
15	FastEthernet 0/15	Access	42	56	FECYT Laboratorios
16	FastEthernet 0/16	Access	42	56	FECYT Laboratorios
17	FastEthernet 0/17	Access	42	56	FECYT Laboratorios
18	FastEthernet 0/18	Access	42	56	FECYT Laboratorios
19	FastEthernet 0/19	Access	42	56	FECYT Laboratorios
20	FastEthernet 0/20	Access	42	56	FECYT Laboratorios

21	FastEthernet 0/21	Access	42	56	FECYT Laboratorios
22	FastEthernet 0/22	Access	42	56	FECYT Laboratorios
23	FastEthernet 0/23	Access	42	56	FECYT Laboratorios
24	FastEthernet 0/24	Access	42	56	FECYT Laboratorios
25	FastEthernet 0/25	Access	42	56	FECYT Laboratorios
26	FastEthernet 0/26	Access	42	56	FECYT Laboratorios
27	FastEthernet 0/27	Access	42	56	FECYT Laboratorios
28	FastEthernet 0/28	Access	42	56	FECYT Laboratorios
29	FastEthernet 0/29	Access	42	56	FECYT Laboratorios
30	FastEthernet 0/30	Access	42	56	FECYT Laboratorios
31	FastEthernet 0/31	Access	42	56	FECYT Laboratorios
32	FastEthernet 0/32	Access	42	56	FECYT Laboratorios
33	FastEthernet 0/33	Access	42	56	FECYT Laboratorios
34	FastEthernet 0/34	Access	42	56	FECYT Laboratorios
35	FastEthernet 0/35	Access	42	56	FECYT Laboratorios
36	FastEthernet 0/36	Access	42	56	FECYT Laboratorios
37	FastEthernet 0/37	Access	42	56	FECYT Laboratorios
38	FastEthernet 0/38	Access	42	56	FECYT Laboratorios
39	FastEthernet 0/39	Access	42	56	FECYT Laboratorios
40	FastEthernet 0/40	Access	42	56	FECYT Laboratorios
41	FastEthernet 0/41	Access	42	56	FECYT Laboratorios
42	FastEthernet 0/42	Access	42	56	FECYT Laboratorios
43	FastEthernet 0/43	Access	42	56	FECYT Laboratorios
44	FastEthernet 0/44	Access	42	56	FECYT Laboratorios
45	FastEthernet 0/45	Access	42	56	FECYT Laboratorios
46	FastEthernet 0/46	Access	42	56	FECYT Laboratorios
47	FastEthernet 0/47	Access	42	56	FECYT Laboratorios
48	FastEthernet 0/48	Access	42	56	FECYT Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	FECYT Rack Prin. 02
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 118.- *Descripción de las interfaces del Switch 03 del cuarto de equipos de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL CUARTO DE EQUIPOS DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	40	60	FECYT Admin.
2	FastEthernet 0/2	Access	40	60	FECYT Admin.
3	FastEthernet 0/3	Access	40	60	FECYT Admin.
4	FastEthernet 0/4	Access	40	60	FECYT Admin.
5	FastEthernet 0/5	Access	40	60	FECYT Admin.
6	FastEthernet 0/6	Access	40	60	FECYT Admin.
7	FastEthernet 0/7	Access	40	60	FECYT Admin.
8	FastEthernet 0/8	Access	40	60	FECYT Admin.
9	FastEthernet 0/9	Access	40	60	FECYT Admin.
10	FastEthernet 0/10	Access	40	60	FECYT Admin.
11	FastEthernet 0/11	Access	40	60	FECYT Admin.
12	FastEthernet 0/12	Access	40	60	FECYT Admin.
13	FastEthernet 0/13	Access	40	60	FECYT Admin.
14	FastEthernet 0/14	Access	40	60	FECYT Admin.
15	FastEthernet 0/15	Access	40	60	FECYT Admin.
16	FastEthernet 0/16	Access	40	60	FECYT Admin.
17	FastEthernet 0/17	Access	40	60	FECYT Admin.
18	FastEthernet 0/18	Access	40	60	FECYT Admin.
19	FastEthernet 0/19	Access	40	60	FECYT Admin.
20	FastEthernet 0/20	Access	40	60	FECYT Admin.
21	FastEthernet 0/21	Access	2	6	AP - UTN
22	FastEthernet 0/22	Access	2	6	AP - UTN
23	FastEthernet 0/23	Access	2	6	AP - UTN
24	FastEthernet 0/24	Access	2	6	AP - UTN
25	GigabitEthernet 0/1	Trunk	-	-	FECYT principal 01
26	**GigabitEthernet 0/2**	**Access**	**1**	**1**	**Libre**

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Laboratorio I

En el Laboratorio I hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 118 se muestra la descripción de las interfaces de dicho Switch.

TABLA 119.- *Descripción de las interfaces del Switch del Laboratorio I de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL LABORATORIO I DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	42	56	FECYT Laboratorios
2	FastEthernet 0/2	Access	42	56	FECYT Laboratorios
3	FastEthernet 0/3	Access	42	56	FECYT Laboratorios
4	FastEthernet 0/4	Access	42	56	FECYT Laboratorios
5	FastEthernet 0/5	Access	42	56	FECYT Laboratorios
6	FastEthernet 0/6	Access	42	56	FECYT Laboratorios
7	FastEthernet 0/7	Access	42	56	FECYT Laboratorios
8	FastEthernet 0/8	Access	42	56	FECYT Laboratorios
9	FastEthernet 0/9	Access	42	56	FECYT Laboratorios
10	FastEthernet 0/10	Access	42	56	FECYT Laboratorios
11	FastEthernet 0/11	Access	42	56	FECYT Laboratorios
12	FastEthernet 0/12	Access	42	56	FECYT Laboratorios
13	FastEthernet 0/13	Access	42	56	FECYT Laboratorios
14	FastEthernet 0/14	Access	42	56	FECYT Laboratorios
15	FastEthernet 0/15	Access	42	56	FECYT Laboratorios
16	FastEthernet 0/16	Access	42	56	FECYT Laboratorios
17	FastEthernet 0/17	Access	42	56	FECYT Laboratorios
18	FastEthernet 0/18	Access	42	56	FECYT Laboratorios
19	FastEthernet 0/19	Access	42	56	FECYT Laboratorios
20	FastEthernet 0/20	Access	42	56	FECYT Laboratorios
21	FastEthernet 0/21	Access	42	56	FECYT Laboratorios
22	FastEthernet 0/22	Access	42	56	FECYT Laboratorios
23	FastEthernet 0/23	Access	42	56	FECYT Laboratorios
24	FastEthernet 0/24	Access	42	56	FECYT Laboratorios
25	FastEthernet 0/25	Access	42	56	FECYT Laboratorios
26	FastEthernet 0/26	Access	42	56	FECYT Laboratorios
27	FastEthernet 0/27	Access	42	56	FECYT Laboratorios
28	FastEthernet 0/28	Access	42	56	FECYT Laboratorios
29	FastEthernet 0/29	Access	42	56	FECYT Laboratorios
30	FastEthernet 0/30	Access	42	56	FECYT Laboratorios

31	FastEthernet 0/31	Access	42	56	FECYT Laboratorios
32	FastEthernet 0/32	Access	42	56	FECYT Laboratorios
33	FastEthernet 0/33	Access	42	56	FECYT Laboratorios
34	FastEthernet 0/34	Access	42	56	FECYT Laboratorios
35	FastEthernet 0/35	Access	42	56	FECYT Laboratorios
36	FastEthernet 0/36	Access	42	56	FECYT Laboratorios
37	FastEthernet 0/37	Access	42	56	FECYT Laboratorios
38	FastEthernet 0/38	Access	42	56	FECYT Laboratorios
39	FastEthernet 0/39	Access	42	56	FECYT Laboratorios
40	FastEthernet 0/40	Access	42	56	FECYT Laboratorios
41	FastEthernet 0/41	Access	42	56	FECYT Laboratorios
42	FastEthernet 0/42	Access	42	56	FECYT Laboratorios
43	FastEthernet 0/43	Access	42	56	FECYT Laboratorios
44	FastEthernet 0/44	Access	42	56	FECYT Laboratorios
45	FastEthernet 0/45	Access	42	56	FECYT Laboratorios
46	FastEthernet 0/46	Access	42	56	FECYT Laboratorios
47	FastEthernet 0/47	Access	42	56	FECYT Laboratorios
48	FastEthernet 0/48	Access	42	56	FECYT Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	FECYT Rack Prin. 01
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio II**

En el Laboratorio II hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 119 se muestra la descripción de las interfaces de dicho Switch.

TABLA 120.- *Descripción de las interfaces del Switch del Laboratorio II de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL LABORATORIO II DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	42	56	FECYT Laboratorios
2	FastEthernet 0/2	Access	42	56	FECYT Laboratorios
3	FastEthernet 0/3	Access	42	56	FECYT Laboratorios
4	FastEthernet 0/4	Access	42	56	FECYT Laboratorios
5	FastEthernet 0/5	Access	42	56	FECYT Laboratorios

6	FastEthernet 0/6	Access	42	56	FECYT Laboratorios
7	FastEthernet 0/7	Access	42	56	FECYT Laboratorios
8	FastEthernet 0/8	Access	42	56	FECYT Laboratorios
9	FastEthernet 0/9	Access	42	56	FECYT Laboratorios
10	FastEthernet 0/10	Access	42	56	FECYT Laboratorios
11	FastEthernet 0/11	Access	42	56	FECYT Laboratorios
12	FastEthernet 0/12	Access	42	56	FECYT Laboratorios
13	FastEthernet 0/13	Access	42	56	FECYT Laboratorios
14	FastEthernet 0/14	Access	42	56	FECYT Laboratorios
15	FastEthernet 0/15	Access	42	56	FECYT Laboratorios
16	FastEthernet 0/16	Access	42	56	FECYT Laboratorios
17	FastEthernet 0/17	Access	42	56	FECYT Laboratorios
18	FastEthernet 0/18	Access	42	56	FECYT Laboratorios
19	FastEthernet 0/19	Access	42	56	FECYT Laboratorios
20	FastEthernet 0/20	Access	42	56	FECYT Laboratorios
21	FastEthernet 0/21	Access	42	56	FECYT Laboratorios
22	FastEthernet 0/22	Access	42	56	FECYT Laboratorios
23	FastEthernet 0/23	Access	42	56	FECYT Laboratorios
24	FastEthernet 0/24	Access	42	56	FECYT Laboratorios
25	FastEthernet 0/25	Access	42	56	FECYT Laboratorios
26	FastEthernet 0/26	Access	42	56	FECYT Laboratorios
27	FastEthernet 0/27	Access	42	56	FECYT Laboratorios
28	FastEthernet 0/28	Access	42	56	FECYT Laboratorios
29	FastEthernet 0/29	Access	42	56	FECYT Laboratorios
30	FastEthernet 0/30	Access	42	56	FECYT Laboratorios
31	FastEthernet 0/31	Access	42	56	FECYT Laboratorios
32	FastEthernet 0/32	Access	42	56	FECYT Laboratorios
33	FastEthernet 0/33	Access	42	56	FECYT Laboratorios
34	FastEthernet 0/34	Access	42	56	FECYT Laboratorios
35	FastEthernet 0/35	Access	42	56	FECYT Laboratorios
36	FastEthernet 0/36	Access	42	56	FECYT Laboratorios
37	FastEthernet 0/37	Access	42	56	FECYT Laboratorios
38	FastEthernet 0/38	Access	42	56	FECYT Laboratorios
39	FastEthernet 0/39	Access	42	56	FECYT Laboratorios
40	FastEthernet 0/40	Access	42	56	FECYT Laboratorios

41	FastEthernet 0/41	Access	42	56	FECYT Laboratorios
42	FastEthernet 0/42	Access	42	56	FECYT Laboratorios
43	FastEthernet 0/43	Access	42	56	FECYT Laboratorios
44	FastEthernet 0/44	Access	42	56	FECYT Laboratorios
45	FastEthernet 0/45	Access	42	56	FECYT Laboratorios
46	FastEthernet 0/46	Access	42	56	FECYT Laboratorios
47	FastEthernet 0/47	Access	42	56	FECYT Laboratorios
48	FastEthernet 0/48	Access	42	56	FECYT Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	FECYT Rack Prin. 01
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio MAC**

En el Laboratorio MAC hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 120 se muestra la descripción de las interfaces de dicho Switch.

TABLA 121.- *Descripción de las interfaces del Switch del Laboratorio MAC de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL LABORATORIO MAC DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	42	56	FECYT Laboratorios
2	FastEthernet 0/2	Access	42	56	FECYT Laboratorios
3	FastEthernet 0/3	Access	42	56	FECYT Laboratorios
4	FastEthernet 0/4	Access	42	56	FECYT Laboratorios
5	FastEthernet 0/5	Access	42	56	FECYT Laboratorios
6	FastEthernet 0/6	Access	42	56	FECYT Laboratorios
7	FastEthernet 0/7	Access	42	56	FECYT Laboratorios
8	FastEthernet 0/8	Access	42	56	FECYT Laboratorios
9	FastEthernet 0/9	Access	42	56	FECYT Laboratorios
10	FastEthernet 0/10	Access	42	56	FECYT Laboratorios
11	FastEthernet 0/11	Access	42	56	FECYT Laboratorios
12	FastEthernet 0/12	Access	42	56	FECYT Laboratorios
13	FastEthernet 0/13	Access	42	56	FECYT Laboratorios
14	FastEthernet 0/14	Access	42	56	FECYT Laboratorios
15	FastEthernet 0/15	Access	42	56	FECYT Laboratorios
16	FastEthernet 0/16	Access	42	56	FECYT Laboratorios

17	FastEthernet 0/17	Access	42	56	FECYT Laboratorios
18	FastEthernet 0/18	Access	42	56	FECYT Laboratorios
19	FastEthernet 0/19	Access	42	56	FECYT Laboratorios
20	FastEthernet 0/20	Access	42	56	FECYT Laboratorios
21	FastEthernet 0/21	Access	42	56	FECYT Laboratorios
22	FastEthernet 0/22	Access	42	56	FECYT Laboratorios
23	FastEthernet 0/23	Access	42	56	FECYT Laboratorios
24	FastEthernet 0/24	Access	42	56	FECYT Laboratorios
25	FastEthernet 0/25	Access	42	56	FECYT Laboratorios
26	FastEthernet 0/26	Access	42	56	FECYT Laboratorios
27	FastEthernet 0/27	Access	42	56	FECYT Laboratorios
28	FastEthernet 0/28	Access	42	56	FECYT Laboratorios
29	FastEthernet 0/29	Access	42	56	FECYT Laboratorios
30	FastEthernet 0/30	Access	42	56	FECYT Laboratorios
31	FastEthernet 0/31	Access	42	56	FECYT Laboratorios
32	FastEthernet 0/32	Access	42	56	FECYT Laboratorios
33	FastEthernet 0/33	Access	42	56	FECYT Laboratorios
34	FastEthernet 0/34	Access	42	56	FECYT Laboratorios
35	FastEthernet 0/35	Access	42	56	FECYT Laboratorios
36	FastEthernet 0/36	Access	42	56	FECYT Laboratorios
37	FastEthernet 0/37	Access	42	56	FECYT Laboratorios
38	FastEthernet 0/38	Access	42	56	FECYT Laboratorios
39	FastEthernet 0/39	Access	42	56	FECYT Laboratorios
40	FastEthernet 0/40	Access	42	56	FECYT Laboratorios
41	FastEthernet 0/41	Access	42	56	FECYT Laboratorios
42	FastEthernet 0/42	Access	42	56	FECYT Laboratorios
43	FastEthernet 0/43	Access	42	56	FECYT Laboratorios
44	FastEthernet 0/44	Access	42	56	FECYT Laboratorios
45	FastEthernet 0/45	Access	42	56	FECYT Laboratorios
46	FastEthernet 0/46	Access	42	56	FECYT Laboratorios
47	FastEthernet 0/47	Access	42	56	FECYT Laboratorios
48	FastEthernet 0/48	Access	42	56	FECYT Laboratorios
49	GigabitEthernet 0/1	Trunk	-	-	FECYT Rack Prin. 01
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Coordinaciones de Carrera**

En la Oficina de Coordinación de Carreras hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 121 se muestra la descripción de las interfaces de dicho Switch.

TABLA 122.- *Descripción de las interfaces del Switch de la Coordinación de Carreras de la FECYT*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA COORDINACIÓN DE CARRERAS DE LA FECYT					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	40	60	FECYT Admin.
2	FastEthernet 0/2	Access	40	60	FECYT Admin.
3	FastEthernet 0/3	Access	40	60	FECYT Admin.
4	FastEthernet 0/4	Access	40	60	FECYT Admin.
5	FastEthernet 0/5	Access	40	60	FECYT Admin.
6	FastEthernet 0/6	Access	40	60	FECYT Admin.
7	FastEthernet 0/7	Access	40	60	FECYT Admin.
8	FastEthernet 0/8	Access	40	60	FECYT Admin.
9	FastEthernet 0/9	Access	40	60	FECYT Admin.
10	FastEthernet 0/10	Access	40	60	FECYT Admin.
11	FastEthernet 0/11	Access	40	60	FECYT Admin.
12	FastEthernet 0/12	Access	40	60	FECYT Admin.
13	FastEthernet 0/13	Access	40	60	FECYT Admin.
14	FastEthernet 0/14	Access	40	60	FECYT Admin.
15	FastEthernet 0/15	Access	40	60	FECYT Admin.
16	FastEthernet 0/16	Access	40	60	FECYT Admin.
17	FastEthernet 0/17	Access	40	60	FECYT Admin.
18	FastEthernet 0/18	Access	40	60	FECYT Admin.
19	FastEthernet 0/19	Access	40	60	FECYT Admin.
20	FastEthernet 0/20	Access	40	60	FECYT Admin.
21	FastEthernet 0/21	Access	40	60	FECYT Admin.
22	FastEthernet 0/22	Access	40	60	FECYT Admin.
23	FastEthernet 0/23	Access	40	60	FECYT Admin.
24	FastEthernet 0/24	Access	40	60	FECYT Admin.
25	GigabitEthernet 0/1	Trunk	-	-	FECYT principal 01
26	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Instituto de Educación física**

En el Instituto de Educación Física hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 122 se muestra la descripción de las interfaces de dicho Switch.

TABLA 123.- *Descripción de las interfaces del Switch del Instituto de Educación Física*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH D EL INSTITUTO DE EDUCACIÓN FÍSICA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	40	60	FECYT Admin.
2	GigabitEthernet 0/2	Access	40	60	FECYT Admin.
3	GigabitEthernet 0/3	Access	40	60	FECYT Admin.
4	GigabitEthernet 0/4	Access	40	60	FECYT Admin.
5	GigabitEthernet 0/5	Access	40	60	FECYT Admin.
6	GigabitEthernet 0/6	Access	40	60	FECYT Admin.
7	GigabitEthernet 0/7	Access	40	60	FECYT Admin.
8	GigabitEthernet 0/8	Access	40	60	FECYT Admin.
9	GigabitEthernet 0/9	Access	40	60	FECYT Admin.
10	GigabitEthernet 0/10	Access	40	60	FECYT Admin.
11	GigabitEthernet 0/11	Access	40	60	FECYT Admin.
12	GigabitEthernet 0/12	Access	40	60	FECYT Admin.
13	GigabitEthernet 0/13	Access	40	60	FECYT Admin.
14	GigabitEthernet 0/14	Access	40	60	FECYT Admin.
15	GigabitEthernet 0/15	Access	40	60	FECYT Admin.
16	GigabitEthernet 0/16	Access	40	60	FECYT Admin.
17	GigabitEthernet 0/17	Access	40	60	FECYT Admin.
18	GigabitEthernet 0/18	Access	40	60	FECYT Admin.
19	GigabitEthernet 0/19	Access	40	60	FECYT Admin.
20	GigabitEthernet 0/20	Access	40	60	FECYT Admin.
21	GigabitEthernet 0/21	Access	40	60	FECYT Admin.
22	GigabitEthernet 0/22	Access	40	60	FECYT Admin.
23	GigabitEthernet 0/23	Access	2	2	AP - UTN
24	GigabitEthernet 0/24	Access	2	2	AP - UTN
25	GigabitEthernet 0/25	Trunk	-	-	FECYT-Principal
26	GigabitEthernet 0/26	Trunk	-	-	FECYT-Piscina

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **Piscina Semi-Olímpica UTN**

En la Piscina Semi-Olímpica de la Universidad hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 123 se muestra la descripción de las interfaces de dicho Switch.

TABLA 124.- *Descripción de las interfaces del Switch de la Piscina Semi-Olímpica UTN*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DE LA PISCINA SEMI OLÍMPICA UTN					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Access	10	20	Ed. Central Admin
2	FastEthernet 1/2	Access	10	20	Ed. Central Admin
3	FastEthernet 1/3	Access	10	20	Ed. Central Admin
4	FastEthernet 1/4	Access	10	20	Ed. Central Admin
5	FastEthernet 1/5	Access	10	20	Ed. Central Admin
6	FastEthernet 1/6	Access	10	20	Ed. Central Admin
7	FastEthernet 1/7	Access	10	20	Ed. Central Admin
8	FastEthernet 1/8	Access	10	20	Ed. Central Admin
9	FastEthernet 1/9	Access	10	20	Ed. Central Admin
10	FastEthernet 1/10	Access	10	20	Ed. Central Admin
11	FastEthernet 1/11	Access	10	20	Ed. Central Admin
12	FastEthernet 1/12	Access	10	20	Ed. Central Admin
13	FastEthernet 1/13	Access	10	20	Ed. Central Admin
14	FastEthernet 1/14	Access	10	20	Ed. Central Admin
15	FastEthernet 1/15	Access	10	20	Ed. Central Admin
16	FastEthernet 1/16	Access	10	20	Ed. Central Admin
17	FastEthernet 1/17	Access	10	20	Ed. Central Admin
18	FastEthernet 1/18	Access	10	20	Ed. Central Admin
19	FastEthernet 1/19	Access	10	20	Ed. Central Admin
20	FastEthernet 1/20	Access	10	20	Ed. Central Admin
21	FastEthernet 1/21	Access	10	20	Ed. Central Admin
22	FastEthernet 1/22	Access	10	20	Ed. Central Admin
23	FastEthernet 1/23	Access	2	6	AP - UTN
24	FastEthernet 1/24	Access	2	6	AP - UTN
25	GigabitEthernet 1/25	Trunk	-	-	-

26	GigabitEthernet 1/26	Trunk	-	-	-
27	GigabitEthernet 1/27	Trunk			-
28	GigabitEthernet 1/28	Trunk	-	-	-

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red de la FACAE

En la Facultad de Ciencias Administrativas y Económicas existen dos Racks en el cuarto de equipos y en el Laboratorio IV.

- **Cuarto de Equipos**

En el cuarto de equipos de la Facultad de Ciencias Administrativas y Económicas existen varios Switchs de Acceso, y la descripción de cada una de las interfaces de los mismos se muestran en las Tablas 124, 125, 126, 127, 128, y 129.

TABLA 125*.- Descripción de las interfaces del Switch 01 del cuarto de equipos de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL CUARTO DE EQUIPOS DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Trunk	-	-	
2	FastEthernet 1/2	Trunk	-	-	
3	FastEthernet 1/3	Trunk	-	-	
4	FastEthernet 1/4	Trunk	-	-	
5	FastEthernet 1/5	Access	2	6	AP – UTN
6	FastEthernet 1/6	Access	44	68	FACAE Admin.
7	FastEthernet 1/7	Access	44	68	FACAE Admin.
8	FastEthernet 1/8	Access	44	68	FACAE Admin.
9	FastEthernet 1/9	Access	44	68	FACAE Admin.
10	FastEthernet 1/10	Access	44	68	FACAE Admin.
11	FastEthernet 1/11	Access	44	68	FACAE Admin.
12	FastEthernet 1/12	Access	44	68	FACAE Admin.
13	FastEthernet 1/13	Access	44	68	FACAE Admin.
14	FastEthernet 1/14	Access	44	68	FACAE Admin.
15	FastEthernet 1/15	Access	44	68	FACAE Admin.

16	FastEthernet 1/16	Access	44	68	FACAE Admin.
17	FastEthernet 1/17	Access	44	68	FACAE Admin.
18	FastEthernet 1/18	Access	44	68	FACAE Admin.
19	FastEthernet 1/19	Access	44	68	FACAE Admin.
20	FastEthernet 1/20	Access	44	68	FACAE Admin.
21	FastEthernet 1/21	Access	44	68	FACAE Admin.
22	FastEthernet 1/22	Access	44	68	FACAE Admin.
23	FastEthernet 1/23	Access	2	2	AP - UTN
24	FastEthernet 1/24	Access	2	2	AP - UTN
25	GigabitEthernet 1/25	Trunk	-	-	-
26	GigabitEthernet 1/26	Trunk	-	-	-

Tabla 126.- *Descripción de las interfaces del Switch 02 del cuarto de equipos de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL CUARTO DE EQUIPOS DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Trunk	-	-	
2	FastEthernet 1/2	Access	44	68	FACAE Admin.
3	FastEthernet 1/3	Access	44	68	FACAE Admin.
4	FastEthernet 1/4	Access	44	68	FACAE Admin.
5	FastEthernet 1/5	Access	44	68	FACAE Admin.
6	FastEthernet 1/6	Access	44	68	FACAE Admin.
7	FastEthernet 1/7	Access	44	68	FACAE Admin.
8	FastEthernet 1/8	Access	44	68	FACAE Admin.
9	FastEthernet 1/9	Access	44	68	FACAE Admin.
10	FastEthernet 1/10	Access	44	68	FACAE Admin.
11	FastEthernet 1/11	Access	44	68	FACAE Admin.
12	FastEthernet 1/12	Access	44	68	FACAE Admin.
13	FastEthernet 1/13	Access	44	68	FACAE Admin.
14	FastEthernet 1/14	Access	44	68	FACAE Admin.
15	FastEthernet 1/15	Access	44	68	FACAE Admin.
16	FastEthernet 1/16	Access	44	68	FACAE Admin.
17	FastEthernet 1/17	Access	44	68	FACAE Admin.

18	FastEthernet 1/18	Access	44	68	FACAE Admin.
19	FastEthernet 1/19	Access	44	68	FACAE Admin.
20	FastEthernet 1/20	Access	44	68	FACAE Admin.
21	FastEthernet 1/21	Access	44	68	FACAE Admin.
22	FastEthernet 1/22	Access	44	68	FACAE Admin.
23	FastEthernet 1/23	Access	44	68	FACAE Admin.
24	FastEthernet 1/24	Access	44	68	FACAE Admin.

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 127.- *Descripción de las interfaces del Switch 03 del cuarto de equipos de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL CUARTO DE EQUIPOS DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Trunk	-	-	
2	FastEthernet 1/2	Access	44	68	FACAE Admin.
3	FastEthernet 1/3	Access	44	68	FACAE Admin.
4	FastEthernet 1/4	Access	44	68	FACAE Admin.
5	FastEthernet 1/5	Access	44	68	FACAE Admin.
6	FastEthernet 1/6	Access	44	68	FACAE Admin.
7	FastEthernet 1/7	Access	44	68	FACAE Admin.
8	FastEthernet 1/8	Access	2	6	AP - UTN
9	FastEthernet 1/9	Access	2	6	AP - UTN
10	FastEthernet 1/10	Access	2	6	AP - UTN
11	FastEthernet 1/11	Access	2	6	AP - UTN
12	FastEthernet 1/12	Access	2	6	AP - UTN
13	FastEthernet 1/13	Access	44	68	FACAE Admin.
14	FastEthernet 1/14	Access	44	68	FACAE Admin.
15	FastEthernet 1/15	Access	44	68	FACAE Admin.
16	FastEthernet 1/16	Access	44	68	FACAE Admin.
17	FastEthernet 1/17	Access	44	68	FACAE Admin.
18	FastEthernet 1/18	Access	44	68	FACAE Admin.
19	FastEthernet 1/19	Access	44	68	FACAE Admin.

20	FastEthernet 1/20	Access	44	68	FACAE Admin.
21	FastEthernet 1/21	Access	44	68	FACAE Admin.
22	FastEthernet 1/22	Access	44	68	FACAE Admin.
23	FastEthernet 1/23	Access	44	68	FACAE Admin.
24	FastEthernet 1/24	Access	44	68	FACAE Admin.

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 128.- *Descripción de las interfaces de un Switch 04 del cuarto de equipos de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 04 DEL CUARTO DE EQUIPOS DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1/0/1	Trunk	-	-	-
2	GigabitEthernet 1/0/2	Access	44	68	FACAE Admin.
3	GigabitEthernet 1/0/3	Access	44	68	FACAE Admin.
4	GigabitEthernet 1/0/4	Access	44	68	FACAE Admin.
5	GigabitEthernet 1/0/5	Access	44	68	FACAE Admin.
6	GigabitEthernet 1/0/6	Access	44	68	FACAE Admin.
7	GigabitEthernet 1/0/7	Access	44	68	FACAE Admin.
8	GigabitEthernet 1/0/8	Access	44	68	FACAE Admin.
9	GigabitEthernet 1/0/9	Access	44	68	FACAE Admin.
10	GigabitEthernet 1/0/10	Access	44	68	FACAE Admin
11	GigabitEthernet 1/0/11	Access	44	68	FACAE Admin
12	GigabitEthernet 1/0/12	Access	44	68	FACAE Admin.
13	GigabitEthernet 1/0/13	Access	44	68	FACAE Admin.
14	GigabitEthernet 1/0/14	Access	44	68	FACAE Admin.
15	GigabitEthernet 1/0/15	Access	44	68	FACAE Admin.
16	GigabitEthernet 1/0/16	Access	44	68	FACAE Admin.
17	GigabitEthernet 1/0/17	Access	44	68	FACAE Admin.
18	GigabitEthernet 1/0/18	Access	44	68	FACAE Admin.
19	GigabitEthernet 1/0/19	Access	44	68	FACAE Admin.
20	GigabitEthernet 1/0/20	Access	44	68	FACAE Admin.
21	GigabitEthernet 1/0/21	Access	44	68	FACAE Admin.
22	GigabitEthernet 1/0/22	Access	44	68	FACAE Admin.

23	GigabitEthernet 1/0/23	Access	44	68	FACAE Admin.
24	GigabitEthernet 1/0/24	Access	44	68	FACAE Admin.
25	GigabitEthernet 1/0/25	Access	44	68	FACAE Admin.
26	GigabitEthernet 1/0/26	Access	44	68	FACAE Admin.
27	GigabitEthernet 1/0/27	Access	44	68	FACAE Admin.
28	GigabitEthernet 1/0/28	Access	44	68	FACAE Admin.
29	GigabitEthernet 1/0/29	Access	44	68	FACAE Admin.
30	GigabitEthernet 1/0/30	Access	44	68	FACAE Admin.
31	GigabitEthernet 1/0/31	Access	44	68	FACAE Admin.
32	GigabitEthernet 1/0/32	Access	44	68	FACAE Admin.
33	GigabitEthernet 1/0/33	Access	44	68	FACAE Admin.
34	GigabitEthernet 1/0/34	Access	44	68	FACAE Admin.
35	GigabitEthernet 1/0/35	Access	44	68	FACAE Admin.
36	GigabitEthernet 1/0/36	Access	44	68	FACAE Admin.
37	GigabitEthernet 1/0/37	Access	44	68	FACAE Admin.
38	GigabitEthernet 1/0/38	Access	44	68	FACAE Admin.
39	GigabitEthernet 1/0/39	Access	44	68	FACAE Admin.
40	GigabitEthernet 1/0/40	Access	44	68	FACAE Admin.
41	GigabitEthernet 1/0/41	Access	44	68	FACAE Admin.
42	GigabitEthernet 1/0/42	Access	44	68	FACAE Admin.
43	GigabitEthernet 1/0/43	Access	44	68	FACAE Admin.
44	GigabitEthernet 1/0/44	Access	44	68	FACAE Admin.
45	GigabitEthernet 1/0/45	Access	44	68	FACAE Admin.
46	GigabitEthernet 1/0/46	Access	44	68	FACAE Admin.
47	GigabitEthernet 1/0/47	Access	44	68	FACAE Admin.
48	GigabitEthernet 1/0/48	Access	44	68	FACAE Admin.

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 129.- *Descripción de las interfaces de un Switch 05 del Cuarto de Equipos de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 05 DEL CUARTO DE EQUIPOS DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	44	68	FACAE Admin.
2	GigabitEthernet 2	Access	44	68	FACAE Admin.
3	GigabitEthernet 3	Access	44	68	FACAE Admin.
4	GigabitEthernet 4	Access	44	68	FACAE Admin.
5	GigabitEthernet 5	Access	44	68	FACAE Admin.
6	GigabitEthernet 6	Access	44	68	FACAE Admin.
7	GigabitEthernet 7	Access	44	68	FACAE Admin.
8	GigabitEthernet 8	Access	44	68	FACAE Admin.
9	GigabitEthernet 9	Access	44	68	FACAE Admin.
10	GigabitEthernet 10	Access	44	68	FACAE Admin
11	GigabitEthernet 11	Access	44	68	FACAE Admin
12	GigabitEthernet 12	Access	44	68	FACAE Admin.
13	GigabitEthernet 13	Access	44	68	FACAE Admin.
14	GigabitEthernet 14	Access	44	68	FACAE Admin.
15	GigabitEthernet 15	Access	44	68	FACAE Admin.
16	GigabitEthernet 16	Access	44	68	FACAE Admin.
17	GigabitEthernet 17	Access	44	68	FACAE Admin.
18	GigabitEthernet 18	Access	44	68	FACAE Admin.
19	GigabitEthernet 19	Access	44	68	FACAE Admin.
20	GigabitEthernet 20	Access	44	68	FACAE Admin.
21	GigabitEthernet 21	Access	44	68	FACAE Admin.
22	GigabitEthernet 22	Access	44	68	FACAE Admin.
23	GigabitEthernet 23	Trunk	-	-	
24	GigabitEthernet 24	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Tabla 130.- *Descripción de las interfaces de un Switch 06 del Cuarto de Equipos de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 06 DEL CUARTO DE EQUIPOS DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	44	68	FACAE Admin.
2	GigabitEthernet 2	Access	44	68	FACAE Admin.
3	GigabitEthernet 3	Access	44	68	FACAE Admin.
4	GigabitEthernet 4	Access	44	68	FACAE Admin.
5	GigabitEthernet 5	Access	44	68	FACAE Admin.
6	GigabitEthernet 6	Access	44	68	FACAE Admin.
7	GigabitEthernet 7	Access	44	68	FACAE Admin.
8	GigabitEthernet 8	Access	44	68	FACAE Admin.
9	GigabitEthernet 9	Access	44	68	FACAE Admin.
10	GigabitEthernet 10	Access	44	68	FACAE Admin
11	GigabitEthernet 11	Access	44	68	FACAE Admin
12	GigabitEthernet 12	Access	44	68	FACAE Admin.
13	GigabitEthernet 13	Access	44	68	FACAE Admin.
14	GigabitEthernet 14	Access	44	68	FACAE Admin.
15	GigabitEthernet 15	Access	44	68	FACAE Admin.
16	GigabitEthernet 16	Access	44	68	FACAE Admin.
17	GigabitEthernet 17	Access	44	68	FACAE Admin.
18	GigabitEthernet 18	Access	44	68	FACAE Admin.
19	GigabitEthernet 19	Access	44	68	FACAE Admin.
20	GigabitEthernet 20	Access	44	68	FACAE Admin.
21	GigabitEthernet 21	Access	44	68	FACAE Admin.
22	GigabitEthernet 22	Access	44	68	FACAE Admin.
23	GigabitEthernet 23	Access	44	68	FACAE Admin.
24	GigabitEthernet 24	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Laboratorio IV**

En el Laboratorio IV hay un Switch de acceso para todos los equipos que existen en el mismo, en la Tabla 130 se muestra la descripción de las interfaces de dicho Switch.

TABLA 131.- *Descripción de las interfaces de un Switch del Laboratorio IV de la FACAE*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL LABORATORIO IV DE LA FACAE					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	44	68	FACAE Admin
2	GigabitEthernet 0/2	Access	44	68	FACAE Admin
3	GigabitEthernet 0/3	Access	44	68	FACAE Admin
4	GigabitEthernet 0/4	Access	44	68	FACAE Admin
5	GigabitEthernet 0/5	Access	44	68	FACAE Admin
6	GigabitEthernet 0/6	Access	44	68	FACAE Admin
7	GigabitEthernet 0/7	Access	44	68	FACAE Admin
8	GigabitEthernet 0/8	Access	44	68	FACAE Admin
9	GigabitEthernet 0/9	Access	44	68	FACAE Admin
10	GigabitEthernet 0/10	Access	44	68	FACAE Admin
11	GigabitEthernet 0/11	Access	44	68	FACAE Admin
12	GigabitEthernet 0/12	Access	44	68	FACAE Admin
13	GigabitEthernet 0/13	Access	44	68	FACAE Admin
14	GigabitEthernet 0/14	Access	44	68	FACAE Admin
15	GigabitEthernet 0/15	Access	44	68	FACAE Admin
16	GigabitEthernet 0/16	Access	44	68	FACAE Admin
17	GigabitEthernet 0/17	Access	44	68	FACAE Admin
18	GigabitEthernet 0/18	Access	44	68	FACAE Admin
19	GigabitEthernet 0/19	Access	44	68	FACAE Admin
20	GigabitEthernet 0/20	Access	44	68	FACAE Admin
21	GigabitEthernet 0/21	Access	44	68	FACAE Admin
22	GigabitEthernet 0/22	Access	44	68	FACAE Admin
23	GigabitEthernet 0/23	Access	44	68	FACAE Admin
24	GigabitEthernet 0/24	Access	44	68	FACAE Admin
25	GigabitEthernet 0/25	Access	44	68	FACAE Admin
26	GigabitEthernet 0/26	Access	44	68	FACAE Admin
27	GigabitEthernet 0/27	Access	44	68	FACAE Admin

28	GigabitEthernet 0/28	Access	44	68	FACAE Admin
29	GigabitEthernet 0/29	Access	44	68	FACAE Admin
30	GigabitEthernet 0/30	Access	44	68	FACAE Admin
31	GigabitEthernet 0/31	Access	44	68	FACAE Admin
32	GigabitEthernet 0/32	Access	44	68	FACAE Admin
33	GigabitEthernet 0/33	Access	44	68	FACAE Admin
34	GigabitEthernet 0/34	Access	44	68	FACAE Admin
35	GigabitEthernet 0/35	Access	44	68	FACAE Admin
36	GigabitEthernet 0/36	Access	44	68	FACAE Admin
37	GigabitEthernet 0/37	Access	44	68	FACAE Admin
38	GigabitEthernet 0/38	Access	44	68	FACAE Admin
39	GigabitEthernet 0/39	Access	44	68	FACAE Admin
40	GigabitEthernet 0/40	Access	44	68	FACAE Admin
41	GigabitEthernet 0/41	Access	44	68	FACAE Admin
42	GigabitEthernet 0/42	Access	44	68	FACAE Admin
43	GigabitEthernet 0/43	Access	44	68	FACAE Admin
44	GigabitEthernet 0/44	Trunk	-	-	Enlace Rack FACAE
45	GigabitEthernet 0/45	Access	44	68	FACAE Admin
46	GigabitEthernet 0/46	Access	44	68	FACAE Admin
47	GigabitEthernet 0/47	Access	44	68	FACAE Admin
48	GigabitEthernet 0/48	Access	44	68	FACAE Admin

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red de la FCCSS

En la Facultad de Ciencias de la Salud existen varios Switchs en un solo rack, además de los Switchs que existen en el Antiguo Hospital San Vicente de Paúl

- **Cuarto de equipos**

En el cuarto de equipos de la Facultad de Ciencias de la Salud existen dos Switchs de Acceso, y la descripción de cada una de las interfaces de los mismos se muestran en la Tabla 131.

TABLA 132.- *Descripción de las interfaces del Switch 01 del cuarto de equipos de la FCCSS*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL CUARTO DE EQUIPOS DE LA FCCSS					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Trunk	-	-	
2	FastEthernet 1/2	Access	32	76	FCCSS Admin.
3	FastEthernet 1/3	Access	32	76	FCCSS Admin.
4	FastEthernet 1/4	Access	32	76	FCCSS Admin.
5	FastEthernet 1/5	Access	32	76	FCCSS Admin.
6	FastEthernet 1/6	Access	32	76	FCCSS Admin.
7	FastEthernet 1/7	Access	32	76	FCCSS Admin.
8	FastEthernet 1/8	Access	32	76	FCCSS Admin.
9	FastEthernet 1/9	Access	32	76	FCCSS Admin.
10	FastEthernet 1/10	Access	32	76	FCCSS Admin.
11	FastEthernet 1/11	Access	32	76	FCCSS Admin.
12	FastEthernet 1/12	Access	32	76	FCCSS Admin.
13	FastEthernet 1/13	Access	32	76	FCCSS Admin.
14	FastEthernet 1/14	Access	32	76	FCCSS Admin.
15	FastEthernet 1/15	Access	32	76	FCCSS Admin.
16	FastEthernet 1/16	Access	32	76	FCCSS Admin.
17	FastEthernet 1/17	Access	32	76	FCCSS Admin.
18	FastEthernet 1/18	Access	32	76	FCCSS Admin.
19	FastEthernet 1/19	Access	32	76	FCCSS Admin.
20	FastEthernet 1/20	Access	32	76	FCCSS Admin.
21	FastEthernet 1/21	Access	32	76	FCCSS Admin.
22	FastEthernet 1/22	Access	32	76	FCCSS Admin.
23	FastEthernet 1/23	Access	32	76	FCCSS Admin.
24	FastEthernet 1/24	Access	32	76	FCCSS Admin.
25	FastEthernet 1/25	Access	32	76	FCCSS Admin.
26	FastEthernet 1/26	Access	32	76	FCCSS Admin.
27	FastEthernet 1/27	Access	32	76	FCCSS Admin.
28	FastEthernet 1/28	Access	32	76	FCCSS Admin.
29	FastEthernet 1/29	Access	32	76	FCCSS Admin.
30	FastEthernet 1/30	Access	32	76	FCCSS Admin.

31	FastEthernet 1/31	Access	32	76	FCCSS Admin.
32	FastEthernet 1/32	Access	32	76	FCCSS Admin.
33	FastEthernet 1/33	Access	32	76	FCCSS Admin.
34	FastEthernet 1/34	Access	32	76	FCCSS Admin.
35	FastEthernet 1/35	Access	32	76	FCCSS Admin.
36	FastEthernet 1/36	Access	32	76	FCCSS Admin.
37	FastEthernet 1/37	Access	32	76	FCCSS Admin.
38	FastEthernet 1/38	Access	32	76	FCCSS Admin.
39	FastEthernet 1/39	Access	32	76	FCCSS Admin.
40	FastEthernet 1/40	Access	32	76	FCCSS Admin.
41	FastEthernet 1/41	Access	32	76	FCCSS Admin.
42	FastEthernet 1/42	Access	32	76	FCCSS Admin.
43	FastEthernet 1/43	Access	32	76	FCCSS Admin.
44	FastEthernet 1/44	Access	32	76	FCCSS Admin.
45	FastEthernet 1/45	Access	32	76	FCCSS Admin.
46	FastEthernet 1/46	Access	32	76	FCCSS Admin.
47	FastEthernet 1/47	Access	32	76	FCCSS Admin.
48	FastEthernet 1/48	Access	32	76	FCCSS Admin.
49	FastEthernet 1/49	Trunk	-	-	
50	FastEthernet 1/50	Trunk	-	-	

***Fuente**: Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Antiguo Hospital San Vicente de Paúl**

En el Antiguo Hospital San Vicente de Paúl existen dos Switch de los cuales solo uno es administrable. En la Tabla 132, se indica la descripción de las interfaces del Switch configurable.

***TABLA 133.-** Descripción de las interfaces del Switch del Antiguo Hospital San Vicente de Paul*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL ANTIGUO HOSPITAL SAN VICENTE DE PAUL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	32	76	FCCSS Admin.
2	GigabitEthernet 2	Access	32	76	FCCSS Admin.

3	GigabitEthernet 3	Access	32	76	FCCSS Admin.
4	GigabitEthernet 4	Access	32	76	FCCSS Admin.
5	GigabitEthernet 5	Access	32	76	FCCSS Admin.
6	GigabitEthernet 6	Access	32	76	FCCSS Admin.
7	GigabitEthernet 7	Access	32	76	FCCSS Admin.
8	GigabitEthernet 8	Access	32	76	FCCSS Admin.
9	GigabitEthernet 9	Access	32	76	FCCSS Admin.
10	GigabitEthernet 10	Access	32	76	FCCSS Admin.
11	GigabitEthernet 11	Access	32	76	FCCSS Admin.
12	GigabitEthernet 12	Access	32	76	FCCSS Admin.
13	GigabitEthernet 13	Access	32	76	FCCSS Admin.
14	GigabitEthernet 14	Access	32	76	FCCSS Admin.
15	GigabitEthernet 15	Trunk	-	-	
16	GigabitEthernet 16	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red en el Edificio de Postgrado

En el Nuevo edificio de Postgrado existen varios Switch de acceso tanto en el cuarto de equipos como en el tercer piso.

- **Cuarto de Equipos**

En el cuarto de equipos existen tres Switchs de los cuales se indican en las Tablas 133, 134 y 135 la descripción de cada una de las interfaces.

TABLA 134.- *Descripción de las interfaces del Switch 01 del cuarto de equipos del Edificio de Postgrado*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL CUARTO DE EQUIPOS DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	TenGigabitEthernet 1/1	Trunk	-		Enlace
2	TenGigabitEthernet 1/2	Trunk	-		Enlace
3	GigabitEthernet 1/3	Inactive	1	-	-
4	GigabitEthernet 1/4	Inactive	1	-	-
5	GigabitEthernet 1/5	Inactive	1	-	-
6	GigabitEthernet 1/6	Inactive	1	-	-

7	GigabitEthernet 2/1	Access	26	80	Postgrado
8	GigabitEthernet 2/2	Access	26	80	Postgrado
9	GigabitEthernet 2/3	Access	26	80	Postgrado
10	GigabitEthernet 2/4	Access	26	80	Postgrado
11	GigabitEthernet 2/5	Access	26	80	Postgrado
12	GigabitEthernet 2/6	Access	26	80	Postgrado
13	GigabitEthernet 2/7	Access	26	80	Postgrado
14	GigabitEthernet 2/8	Access	26	80	Postgrado
15	GigabitEthernet 2/9	Access	26	80	Postgrado
16	GigabitEthernet 2/10	Access	26	80	Postgrado
17	GigabitEthernet 2/11	Access	26	80	Postgrado
18	GigabitEthernet 2/12	Access	26	80	Postgrado
19	GigabitEthernet 2/13	Access	26	80	Postgrado
20	GigabitEthernet 2/14	Access	26	80	Postgrado
21	GigabitEthernet 2/15	Access	26	80	Postgrado
22	GigabitEthernet 2/16	Access	26	80	Postgrado
23	GigabitEthernet 2/17	Access	26	80	Postgrado
24	GigabitEthernet 2/18	Access	26	80	Postgrado
25	GigabitEthernet 2/19	Access	26	80	Postgrado
26	GigabitEthernet 2/20	Access	26	80	Postgrado
27	GigabitEthernet 2/21	Access	26	80	Postgrado
28	GigabitEthernet 2/22	Access	26	80	Postgrado
29	GigabitEthernet 2/23	Access	26	80	Postgrado
30	GigabitEthernet 2/24	Access	26	80	Postgrado
31	GigabitEthernet 2/25	Access	26	80	Postgrado
32	GigabitEthernet 2/26	Access	26	80	Postgrado
33	GigabitEthernet 2/27	Access	26	80	Postgrado
34	GigabitEthernet 2/28	Access	26	80	Postgrado
35	GigabitEthernet 2/29	Access	26	80	Postgrado
36	GigabitEthernet 2/30	Access	26	80	Postgrado
37	GigabitEthernet 2/31	Access	26	80	Postgrado
38	GigabitEthernet 2/32	Access	26	80	Postgrado
39	GigabitEthernet 2/33	Access	26	80	Postgrado
40	GigabitEthernet 2/34	Access	26	80	Postgrado
41	GigabitEthernet 2/35	Access	26	80	Postgrado

42	GigabitEthernet 2/36	Access	26	80	Postgrado
43	GigabitEthernet 2/37	Access	26	80	Postgrado
44	GigabitEthernet 2/38	Access	26	80	Postgrado
45	GigabitEthernet 2/39	Access	26	80	Postgrado
46	GigabitEthernet 2/40	Access	26	80	Postgrado
47	GigabitEthernet 2/41	Access	26	80	Postgrado
48	GigabitEthernet 2/42	Access	26	80	Postgrado
49	GigabitEthernet 2/43	Access	26	80	Postgrado
50	GigabitEthernet 2/44	Access	2	6	AP - UTN
51	GigabitEthernet 2/45	Access	2	6	AP - UTN
52	GigabitEthernet 2/46	Access	2	6	AP - UTN
53	GigabitEthernet 2/47	Trunk	-	-	Postgrado
54	GigabitEthernet 2/48	Trunk	-	-	Postgrado

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 135.- Descripción de las interfaces del Switch 02 del cuarto de equipos del Edificio de Postgrado

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL CUARTO DE EQUIPOS DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	26	80	Postgrado
2	GigabitEthernet 0/2	Access	26	80	Postgrado
3	GigabitEthernet 0/3	Access	26	80	Postgrado
4	GigabitEthernet 0/4	Access	26	80	Postgrado
5	GigabitEthernet 0/5	Access	26	80	Postgrado
6	GigabitEthernet 0/6	Access	26	80	Postgrado
7	GigabitEthernet 0/7	Access	26	80	Postgrado
8	GigabitEthernet 0/8	Access	26	80	Postgrado
9	GigabitEthernet 0/9	Access	26	80	Postgrado
10	GigabitEthernet 0/10	Access	26	80	Postgrado
11	GigabitEthernet 0/11	Access	121	3	Públicas
12	GigabitEthernet 0/12	Access	26	80	Postgrado
13	GigabitEthernet 0/13	Access	26	80	Postgrado
14	GigabitEthernet 0/14	Access	26	80	Postgrado
15	GigabitEthernet 0/15	Access	26	80	Postgrado
16	GigabitEthernet 0/16	Access	26	80	Postgrado

17	GigabitEthernet 0/17	Access	26	80	Postgrado
18	GigabitEthernet 0/18	Access	26	80	Postgrado
19	GigabitEthernet 0/19	Access	26	80	Postgrado
20	GigabitEthernet 0/20	Access	26	80	Postgrado
21	GigabitEthernet 0/21	Access	26	80	Postgrado
22	GigabitEthernet 0/22	Access	26	80	Postgrado
23	GigabitEthernet 0/23	Access	26	80	Postgrado
24	GigabitEthernet 0/24	Access	26	80	Postgrado
25	GigabitEthernet 0/25	Access	26	80	Postgrado
26	GigabitEthernet 0/26	Access	26	80	Postgrado
27	GigabitEthernet 0/27	Access	26	80	Postgrado
28	GigabitEthernet 0/28	Access	26	80	Postgrado
29	GigabitEthernet 0/29	Access	26	80	Postgrado
30	GigabitEthernet 0/30	Access	26	80	Postgrado
31	GigabitEthernet 0/31	Access	26	80	Postgrado
32	GigabitEthernet 0/32	Access	26	80	Postgrado
33	GigabitEthernet 0/33	Access	26	80	Postgrado
34	GigabitEthernet 0/34	Access	26	80	Postgrado
35	GigabitEthernet 0/35	Access	26	80	Postgrado
36	GigabitEthernet 0/36	Access	26	80	Postgrado
37	GigabitEthernet 0/37	Access	26	80	Postgrado
38	GigabitEthernet 0/38	Access	26	80	Postgrado
39	GigabitEthernet 0/39	Access	26	80	Postgrado
40	GigabitEthernet 0/40	Access	26	80	Postgrado
41	GigabitEthernet 0/41	Access	26	80	Postgrado
42	GigabitEthernet 0/42	Access	26	80	Postgrado
43	GigabitEthernet 0/43	Access	26	80	Postgrado
44	GigabitEthernet 0/44	Access	26	80	Postgrado
45	GigabitEthernet 0/45	Access	26	80	Postgrado
46	GigabitEthernet 0/46	Access	26	80	Postgrado
47	GigabitEthernet 0/47	Access	26	80	Postgrado
48	GigabitEthernet 0/48	Trunk	-	-	Enlace SW-Core
49	GigabitEthernet 0/49	Access	1	1	Libre
50	GigabitEthernet 0/50	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 136.- *Descripción de las interfaces del Switch 03 del cuarto de equipos del Edificio de Postgrado*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL CUARTO DE EQUIPOS DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	26	80	Postgrado
2	GigabitEthernet 0/2	Access	26	80	Postgrado
3	GigabitEthernet 0/3	Access	26	80	Postgrado
4	GigabitEthernet 0/4	Access	26	80	Postgrado
5	GigabitEthernet 0/5	Access	26	80	Postgrado
6	GigabitEthernet 0/6	Access	26	80	Postgrado
7	GigabitEthernet 0/7	Access	26	80	Postgrado
8	GigabitEthernet 0/8	Access	26	80	Postgrado
9	GigabitEthernet 0/9	Access	26	80	Postgrado
10	GigabitEthernet 0/10	Access	26	80	Postgrado
11	GigabitEthernet 0/11	Access	26	80	Postgrado
12	GigabitEthernet 0/12	Access	26	80	Postgrado
13	GigabitEthernet 0/13	Access	26	80	Postgrado
14	GigabitEthernet 0/14	Access	26	80	Postgrado
15	GigabitEthernet 0/15	Access	26	80	Postgrado
16	GigabitEthernet 0/16	Access	26	80	Postgrado
17	GigabitEthernet 0/17	Access	26	80	Postgrado
18	GigabitEthernet 0/18	Access	26	80	Postgrado
19	GigabitEthernet 0/19	Access	26	80	Postgrado
20	GigabitEthernet 0/20	Access	26	80	Postgrado
21	GigabitEthernet 0/21	Access	26	80	Postgrado
22	GigabitEthernet 0/22	Access	26	80	Postgrado
23	GigabitEthernet 0/23	Access	26	80	Postgrado
24	GigabitEthernet 0/24	Access	122	4	DMZ
25	GigabitEthernet 0/25	Access	26	80	Postgrado
26	GigabitEthernet 0/26	Access	26	80	Postgrado
27	GigabitEthernet 0/27	Access	26	80	Postgrado
28	GigabitEthernet 0/28	Access	26	80	Postgrado
29	GigabitEthernet 0/29	Access	26	80	Postgrado
30	GigabitEthernet 0/30	Access	26	80	Postgrado

31	GigabitEthernet 0/31	Access	26	80	Postgrado
32	GigabitEthernet 0/32	Access	26	80	Postgrado
33	GigabitEthernet 0/33	Access	26	80	Postgrado
34	GigabitEthernet 0/34	Access	26	80	Postgrado
35	GigabitEthernet 0/35	Access	26	80	Postgrado
36	GigabitEthernet 0/36	Access	26	80	Postgrado
37	GigabitEthernet 0/37	Access	26	80	Postgrado
38	GigabitEthernet 0/38	Access	26	80	Postgrado
39	GigabitEthernet 0/39	Access	26	80	Postgrado
40	GigabitEthernet 0/40	Access	26	80	Postgrado
41	GigabitEthernet 0/41	Access	26	80	Postgrado
42	GigabitEthernet 0/42	Access	26	80	Postgrado
43	GigabitEthernet 0/43	Access	26	80	Postgrado
44	GigabitEthernet 0/44	Access	26	80	Postgrado
45	GigabitEthernet 0/45	Access	26	80	Postgrado
46	GigabitEthernet 0/46	Access	26	80	Postgrado
47	GigabitEthernet 0/47	Access	26	80	Postgrado
48	GigabitEthernet 0/48	Trunk	-	-	Enlace SW-Core
49	GigabitEthernet 0/49	Access	1	1	Libre
50	GigabitEthernet 0/50	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Segundo Piso**

En la terraza del segundo piso hay un rack donde existe 4 Switchs destinados para el Acceso de los usuarios de Postgrado. En las Tablas 136, 137, 138 y 139 se detallan la configuración de las interfaces de los mismos.

TABLA 137.- *Descripción de las interfaces del Switch 01 del segundo piso del Edificio de Postgrado*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL SEGUNDO PISO DEL EDIFICIO DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1/0/1	Access	26	80	Postgrado
2	GigabitEthernet 1/0/2	Access	26	80	Postgrado
3	GigabitEthernet 1/0/3	Access	26	80	Postgrado

4	GigabitEthernet 1/0/4	Access	26	80	Postgrado
5	GigabitEthernet 1/0/5	Access	26	80	Postgrado
6	GigabitEthernet 1/0/6	Access	26	80	Postgrado
7	GigabitEthernet 1/0/7	Access	26	80	Postgrado
8	GigabitEthernet 1/0/8	Access	26	80	Postgrado
9	GigabitEthernet 1/0/9	Access	26	80	Postgrado
10	GigabitEthernet 1/0/10	Access	26	80	Postgrado
11	GigabitEthernet 1/0/11	Access	26	80	Postgrado
12	GigabitEthernet 1/0/12	Access	26	80	Postgrado
13	GigabitEthernet 1/0/13	Access	26	80	Postgrado
14	GigabitEthernet 1/0/14	Access	26	80	Postgrado
15	GigabitEthernet 1/0/15	Access	26	80	Postgrado
16	GigabitEthernet 1/0/16	Access	26	80	Postgrado
17	GigabitEthernet 1/0/17	Access	26	80	Postgrado
18	GigabitEthernet 1/0/18	Access	26	80	Postgrado
19	GigabitEthernet 1/0/19	Access	26	80	Postgrado
20	GigabitEthernet 1/0/20	Access	26	80	Postgrado
21	GigabitEthernet 1/0/21	Access	26	80	Postgrado
22	GigabitEthernet 1/0/22	Access	26	80	Postgrado
23	GigabitEthernet 1/0/23	Access	26	80	Postgrado
24	GigabitEthernet 1/0/24	Access	122	4	DMZ
25	GigabitEthernet 1/0/25	Access	26	80	Postgrado
26	GigabitEthernet 1/0/26	Access	26	80	Postgrado
27	GigabitEthernet 1/0/27	Access	26	80	Postgrado
28	GigabitEthernet 1/0/28	Access	26	80	Postgrado
29	GigabitEthernet 1/0/29	Access	26	80	Postgrado
30	GigabitEthernet 1/0/30	Access	26	80	Postgrado
31	GigabitEthernet 1/0/31	Access	26	80	Postgrado
32	GigabitEthernet 1/0/32	Access	26	80	Postgrado
33	GigabitEthernet 1/0/33	Access	26	80	Postgrado
34	GigabitEthernet 1/0/34	Access	26	80	Postgrado
35	GigabitEthernet 1/0/35	Access	26	80	Postgrado
36	GigabitEthernet 1/0/36	Access	26	80	Postgrado
37	GigabitEthernet 1/0/37	Access	26	80	Postgrado
38	GigabitEthernet 1/0/38	Access	26	80	Postgrado

39	GigabitEthernet 1/0/39	Access	26	80	Postgrado
40	GigabitEthernet 1/0/40	Access	26	80	Postgrado
41	GigabitEthernet 1/0/41	Access	26	80	Postgrado
42	GigabitEthernet 1/0/42	Access	26	80	Postgrado
43	GigabitEthernet 1/0/43	Access	26	80	Postgrado
44	GigabitEthernet 1/0/44	Access	26	80	Postgrado
45	GigabitEthernet 1/0/45	Access	26	80	Postgrado
46	GigabitEthernet 1/0/46	Access	26	80	Postgrado
47	GigabitEthernet 1/0/47	Trunk	-	-	Post-Rack02
48	GigabitEthernet 1/0/48	Trunk	-	-	Post-Rack02
49	TenGigabitEthernet 1/0/1	Trunk	-	-	Core-Postg.
50	TenGigabitEthernet 1/0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 138.- *Descripción de las interfaces del Switch 02 del segundo piso del Edificio de Postgrado*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL SEGUNDO PISO DEL EDIFICIO DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	26	80	Postgrado
2	GigabitEthernet 0/2	Access	26	80	Postgrado
3	GigabitEthernet 0/3	Access	26	80	Postgrado
4	GigabitEthernet 0/4	Access	26	80	Postgrado
5	GigabitEthernet 0/5	Access	26	80	Postgrado
6	GigabitEthernet 0/6	Access	26	80	Postgrado
7	GigabitEthernet 0/7	Access	26	80	Postgrado
8	GigabitEthernet 0/8	Access	26	80	Postgrado
9	GigabitEthernet 0/9	Access	26	80	Postgrado
10	GigabitEthernet 0/10	Access	26	80	Postgrado
11	GigabitEthernet 0/11	Access	26	80	Postgrado
12	GigabitEthernet 0/12	Access	26	80	Postgrado
13	GigabitEthernet 0/13	Access	26	80	Postgrado
14	GigabitEthernet 0/14	Access	26	80	Postgrado
15	GigabitEthernet 0/15	Access	26	80	Postgrado
16	GigabitEthernet 0/16	Access	26	80	Postgrado

17	GigabitEthernet 0/17	Access	26	80	Postgrado
18	GigabitEthernet 0/18	Access	26	80	Postgrado
19	GigabitEthernet 0/19	Access	26	80	Postgrado
20	GigabitEthernet 0/20	Access	26	80	Postgrado
21	GigabitEthernet 0/21	Access	26	80	Postgrado
22	GigabitEthernet 0/22	Access	26	80	Postgrado
23	GigabitEthernet 0/23	Access	26	80	Postgrado
24	GigabitEthernet 0/24	Access	26	80	Postgrado
25	GigabitEthernet 0/25	Access	26	80	Postgrado
26	GigabitEthernet 0/26	Access	26	80	Postgrado
27	GigabitEthernet 0/27	Access	26	80	Postgrado
28	GigabitEthernet 0/28	Access	26	80	Postgrado
29	GigabitEthernet 0/29	Access	26	80	Postgrado
30	GigabitEthernet 0/30	Access	26	80	Postgrado
31	GigabitEthernet 0/31	Access	26	80	Postgrado
32	GigabitEthernet 0/32	Access	26	80	Postgrado
33	GigabitEthernet 0/33	Access	26	80	Postgrado
34	GigabitEthernet 0/34	Access	26	80	Postgrado
35	GigabitEthernet 0/35	Access	26	80	Postgrado
36	GigabitEthernet 0/36	Access	26	80	Postgrado
37	GigabitEthernet 0/37	Access	26	80	Postgrado
38	GigabitEthernet 0/38	Access	26	80	Postgrado
39	GigabitEthernet 0/39	Access	26	80	Postgrado
40	GigabitEthernet 0/40	Access	26	80	Postgrado
41	GigabitEthernet 0/41	Access	26	80	Postgrado
42	GigabitEthernet 0/42	Access	26	80	Postgrado
43	GigabitEthernet 0/43	Access	26	80	Postgrado
44	GigabitEthernet 0/44	Access	26	80	Postgrado
45	GigabitEthernet 0/45	Access	26	80	Postgrado
46	GigabitEthernet 0/46	Access	26	80	Postgrado
47	GigabitEthernet 0/47	Access	26	80	Postgrado
48	GigabitEthernet 0/48	Trunk	-	-	SW-Postgrado-Rack02
49	GigabitEthernet 0/49	Access	1	1	Libre
50	GigabitEthernet 0/50	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Tabla 138.-*Descripción de las interfaces del Switch 03 del segundo piso del Edificio de Postgrado*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL SEGUNDO PISO DEL EDIFICIO DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	26	80	Postgrado
2	GigabitEthernet 0/2	Access	26	80	Postgrado
3	GigabitEthernet 0/3	Access	26	80	Postgrado
4	GigabitEthernet 0/4	Access	26	80	Postgrado
5	GigabitEthernet 0/5	Access	26	80	Postgrado
6	GigabitEthernet 0/6	Access	26	80	Postgrado
7	GigabitEthernet 0/7	Access	26	80	Postgrado
8	GigabitEthernet 0/8	Access	26	80	Postgrado
9	GigabitEthernet 0/9	Access	26	80	Postgrado
10	GigabitEthernet 0/10	Access	26	80	Postgrado
11	GigabitEthernet 0/11	Access	26	80	Postgrado
12	GigabitEthernet 0/12	Access	26	80	Postgrado
13	GigabitEthernet 0/13	Access	26	80	Postgrado
14	GigabitEthernet 0/14	Access	26	80	Postgrado
15	GigabitEthernet 0/15	Access	26	80	Postgrado
16	GigabitEthernet 0/16	Access	26	80	Postgrado
17	GigabitEthernet 0/17	Access	26	80	Postgrado
18	GigabitEthernet 0/18	Access	26	80	Postgrado
19	GigabitEthernet 0/19	Access	26	80	Postgrado
20	GigabitEthernet 0/20	Access	26	80	Postgrado
21	GigabitEthernet 0/21	Access	26	80	Postgrado
22	GigabitEthernet 0/22	Access	26	80	Postgrado
23	GigabitEthernet 0/23	Access	26	80	Postgrado
24	GigabitEthernet 0/24	Access	26	80	Postgrado
25	GigabitEthernet 0/25	Access	26	80	Postgrado
26	GigabitEthernet 0/26	Access	26	80	Postgrado
27	GigabitEthernet 0/27	Access	26	80	Postgrado
28	GigabitEthernet 0/28	Access	26	80	Postgrado
29	GigabitEthernet 0/29	Access	26	80	Postgrado
30	GigabitEthernet 0/30	Access	26	80	Postgrado

31	GigabitEthernet 0/31	Access	26	80	Postgrado
32	GigabitEthernet 0/32	Access	26	80	Postgrado
33	GigabitEthernet 0/33	Access	26	80	Postgrado
34	GigabitEthernet 0/34	Access	26	80	Postgrado
35	GigabitEthernet 0/35	Access	26	80	Postgrado
36	GigabitEthernet 0/36	Access	26	80	Postgrado
37	GigabitEthernet 0/37	Access	26	80	Postgrado
38	GigabitEthernet 0/38	Access	26	80	Postgrado
39	GigabitEthernet 0/39	Access	26	80	Postgrado
40	GigabitEthernet 0/40	Access	26	80	Postgrado
41	GigabitEthernet 0/41	Access	26	80	Postgrado
42	GigabitEthernet 0/42	Access	26	80	Postgrado
43	GigabitEthernet 0/43	Access	26	80	Postgrado
44	GigabitEthernet 0/44	Access	26	80	Postgrado
45	GigabitEthernet 0/45	Access	26	80	Postgrado
46	GigabitEthernet 0/46	Access	26	80	Postgrado
47	GigabitEthernet 0/47	Trunk	-	-	SW-Postgrado-Rack02
48	GigabitEthernet 0/48	Trunk	-	-	SW-Postgrado-Rack02
49	GigabitEthernet 0/49	Access	1	1	Libre
50	GigabitEthernet 0/50	Access	1	1	Libre

***Fuente**: Dirección de Desarrollo Tecnológico e Informático – UTN*

***TABLA 139.-** Descripción de las interfaces del Switch 04 del segundo piso del Edificio de Postgrado*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 04 DEL SEGUNDO PISO DEL EDIFICIO DE POSTGRADO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1/0/1	Access	2	6	AP – UTN
2	GigabitEthernet 1/0/2	Access	2	6	AP - UTN
3	GigabitEthernet 1/0/3	Access	26	80	Postgrado
4	GigabitEthernet 1/0/4	Access	26	80	Postgrado
5	GigabitEthernet 1/0/5	Access	26	80	Postgrado
6	GigabitEthernet 1/0/6	Access	26	80	Postgrado
7	GigabitEthernet 1/0/7	Access	26	80	Postgrado
8	GigabitEthernet 1/0/8	Access	26	80	Postgrado

9	GigabitEthernet 1/0/9	Access	26	80	Postgrado
10	GigabitEthernet 1/0/10	Access	26	80	Postgrado
11	GigabitEthernet 1/0/11	Access	26	80	Postgrado
12	GigabitEthernet 1/0/12	Access	26	80	Postgrado
13	GigabitEthernet 1/0/13	Access	26	80	Postgrado
14	GigabitEthernet 1/0/14	Access	26	80	Postgrado
15	GigabitEthernet 1/0/15	Access	26	80	Postgrado
16	GigabitEthernet 1/0/16	Access	26	80	Postgrado
17	GigabitEthernet 1/0/17	Access	26	80	Postgrado
18	GigabitEthernet 1/0/18	Access	26	80	Postgrado
19	GigabitEthernet 1/0/19	Access	26	80	Postgrado
20	GigabitEthernet 1/0/20	Access	26	80	Postgrado
21	GigabitEthernet 1/0/21	Access	26	80	Postgrado
22	GigabitEthernet 1/0/22	Access	26	80	Postgrado
23	GigabitEthernet 1/0/23	Access	26	80	Postgrado
24	GigabitEthernet 1/0/24	Trunk	-	-	SW-Postgrado
25	GigabitEthernet 1/0/25	Access	1	1	Libre
26	GigabitEthernet 1/0/26	Access	1	1	Libre
27	GigabitEthernet 1/0/27	Access	1	1	Libre
28	GigabitEthernet 1/0/28	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red en el Edificio del Centro Académico de Idiomas CAI

En el CAI existen dos racks de comunicaciones en la planta baja y en el segundo piso.

- **Planta Baja**

En el Rack de la planta baja existen dos Switchs de Acceso y en las Tablas 140 y 141 se muestra la descripción de cada una de las interfaces de los mismos.

TABLA 140.- *Descripción de las interfaces del Switch 01 de la planta baja del CAI*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DE LA PLANTA BAJA DEL CAI					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	28	92	CAI - Admins
2	GigabitEthernet 2	Access	28	92	CAI – Admins

3	GigabitEthernet 3	Access	28	92	CAI – Admins
4	GigabitEthernet 4	Access	28	92	CAI – Admins
5	GigabitEthernet 5	Access	28	92	CAI – Admins
6	GigabitEthernet 6	Access	28	92	CAI – Admins
7	GigabitEthernet 7	Access	28	92	CAI – Admins
8	GigabitEthernet 8	Access	28	92	CAI – Admins
9	GigabitEthernet 9	Access	28	92	CAI – Admins
10	GigabitEthernet 10	Access	28	92	CAI – Admins
11	GigabitEthernet 11	Access	28	92	CAI – Admins
12	GigabitEthernet 12	Access	28	92	CAI – Admins
13	GigabitEthernet 13	Access	28	92	CAI – Admins
14	GigabitEthernet 14	Access	28	92	CAI – Admins
15	GigabitEthernet 15	Access	28	92	CAI – Admins
16	GigabitEthernet 16	Access	28	92	CAI – Admins
17	GigabitEthernet 17	Access	28	92	CAI – Admins
18	GigabitEthernet 18	Access	28	92	CAI – Admins
19	GigabitEthernet 19	Access	28	92	CAI – Admins
20	GigabitEthernet 20	Access	28	92	CAI – Admins
21	GigabitEthernet 21	Access	28	92	CAI – Admins
22	GigabitEthernet 22	Access	28	92	CAI – Admins
23	GigabitEthernet 23	Trunk	-	-	
24	GigabitEthernet 24	Trunk	-	-	
25	GigabitEthernet 25	Access	28	92	CAI – Admins
26	GigabitEthernet 26	Access	28	92	CAI – Admins
27	GigabitEthernet 27	Access	28	92	CAI – Admins
28	GigabitEthernet 28	Access	28	92	CAI – Admins
29	GigabitEthernet 29	Access	28	92	CAI – Admins
30	GigabitEthernet 30	Access	28	92	CAI – Admins
31	GigabitEthernet 31	Access	28	92	CAI – Admins
32	GigabitEthernet 32	Access	28	92	CAI – Admins
33	GigabitEthernet 33	Access	28	92	CAI – Admins
34	GigabitEthernet 34	Access	28	92	CAI – Admins
35	GigabitEthernet 35	Access	28	92	CAI – Admins
36	GigabitEthernet 36	Access	28	92	CAI – Admins
37	GigabitEthernet 37	Access	28	92	CAI – Admins

38	GigabitEthernet 38	Access	28	92	CAI – Admins
39	GigabitEthernet 39	Access	28	92	CAI – Admins
40	GigabitEthernet 40	Access	28	92	CAI – Admins
41	GigabitEthernet 41	Access	28	92	CAI – Admins
42	GigabitEthernet 42	Access	28	92	CAI – Admins
43	GigabitEthernet 43	Access	28	92	CAI – Admins
44	GigabitEthernet 44	Access	28	92	CAI – Admins
45	GigabitEthernet 45	Access	28	92	CAI – Admins
46	GigabitEthernet 46	Access	28	92	CAI – Admins
47	GigabitEthernet 47	Trunk	-	-	
48	GigabitEthernet 48	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 141.- *Descripción de las interfaces del Switch 02 de la planta baja del CAI*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DE LA PLANTA BAJA DEL CAI					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	28	92	CAI - Admins
2	GigabitEthernet 2	Access	28	92	CAI – Admins
3	GigabitEthernet 3	Access	28	92	CAI – Admins
4	GigabitEthernet 4	Access	28	92	CAI – Admins
5	GigabitEthernet 5	Access	28	92	CAI – Admins
6	GigabitEthernet 6	Access	28	92	CAI – Admins
7	GigabitEthernet 7	Access	24	92	CAI – Admins
8	GigabitEthernet 8	Access	28	92	CAI – Admins
9	GigabitEthernet 9	Access	28	92	CAI – Admins
10	GigabitEthernet 10	Access	28	92	CAI – Admins
11	GigabitEthernet 11	Access	28	92	CAI – Admins
12	GigabitEthernet 12	Trunk	-	-	
13	GigabitEthernet 13	Access	28	92	CAI - Admins
14	GigabitEthernet 14	Access	28	92	CAI - Admins
15	GigabitEthernet 15	Access	28	92	CAI - Admins
16	GigabitEthernet 16	Access	28	92	CAI - Admins
17	GigabitEthernet 17	Access	28	92	CAI - Admins

18	GigabitEthernet 18	Access	28	92	CAI - Admins
19	GigabitEthernet 19	Access	28	92	CAI - Admins
20	GigabitEthernet 20	Access	28	92	CAI - Admins
21	GigabitEthernet 21	Access	28	92	CAI - Admins
22	GigabitEthernet 22	Access	28	92	CAI - Admins
23	GigabitEthernet 23	Access	28	92	CAI - Admins
24	GigabitEthernet 24	Trunk	-	-	

***Fuente**: Dirección de Desarrollo Tecnológico e Informático – UTN*

- **Segundo Piso**

Existen cuatro Switchs de Acceso en el Rack del segundo piso del CAI, en las Tablas 142, 143, 144 y 145 se muestra la descripción de las interfaces de red de los mismos.

***TABLA 142.-** Descripción de las interfaces del Switch 01 del segundo piso del CAI*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL SEGUNDO PISO DEL CAI					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	24	92	CAI - Admins
2	GigabitEthernet 2	Access	24	92	CAI - Admins
3	GigabitEthernet 3	Access	24	92	CAI - Admins
4	GigabitEthernet 4	Access	24	92	CAI - Admins
5	GigabitEthernet 5	Access	24	92	CAI - Admins
6	GigabitEthernet 6	Access	24	92	CAI - Admins
7	GigabitEthernet 7	Access	24	92	CAI - Admins
8	GigabitEthernet 8	Access	24	92	CAI - Admins
9	GigabitEthernet 9	Access	24	92	CAI - Admins
10	GigabitEthernet 10	Access	24	92	CAI - Admins
11	GigabitEthernet 11	Access	24	92	CAI - Admins
12	GigabitEthernet 12	Access	24	92	CAI - Admins
13	GigabitEthernet 13	Access	24	92	CAI - Admins
14	GigabitEthernet 14	Access	24	92	CAI - Admins
15	GigabitEthernet 15	Access	24	92	CAI - Admins
16	GigabitEthernet 16	Access	24	92	CAI - Admins
17	GigabitEthernet 17	Access	24	92	CAI - Admins
18	GigabitEthernet 18	Access	24	92	CAI - Admins
19	GigabitEthernet 19	Access	24	92	CAI - Admins

20	GigabitEthernet 20	Access	24	92	CAI - Admins
21	GigabitEthernet 21	Access	24	92	CAI - Admins
22	GigabitEthernet 22	Access	24	92	CAI - Admins
23	GigabitEthernet 23	Access	24	92	CAI - Admins
24	GigabitEthernet 24	Trunk			
25	GigabitEthernet 25	Access	24	92	CAI - Admins
26	GigabitEthernet 26	Access	24	92	CAI - Admins
27	GigabitEthernet 27	Access	24	92	CAI - Admins
28	GigabitEthernet 28	Access	24	92	CAI - Admins
29	GigabitEthernet 29	Access	24	92	CAI - Admins
30	GigabitEthernet 30	Access	24	92	CAI - Admins
31	GigabitEthernet 31	Access	24	92	CAI - Admins
32	GigabitEthernet 32	Access	24	92	CAI - Admins
33	GigabitEthernet 33	Access	24	92	CAI - Admins
34	GigabitEthernet 34	Access	24	92	CAI - Admins
35	GigabitEthernet 35	Access	24	92	CAI - Admins
36	GigabitEthernet 36	Access	24	92	CAI - Admins
37	GigabitEthernet 37	Access	24	92	CAI - Admins
38	GigabitEthernet 38	Access	24	92	CAI - Admins
39	GigabitEthernet 39	Access	24	92	CAI - Admins
40	GigabitEthernet 40	Access	24	92	CAI - Admins
41	GigabitEthernet 41	Access	24	92	CAI - Admins
42	GigabitEthernet 42	Access	24	92	CAI - Admins
43	GigabitEthernet 43	Access	24	92	CAI - Admins
44	GigabitEthernet 44	Access	24	92	CAI - Admins
45	GigabitEthernet 45	Access	24	92	CAI - Admins
46	GigabitEthernet 46	Access	24	92	CAI - Admins
47	GigabitEthernet 47	Access	24	92	CAI - Admins
48	GigabitEthernet 48	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 143.- *Descripción de las interfaces del Switch 02 de la planta baja del CAI*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL SEGUNDO PISO DEL CAI					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	24	92	CAI - Admins
2	GigabitEthernet 0/2	Access	24	92	CAI - Admins
3	GigabitEthernet 0/3	Access	24	92	CAI - Admins
4	GigabitEthernet 0/4	Access	24	92	CAI - Admins
5	GigabitEthernet 0/5	Access	24	92	CAI - Admins
6	GigabitEthernet 0/6	Access	24	92	CAI - Admins
7	GigabitEthernet 0/7	Access	24	92	CAI - Admins
8	GigabitEthernet 0/8	Access	24	92	CAI - Admins
9	GigabitEthernet 0/9	Access	24	92	CAI - Admins
10	GigabitEthernet 0/10	Access	24	92	CAI - Admins
11	GigabitEthernet 0/11	Access	24	92	CAI - Admins
12	GigabitEthernet 0/12	Access	24	92	CAI - Admins
13	GigabitEthernet 0/13	Access	24	92	CAI - Admins
14	GigabitEthernet 0/14	Access	2	6	AP - UTN
15	GigabitEthernet 0/15	Access	24	92	CAI - Admins
16	GigabitEthernet 0/16	Access	24	92	CAI - Admins
17	GigabitEthernet 0/17	Access	24	92	CAI - Admins
18	GigabitEthernet 0/18	Access	24	92	CAI - Admins
19	GigabitEthernet 0/19	Access	24	92	CAI - Admins
20	GigabitEthernet 0/20	Access	24	92	CAI - Admins
21	GigabitEthernet 0/21	Access	24	92	CAI - Admins
22	GigabitEthernet 0/22	Access	24	92	CAI - Admins
23	GigabitEthernet 0/23	Access	24	92	CAI - Admins
24	GigabitEthernet 0/24	Trunk	-	-	
25	GigabitEthernet 0/25	Access	24	92	CAI - Admins
26	GigabitEthernet 0/26	Access	24	92	CAI - Admins
27	GigabitEthernet 0/27	Access	24	92	CAI - Admins
28	GigabitEthernet 0/28	Access	24	92	CAI - Admins
29	GigabitEthernet 0/29	Access	24	92	CAI - Admins
30	GigabitEthernet 0/30	Access	24	92	CAI - Admins
31	GigabitEthernet 0/31	Access	24	92	CAI - Admins
32	GigabitEthernet 0/32	Access	24	92	CAI - Admins
33	GigabitEthernet 0/33	Access	24	92	CAI - Admins
34	GigabitEthernet 0/34	Access	24	92	CAI - Admins
35	GigabitEthernet 0/35	Access	24	92	CAI - Admins
36	GigabitEthernet 0/36	Access	24	92	CAI - Admins
37	GigabitEthernet 0/37	Access	24	92	CAI - Admins
38	GigabitEthernet 0/38	Access	24	92	CAI - Admins
39	GigabitEthernet 0/39	Access	24	92	CAI - Admins
40	GigabitEthernet 0/40	Access	24	92	CAI - Admins
41	GigabitEthernet 0/41	Access	24	92	CAI - Admins
42	GigabitEthernet 0/42	Access	24	92	CAI - Admins
43	GigabitEthernet 0/43	Access	24	92	CAI - Admins
44	GigabitEthernet 0/44	Access	24	92	CAI - Admins
45	GigabitEthernet 0/45	Access	24	92	CAI - Admins
46	GigabitEthernet 0/46	Access	24	92	CAI - Admins
47	GigabitEthernet 0/47	Access	24	92	CAI - Admins
48	GigabitEthernet 0/48	Trunk	-	-	

Fuente*: Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 144.- *Descripción de las interfaces del Switch 03 del segundo piso del CAI*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL SEGUNDO PISO DEL CAI					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Access	24	88	CAI - Laboratorios
2	FastEthernet 1/2	Access	122	4	DMZ
3	FastEthernet 1/3	Access	24	88	CAI - Laboratorios
4	FastEthernet 1/4	Access	24	88	CAI - Laboratorios
5	FastEthernet 1/5	Access	24	88	CAI - Laboratorios
6	FastEthernet 1/6	Access	24	88	CAI - Laboratorios
7	FastEthernet 1/7	Access	24	88	CAI - Laboratorios
8	FastEthernet 1/8	Access	24	88	CAI - Laboratorios
9	FastEthernet 1/9	Access	24	88	CAI - Laboratorios
10	FastEthernet 1/10	Access	24	88	CAI - Laboratorios
11	FastEthernet 1/11	Access	24	88	CAI - Laboratorios
12	FastEthernet 1/12	Access	24	88	CAI - Laboratorios
13	FastEthernet 1/13	Access	24	88	CAI - Laboratorios
14	FastEthernet 1/14	Access	24	88	CAI - Laboratorios
15	FastEthernet 1/15	Access	24	88	CAI - Laboratorios
16	FastEthernet 1/16	Access	24	88	CAI - Laboratorios
17	FastEthernet 1/17	Access	24	88	CAI - Laboratorios
18	FastEthernet 1/18	Access	24	88	CAI - Laboratorios
19	FastEthernet 1/19	Access	24	88	CAI - Laboratorios
20	FastEthernet 1/20	Access	24	88	CAI - Laboratorios
21	FastEthernet 1/21	Access	24	88	CAI - Laboratorios
22	FastEthernet 1/22	Access	24	88	CAI - Laboratorios
23	FastEthernet 1/23	Access	24	88	CAI - Laboratorios
24	FastEthernet 1/24	Access	24	88	CAI - Laboratorios
25	FastEthernet 1/25	-	-	-	-
26	FastEthernet 1/26	Trunk	-	-	
27	FastEthernet 1/27	Trunk	-	-	
28	FastEthernet 1/28	Trunk	-	-	
29	FastEthernet 2/1	Access	24	88	CAI - Laboratorios
30	FastEthernet 2/2	Access	24	88	CAI - Laboratorios
31	FastEthernet 2/3	Access	24	88	CAI - Laboratorios

32	FastEthernet 2/4	Access	24	88	CAI - Laboratorios
33	FastEthernet 2/5	Access	24	88	CAI - Laboratorios
34	FastEthernet 2/6	Access	24	88	CAI - Laboratorios
35	FastEthernet 2/7	Access	24	88	CAI - Laboratorios
36	FastEthernet 2/8	Access	24	88	CAI - Laboratorios
37	FastEthernet 2/9	Access	24	88	CAI - Laboratorios
38	FastEthernet 2/10	Access	24	88	CAI - Laboratorios
39	FastEthernet 2/11	Access	24	88	CAI - Laboratorios
40	FastEthernet 2/12	Access	24	88	CAI - Laboratorios
41	FastEthernet 2/13	Access	24	88	CAI - Laboratorios
42	FastEthernet 2/14	Access	24	88	CAI - Laboratorios
43	FastEthernet 2/15	Access	24	88	CAI - Laboratorios
44	FastEthernet 2/16	Access	24	88	CAI - Laboratorios
45	FastEthernet 2/17	Access	24	88	CAI - Laboratorios
46	FastEthernet 2/18	Access	24	88	CAI - Laboratorios
47	FastEthernet 2/19	Access	24	88	CAI - Laboratorios
48	FastEthernet 2/20	Access	24	88	CAI - Laboratorios
49	FastEthernet 2/21	Access	2	6	AP - UTN
50	FastEthernet 2/22	Access	2	6	AP – UTN
51	FastEthernet 2/23	Access	2	6	AP – UTN
52	FastEthernet 2/24	Access	2	6	AP – UTN
53	FastEthernet 2/25	Trunk	-	-	
54	FastEthernet 2/26	-	-	-	-
55	FastEthernet 2/27	Trunk	-	-	
56	FastEthernet 2/28	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 145.- *Descripción de las interfaces del Switch 04 del segundo piso del CAI*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 04 DEL SEGUNDO PISO DEL CAI					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Access	24	88	CAI - Laboratorios
2	FastEthernet 1/2	Access	122	4	DMZ

3	FastEthernet 1/3	Access	24	88	CAI - Laboratorios
4	FastEthernet 1/4	Access	24	88	CAI - Laboratorios
5	FastEthernet 1/5	Access	24	88	CAI - Laboratorios
6	FastEthernet 1/6	Access	24	88	CAI - Laboratorios
7	FastEthernet 1/7	Access	24	88	CAI - Laboratorios
8	FastEthernet 1/8	Access	24	88	CAI - Laboratorios
9	FastEthernet 1/9	Access	24	88	CAI - Laboratorios
10	FastEthernet 1/10	Access	24	88	CAI - Laboratorios
11	FastEthernet 1/11	Access	24	88	CAI - Laboratorios
12	FastEthernet 1/12	Access	24	88	CAI - Laboratorios
13	FastEthernet 1/13	Access	24	88	CAI - Laboratorios
14	FastEthernet 1/14	Access	24	88	CAI - Laboratorios
15	FastEthernet 1/15	Access	24	88	CAI - Laboratorios
16	FastEthernet 1/16	Access	24	88	CAI - Laboratorios
17	FastEthernet 1/17	Access	24	88	CAI - Laboratorios
18	FastEthernet 1/18	Access	24	88	CAI - Laboratorios
19	FastEthernet 1/19	Access	24	88	CAI - Laboratorios
20	FastEthernet 1/20	Access	24	88	CAI - Laboratorios
21	FastEthernet 1/21	Access	24	88	CAI - Laboratorios
22	FastEthernet 1/22	Access	24	88	CAI - Laboratorios
23	FastEthernet 1/23	Access	24	88	CAI - Laboratorios
24	FastEthernet 1/24	Access	24	88	CAI - Laboratorios
25	FastEthernet 1/25	-	-	-	-
26	FastEthernet 1/26	Trunk	-	-	
27	FastEthernet 1/27	Trunk	-	-	
28	FastEthernet 1/28	Trunk	-	-	
29	FastEthernet 2/1	Access	24	88	CAI - Laboratorios
30	FastEthernet 2/2	Access	24	88	CAI - Laboratorios
31	FastEthernet 2/3	Access	24	88	CAI - Laboratorios
32	FastEthernet 2/4	Access	24	88	CAI - Laboratorios
33	FastEthernet 2/5	Access	24	88	CAI - Laboratorios
34	FastEthernet 2/6	Access	24	88	CAI - Laboratorios
35	FastEthernet 2/7	Access	24	88	CAI - Laboratorios
36	FastEthernet 2/8	Access	24	88	CAI - Laboratorios
37	FastEthernet 2/9	Access	24	88	CAI - Laboratorios

38	FastEthernet 2/10	Access	24	88	CAI - Laboratorios
39	FastEthernet 2/11	Access	24	88	CAI - Laboratorios
40	FastEthernet 2/12	Access	24	88	CAI - Laboratorios
41	FastEthernet 2/13	Access	24	88	CAI - Laboratorios
42	FastEthernet 2/14	Access	24	88	CAI - Laboratorios
43	FastEthernet 2/15	Access	24	88	CAI - Laboratorios
44	FastEthernet 2/16	Access	24	88	CAI - Laboratorios
45	FastEthernet 2/17	Access	24	88	CAI - Laboratorios
46	FastEthernet 2/18	Access	24	88	CAI - Laboratorios
47	FastEthernet 2/19	Access	24	88	CAI - Laboratorios
48	FastEthernet 2/20	Access	24	88	CAI - Laboratorios
49	FastEthernet 2/21	Access	2	6	AP - UTN
50	FastEthernet 2/22	Access	2	6	AP – UTN
51	FastEthernet 2/23	Access	2	6	AP – UTN
52	FastEthernet 2/24	Access	2	6	AP – UTN
53	FastEthernet 2/25	Trunk	-	-	
54	FastEthernet 2/26	-	-	-	-
55	FastEthernet 2/27	Trunk	-	-	
56	FastEthernet 2/28	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red en la Biblioteca

En la Biblioteca existen varios racks donde se alojan los Switchs de Acceso.

- **Cuarto de Equipos**

En el cuarto de equipos de la biblioteca existen 3 Switchs de acceso, y en las tablas 146, 147 y 148 se muestran las configuraciones de las interfaces de red.

TABLA 146.- *Descripción de las interfaces del Switch 01 del cuarto de equipos de la Biblioteca*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL CUARTO DE EQUIPOS DE LA BIBLIOTECA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 0/1	Access	36	100	Biblioteca

2	FastEthernet 0/2	Access	36	100	Biblioteca
3	FastEthernet 0/3	Access	36	100	Biblioteca
4	FastEthernet 0/4	Access	36	100	Biblioteca
5	FastEthernet 0/5	Access	36	100	Biblioteca
6	FastEthernet 0/6	Access	36	100	Biblioteca
7	FastEthernet 0/7	Access	36	100	Biblioteca
8	FastEthernet 0/8	Access	36	100	Biblioteca
9	FastEthernet 0/9	Access	36	100	Biblioteca
10	FastEthernet 0/10	Access	36	100	Biblioteca
11	FastEthernet 0/11	Access	36	100	Biblioteca
12	FastEthernet 0/12	Access	36	100	Biblioteca
13	FastEthernet 0/13	Access	36	100	Biblioteca
14	FastEthernet 0/14	Access	36	100	Biblioteca
15	FastEthernet 0/15	Access	36	100	Biblioteca
16	FastEthernet 0/16	Access	36	100	Biblioteca
17	FastEthernet 0/17	Access	36	100	Biblioteca
18	FastEthernet 0/18	Access	36	100	Biblioteca
19	FastEthernet 0/19	Access	36	100	Biblioteca
20	FastEthernet 0/20	Access	36	100	Biblioteca
21	FastEthernet 0/21	Access	36	100	Biblioteca
22	FastEthernet 0/22	Access	36	100	Biblioteca
23	FastEthernet 0/23	Access	36	100	Biblioteca
24	FastEthernet 0/24	Access	36	100	Biblioteca
25	FastEthernet 0/25	Access	36	100	Biblioteca
26	FastEthernet 0/26	Access	36	100	Biblioteca
27	FastEthernet 0/27	Access	36	100	Biblioteca
28	FastEthernet 0/28	Access	36	100	Biblioteca
29	FastEthernet 0/29	Access	122	4	DMZ-Biblioteca
30	FastEthernet 0/30	Access	36	100	Biblioteca
31	FastEthernet 0/31	Access	36	100	Biblioteca
32	FastEthernet 0/32	Access	36	100	Biblioteca
33	FastEthernet 0/33	Access	36	100	Biblioteca
34	FastEthernet 0/34	Access	36	100	Biblioteca

35	FastEthernet 0/35	Access	36	100	Biblioteca
36	FastEthernet 0/36	Access	36	100	Biblioteca
37	FastEthernet 0/37	Access	36	100	Biblioteca
38	FastEthernet 0/38	Access	36	100	Biblioteca
39	FastEthernet 0/39	Access	36	100	Biblioteca
40	FastEthernet 0/40	Access	36	100	Biblioteca
41	FastEthernet 0/41	Access	36	100	Biblioteca
42	FastEthernet 0/42	Access	36	100	Biblioteca
43	FastEthernet 0/43	Access	36	100	Biblioteca
44	FastEthernet 0/44	Access	36	100	Biblioteca
45	FastEthernet 0/45	Access	36	100	Biblioteca
46	FastEthernet 0/46	Access	36	100	Biblioteca
47	FastEthernet 0/47	Access	2	6	AP – UTN
48	FastEthernet 0/48	Trunk	-	-	Sw-Cisco3G300
49	GigabitEthernet 0/1	Trunk	-	-	Distribución FICA
50	GigabitEthernet 0/2	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 147.- *Descripción de las interfaces del Switch 02 del cuarto de equipos de la Biblioteca*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL CUARTO DE EQUIPOS DE LA BIBLIOTECA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	36	100	Biblioteca
2	GigabitEthernet 2	Access	36	100	Biblioteca
3	GigabitEthernet 3	Access	36	100	Biblioteca
4	GigabitEthernet 4	Access	36	100	Biblioteca
5	GigabitEthernet 5	Access	36	100	Biblioteca
6	GigabitEthernet 6	Access	36	100	Biblioteca
7	GigabitEthernet 7	Access	36	100	Biblioteca
8	GigabitEthernet 8	Access	36	100	Biblioteca
9	GigabitEthernet 9	Access	36	100	Biblioteca

10	GigabitEthernet 10	Access	36	100	Biblioteca
11	GigabitEthernet 11	Access	36	100	Biblioteca
12	GigabitEthernet 12	Access	36	100	Biblioteca
13	GigabitEthernet 13	Access	36	100	Biblioteca
14	GigabitEthernet 14	Access	36	100	Biblioteca
15	GigabitEthernet 15	Access	36	100	Biblioteca
16	GigabitEthernet 16	Access	36	100	Biblioteca
17	GigabitEthernet 17	Access	36	100	Biblioteca
18	GigabitEthernet 18	Access	36	100	Biblioteca
19	GigabitEthernet 19	Access	36	100	Biblioteca
20	GigabitEthernet 20	Access	36	100	Biblioteca
21	GigabitEthernet 21	Access	36	100	Biblioteca
22	GigabitEthernet 22	Access	36	100	Biblioteca
23	GigabitEthernet 23	Access	36	100	Biblioteca
24	GigabitEthernet 24	Access	36	100	Biblioteca
25	GigabitEthernet 25	Access	36	100	Biblioteca
26	GigabitEthernet 26	Access	36	100	Biblioteca
27	GigabitEthernet 27	Access	36	100	Biblioteca
28	GigabitEthernet 28	Access	36	100	Biblioteca
29	GigabitEthernet 29	Access	36	100	Biblioteca
30	GigabitEthernet 30	Access	36	100	Biblioteca
31	GigabitEthernet 31	Access	36	100	Biblioteca
32	GigabitEthernet 32	Access	36	100	Biblioteca
33	GigabitEthernet 33	Access	36	100	Biblioteca
34	GigabitEthernet 34	Access	36	100	Biblioteca
35	GigabitEthernet 35	Access	36	100	Biblioteca
36	GigabitEthernet 36	Access	36	100	Biblioteca
37	GigabitEthernet 37	Access	7	100	Biblioteca
38	GigabitEthernet 38	Access	7	100	Biblioteca
39	GigabitEthernet 39	Access	7	100	Biblioteca
40	GigabitEthernet 40	Access	7	100	Biblioteca
41	GigabitEthernet 41	Access	7	100	Biblioteca
42	GigabitEthernet 42	Access	7	100	Biblioteca
43	GigabitEthernet 43	Access	7	100	Biblioteca
44	GigabitEthernet 44	Access	7	100	Biblioteca

45	GigabitEthernet 45	Access	7	100	Biblioteca
46	GigabitEthernet 46	Access	7	100	Biblioteca
47	GigabitEthernet 47	Access	7	100	Biblioteca
48	GigabitEthernet 48	Access	7	100	Biblioteca
49	GigabitEthernet 49	Trunk	-	-	
50	GigabitEthernet 50	Trunk	-	-	
51	GigabitEthernet 51	Trunk	-	-	
52	GigabitEthernet 52	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 148.- *Descripción de las interfaces del Switch 03 del cuarto de equipos de la Biblioteca*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL CUARTO DE EQUIPOS DE LA BIBLIOTECA					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	36	100	Biblioteca
2	GigabitEthernet 2	Access	36	100	Biblioteca
3	GigabitEthernet 3	Access	36	100	Biblioteca
4	GigabitEthernet 4	Access	36	100	Biblioteca
5	GigabitEthernet 5	Access	36	100	Biblioteca
6	GigabitEthernet 6	Access	36	100	Biblioteca
7	GigabitEthernet 7	Access	36	100	Biblioteca
8	GigabitEthernet 8	Access	36	100	Biblioteca
9	GigabitEthernet 9	Access	36	100	Biblioteca
10	GigabitEthernet 10	Access	36	100	Biblioteca
11	GigabitEthernet 11	Access	36	100	Biblioteca
12	GigabitEthernet 12	Access	36	100	Biblioteca
13	GigabitEthernet 13	Access	36	100	Biblioteca
14	GigabitEthernet 14	Access	36	100	Biblioteca
15	GigabitEthernet 15	Access	36	100	Biblioteca
16	GigabitEthernet 16	Access	36	100	Biblioteca
17	GigabitEthernet 17	Trunk	-	-	
18	GigabitEthernet 18	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

- **IC3**

En el IC3 existen dos Switchs destinados a acceso de red, en las tablas 149 y 150 se indican las configuraciones de las interfaces de red.

TABLA 149.- *Descripción de las interfaces del Switch 01 del IC3*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL IC3					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	7	100	Biblioteca
2	GigabitEthernet 2	Access	7	100	Biblioteca
3	GigabitEthernet 3	Access	7	100	Biblioteca
4	GigabitEthernet 4	Access	7	100	Biblioteca
5	GigabitEthernet 5	Access	7	100	Biblioteca
6	GigabitEthernet 6	Access	7	100	Biblioteca
7	GigabitEthernet 7	Access	7	100	Biblioteca
8	GigabitEthernet 8	Access	7	100	Biblioteca
9	GigabitEthernet 9	Access	7	100	Biblioteca
10	GigabitEthernet 10	Access	7	100	Biblioteca
11	GigabitEthernet 11	Access	7	100	Biblioteca
12	GigabitEthernet 12	Access	7	100	Biblioteca
13	GigabitEthernet 13	Access	7	100	Biblioteca
14	GigabitEthernet 14	Access	7	100	Biblioteca
15	GigabitEthernet 15	Access	7	100	Biblioteca
16	GigabitEthernet 16	Access	7	100	Biblioteca
17	GigabitEthernet 17	Access	7	100	Biblioteca
18	GigabitEthernet 18	Access	7	100	Biblioteca
19	GigabitEthernet 19	Access	7	100	Biblioteca
20	GigabitEthernet 20	Access	7	100	Biblioteca
21	GigabitEthernet 21	Access	7	100	Biblioteca
22	GigabitEthernet 22	Access	7	100	Biblioteca
23	GigabitEthernet 23	Access	7	100	Biblioteca
24	GigabitEthernet 24	Access	7	100	Biblioteca
25	GigabitEthernet 25	Access	7	100	Biblioteca
26	GigabitEthernet 26	Access	7	100	Biblioteca
27	GigabitEthernet 27	Access	7	100	Biblioteca
28	GigabitEthernet 28	Access	7	100	Biblioteca

29	GigabitEthernet 29	Access	7	100	Biblioteca
30	GigabitEthernet 30	Access	7	100	Biblioteca
31	GigabitEthernet 31	Access	7	100	Biblioteca
32	GigabitEthernet 32	Access	7	100	Biblioteca
33	GigabitEthernet 33	Access	7	100	Biblioteca
34	GigabitEthernet 34	Access	7	100	Biblioteca
35	GigabitEthernet 35	Access	7	100	Biblioteca
36	GigabitEthernet 36	Access	7	100	Biblioteca
37	GigabitEthernet 37	Access	7	100	Biblioteca
38	GigabitEthernet 38	Access	7	100	Biblioteca
39	GigabitEthernet 39	Access	7	100	Biblioteca
40	GigabitEthernet 40	Access	7	100	Biblioteca
41	GigabitEthernet 41	Access	7	100	Biblioteca
42	GigabitEthernet 42	Access	7	100	Biblioteca
43	GigabitEthernet 43	Access	7	100	Biblioteca
44	GigabitEthernet 44	Access	7	100	Biblioteca
45	GigabitEthernet 45	Access	7	100	Biblioteca
46	GigabitEthernet 46	Access	7	100	Biblioteca
47	GigabitEthernet 47	Access	7	100	Biblioteca
48	GigabitEthernet 48	Access	7	100	Biblioteca
49	GigabitEthernet 49	Trunk	-	-	
50	GigabitEthernet 50	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

TABLA 150.- *Descripción de las interfaces del Switch 02 del IC3*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL IC3					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 1	Access	7	100	Biblioteca
2	GigabitEthernet 2	Access	7	100	Biblioteca
3	GigabitEthernet 3	Access	7	100	Biblioteca
4	GigabitEthernet 4	Access	7	100	Biblioteca
5	GigabitEthernet 5	Access	7	100	Biblioteca
6	GigabitEthernet 6	Access	7	100	Biblioteca
7	GigabitEthernet 7	Access	7	100	Biblioteca
8	GigabitEthernet 8	Access	7	100	Biblioteca

9	GigabitEthernet 9	Access	7	100	Biblioteca
10	GigabitEthernet 10	Access	7	100	Biblioteca
11	GigabitEthernet 11	Access	7	100	Biblioteca
12	GigabitEthernet 12	Access	7	100	Biblioteca
13	GigabitEthernet 13	Access	7	100	Biblioteca
14	GigabitEthernet 14	Access	7	100	Biblioteca
15	GigabitEthernet 15	Access	7	100	Biblioteca
16	GigabitEthernet 16	Access	7	100	Biblioteca
17	GigabitEthernet 17	Access	7	100	Biblioteca
18	GigabitEthernet 18	Access	7	100	Biblioteca
19	GigabitEthernet 19	Access	7	100	Biblioteca
20	GigabitEthernet 20	Access	7	100	Biblioteca
21	GigabitEthernet 21	Access	7	100	Biblioteca
22	GigabitEthernet 22	Access	7	100	Biblioteca
23	GigabitEthernet 23	Access	7	100	Biblioteca
24	GigabitEthernet 24	Access	7	100	Biblioteca
25	GigabitEthernet 25	Access	7	100	Biblioteca
26	GigabitEthernet 26	Access	7	100	Biblioteca
27	GigabitEthernet 27	Access	7	100	Biblioteca
28	GigabitEthernet 28	Access	7	100	Biblioteca
29	GigabitEthernet 29	Access	7	100	Biblioteca
30	GigabitEthernet 30	Access	7	100	Biblioteca
31	GigabitEthernet 31	Access	7	100	Biblioteca
32	GigabitEthernet 32	Access	7	100	Biblioteca
33	GigabitEthernet 33	Access	7	100	Biblioteca
34	GigabitEthernet 34	Access	7	100	Biblioteca
35	GigabitEthernet 35	Access	7	100	Biblioteca
36	GigabitEthernet 36	Access	7	100	Biblioteca
37	GigabitEthernet 37	Access	7	100	Biblioteca
38	GigabitEthernet 38	Access	7	100	Biblioteca
39	GigabitEthernet 39	Access	7	100	Biblioteca
40	GigabitEthernet 40	Access	7	100	Biblioteca
41	GigabitEthernet 41	Access	7	100	Biblioteca
42	GigabitEthernet 42	Access	7	100	Biblioteca
43	GigabitEthernet 43	Access	7	100	Biblioteca

44	GigabitEthernet 44	Access	7	100	Biblioteca
45	GigabitEthernet 45	Access	7	100	Biblioteca
46	GigabitEthernet 46	Access	7	100	Biblioteca
47	GigabitEthernet 47	Access	7	100	Biblioteca
48	GigabitEthernet 48	Trunk	-	-	
49	GigabitEthernet 49	Trunk	-	-	
50	GigabitEthernet 50	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

Equipos de red en el Colegio Universitario

Se detallan en la Tabla 151 las configuraciones sobre el modo de trabajo, las VLANs y la descripción de cada una de las interfaces de los Switchs que se encuentran en los diferentes Racks del Colegio Universitario.

TABLA 151.- *Descripción de las interfaces del Switch del Colegio Universitario*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH DEL COLEGIO UNIVERSITARIO					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	52	108	Colegio Admin.
2	GigabitEthernet 0/2	Access	52	108	Colegio Admin.
3	GigabitEthernet 0/3	Access	52	108	Colegio Admin.
4	GigabitEthernet 0/4	Access	52	108	Colegio Admin.
5	GigabitEthernet 0/5	Access	52	108	Colegio Admin.
6	GigabitEthernet 0/6	Access	52	108	Colegio Admin.
7	GigabitEthernet 0/7	Access	52	108	Colegio Admin.
8	GigabitEthernet 0/8	Access	52	108	Colegio Admin.
9	GigabitEthernet 0/9	Access	52	108	Colegio Admin.
10	GigabitEthernet 0/10	Access	52	108	Colegio Admin.
11	GigabitEthernet 0/11	Access	52	108	Colegio Admin.
12	GigabitEthernet 0/12	Access	52	108	Colegio Admin.
13	GigabitEthernet 0/13	Access	52	108	Colegio Admin.
14	GigabitEthernet 0/14	Access	52	108	Colegio Admin.
15	GigabitEthernet 0/15	Access	52	108	Colegio Admin.
16	GigabitEthernet 0/16	Access	52	108	Colegio Admin.
17	GigabitEthernet 0/17	Access	52	108	Colegio Admin.

18	GigabitEthernet 0/18	Access	52	108	Colegio Admin.
19	GigabitEthernet 0/19	Access	52	108	Colegio Admin.
20	GigabitEthernet 0/20	Access	52	108	Colegio Admin.
21	GigabitEthernet 0/21	Access	52	108	Colegio Admin.
22	GigabitEthernet 0/22	Access	52	108	Colegio Admin.
23	GigabitEthernet 0/23	Access	52	108	Colegio Admin.
24	GigabitEthernet 0/24	Access	52	108	Colegio Admin.
25	GigabitEthernet 0/25	Access	52	108	Colegio Admin.
26	GigabitEthernet 0/26	Access	52	108	Colegio Admin.
27	GigabitEthernet 0/27	Access	52	108	Colegio Admin.
28	GigabitEthernet 0/28	Access	52	108	Colegio Admin.
29	GigabitEthernet 0/29	Access	52	108	Colegio Admin.
30	GigabitEthernet 0/30	Access	52	108	Colegio Admin.
31	GigabitEthernet 0/31	Access	52	108	Colegio Admin.
32	GigabitEthernet 0/32	Access	52	108	Colegio Admin.
33	GigabitEthernet 0/33	Access	52	108	Colegio Admin.
34	GigabitEthernet 0/34	Access	52	108	Colegio Admin.
35	GigabitEthernet 0/35	Access	52	108	Colegio Admin.
36	GigabitEthernet 0/36	Access	52	108	Colegio Admin.
37	GigabitEthernet 0/37	Access	52	108	Colegio Admin.
38	GigabitEthernet 0/38	Access	52	108	Colegio Admin.
39	GigabitEthernet 0/39	Access	52	108	Colegio Admin.
40	GigabitEthernet 0/40	Access	52	108	Colegio Admin.
41	GigabitEthernet 0/41	Access	52	108	Colegio Admin.
42	GigabitEthernet 0/42	Access	52	108	Colegio Admin.
43	GigabitEthernet 0/43	Access	52	108	Colegio Admin.
44	GigabitEthernet 0/44	Access	52	108	Colegio Admin.
45	GigabitEthernet 0/45	Access	52	108	Colegio Admin.
46	GigabitEthernet 0/46	Access	52	108	Colegio Admin.
47	GigabitEthernet 0/47	Access	52	108	Colegio Admin.
48	GigabitEthernet 0/48	Trunk	-	-	-
49	GigabitEthernet 0/49	Access	1	1	Libre
50	GigabitEthernet 0/50	Access	1	1	Libre

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

Equipos de red en Bienestar Estudiantil

Se detallan en las Tablas 152, 153, 154, 155 y 156 las configuraciones sobre el modo de trabajo, las VLANs y la descripción de cada una de las interfaces de los Switchs que se encuentran en los diferentes Racks del Edificio de Bienestar Estudiantil.

TABLA 152.- *Descripción de las interfaces del Switch 01 del Edificio de Bienestar Estudiantil*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 01 DEL EDIFICO DE BIENESTAR ESTUDIANTIL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	96	112	Wireless-Docentes
2	GigabitEthernet 0/2	Access	96	112	Wireless-Docentes
3	GigabitEthernet 0/3	Access	96	112	Wireless-Docentes
4	GigabitEthernet 0/4	Access	96	112	Wireless-Docentes
5	GigabitEthernet 0/5	Access	96	112	Wireless-Docentes
6	GigabitEthernet 0/6	Access	96	112	Wireless-Docentes
7	GigabitEthernet 0/7	Access	96	112	Wireless-Docentes
8	GigabitEthernet 0/8	Access	96	112	Wireless-Docentes
9	GigabitEthernet 0/9	Access	96	112	Wireless-Docentes
10	GigabitEthernet 0/10	Access	96	112	Wireless-Docentes
11	GigabitEthernet 0/11	Access	96	112	Wireless-Docentes
12	GigabitEthernet 0/12	Access	96	112	Wireless-Docentes
13	GigabitEthernet 0/13	Access	96	112	Wireless-Docentes
14	GigabitEthernet 0/14	Access	96	112	Wireless-Docentes
15	GigabitEthernet 0/15	Access	96	112	Wireless-Docentes
16	GigabitEthernet 0/16	Access	96	112	Wireless-Docentes
17	GigabitEthernet 0/17	Access	96	112	Wireless-Docentes
18	GigabitEthernet 0/18	Access	10	20	Edi.Central Admin
19	GigabitEthernet 0/19	Access	10	20	Edi.Central Admin
20	GigabitEthernet 0/20	Access	10	20	Edi.Central Admin
21	GigabitEthernet 0/21	Access	10	20	Edi.Central Admin
22	GigabitEthernet 0/22	Access	10	20	Edi.Central Admin
23	GigabitEthernet 0/23	Access	10	20	Edi.Central Admin
24	GigabitEthernet 0/24	Access	96	112	Wireless-Docentes
25	GigabitEthernet 0/25	Access	96	112	Wireless-Docentes
26	GigabitEthernet 0/26	Access	96	112	Wireless-Docentes

27	GigabitEthernet 0/27	Access	96	112	Wireless-Docentes
28	GigabitEthernet 0/28	Access	96	112	Wireless-Docentes
29	GigabitEthernet 0/29	Access	96	112	Wireless-Docentes
30	GigabitEthernet 0/30	Access	96	112	Wireless-Docentes
31	GigabitEthernet 0/31	Access	96	112	Wireless-Docentes
32	GigabitEthernet 0/32	Access	96	112	Wireless-Docentes
33	GigabitEthernet 0/33	Access	96	112	Wireless-Docentes
34	GigabitEthernet 0/34	Access	96	112	Wireless-Docentes
35	GigabitEthernet 0/35	Access	96	112	Wireless-Docentes
36	GigabitEthernet 0/36	Access	96	112	Wireless-Docentes
37	GigabitEthernet 0/37	Access	2	6	AP - UTN
38	GigabitEthernet 0/38	Access	96	112	Wireless-Docentes
39	GigabitEthernet 0/39	Access	96	112	Wireless-Docentes
40	GigabitEthernet 0/40	Access	96	112	Wireless-Docentes
41	GigabitEthernet 0/41	Access	96	112	Wireless-Docentes
42	GigabitEthernet 0/42	Access	96	112	Wireless-Docentes
43	GigabitEthernet 0/43	Access	96	112	Wireless-Docentes
44	GigabitEthernet 0/44	Access	96	112	Wireless-Docentes
45	GigabitEthernet 0/45	Access	96	112	Wireless-Docentes
46	GigabitEthernet 0/46	Access	96	112	Wireless-Docentes
47	GigabitEthernet 0/47	Access	96	112	Wireless-Docentes
48	GigabitEthernet 0/48	Access	96	112	Wireless-Docentes
49	GigabitEthernet 0/49	Trunk	-	-	
50	GigabitEthernet 0/50	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 153.- *Descripción de las interfaces del Switch 02 del Edificio de Bienestar Estudiantil*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 02 DEL EDIFICIO DE BIENESTAR ESTUDIANTIL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	96	112	Wireless-Docentes
2	GigabitEthernet 0/2	Access	96	112	Wireless-Docentes
3	GigabitEthernet 0/3	Access	96	112	Wireless-Docentes
4	GigabitEthernet 0/4	Access	10	20	Edi.Central Admin.

5	GigabitEthernet 0/5	Access	10	20	Edi.Central Admin.
6	GigabitEthernet 0/6	Access	10	20	Edi.Central Admin.
7	GigabitEthernet 0/7	Access	10	20	Edi.Central Admin.
8	GigabitEthernet 0/8	Access	10	20	Edi.Central Admin.
9	GigabitEthernet 0/9	Access	10	20	Edi.Central Admin.
10	GigabitEthernet 0/10	Access	10	20	Edi.Central Admin.
11	GigabitEthernet 0/11	Access	10	20	Edi.Central Admin.
12	GigabitEthernet 0/12	Access	10	20	Edi.Central Admin.
13	GigabitEthernet 0/13	Access	10	20	Edi.Central Admin.
14	GigabitEthernet 0/14	Access	10	20	Edi.Central Admin.
15	GigabitEthernet 0/15	Access	10	20	Edi.Central Admin.
16	GigabitEthernet 0/16	Access	10	20	Edi.Central Admin.
17	GigabitEthernet 0/17	Access	10	20	Edi.Central Admin.
18	GigabitEthernet 0/18	Access	10	20	Edi.Central Admin.
19	GigabitEthernet 0/19	Access	10	20	Edi.Central Admin.
20	GigabitEthernet 0/20	Access	10	20	Edi.Central Admin.
21	GigabitEthernet 0/21	Access	10	20	Edi.Central Admin.
22	GigabitEthernet 0/22	Access	10	20	Edi.Central Admin.
23	GigabitEthernet 0/23	Access	10	20	Edi.Central Admin.
24	GigabitEthernet 0/24	Access	10	20	Edi.Central Admin.
25	GigabitEthernet 0/25	Access	10	20	Edi.Central Admin.
26	GigabitEthernet 0/26	Access	10	20	Edi.Central Admin.
27	GigabitEthernet 0/27	Access	10	20	Edi.Central Admin.
28	GigabitEthernet 0/28	Access	10	20	Edi.Central Admin.
29	GigabitEthernet 0/29	Access	10	20	Edi.Central Admin.
30	GigabitEthernet 0/30	Access	10	20	Edi.Central Admin.
31	GigabitEthernet 0/31	Access	10	20	Edi.Central Admin.
32	GigabitEthernet 0/32	Access	10	20	Edi.Central Admin.
33	GigabitEthernet 0/33	Access	10	20	Edi.Central Admin.
34	GigabitEthernet 0/34	Access	10	20	Edi.Central Admin.
35	GigabitEthernet 0/35	Access	10	20	Edi.Central Admin.
36	GigabitEthernet 0/36	Access	10	20	Edi.Central Admin.
37	GigabitEthernet 0/37	Access	10	20	Edi.Central Admin.
38	GigabitEthernet 0/38	Access	10	20	Edi.Central Admin.
39	GigabitEthernet 0/39	Access	10	20	Edi.Central Admin.

40	GigabitEthernet 0/40	Access	2	6	AP - UTN
41	GigabitEthernet 0/41	Access	10	20	Edi.Central Admin.
42	GigabitEthernet 0/42	Access	10	20	Edi.Central Admin.
43	GigabitEthernet 0/43	Trunk	-	-	
44	GigabitEthernet 0/44	Access	1	1	Libre
45	GigabitEthernet 0/45	Access	10	20	Edi.Central Admin.
46	GigabitEthernet 0/46	Access	10	20	Edi.Central Admin.
47	GigabitEthernet 0/47	Access	1	1	
48	GigabitEthernet 0/48	Access	10	20	Edi.Central Admin.
49	GigabitEthernet 0/49	Trunk	-	-	
50	GigabitEthernet 0/50	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 154.- *Descripción de las interfaces del Switch 03 del Edificio de Bienestar Estudiantil*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 03 DEL EDIFICIO DE BIENESTAR ESTUDIANTIL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	96	112	Wireless-Docentes
2	GigabitEthernet 0/2	Access	96	112	Wireless-Docentes
3	GigabitEthernet 0/3	Access	96	112	Wireless-Docentes
4	GigabitEthernet 0/4	Access	96	112	Wireless-Docentes
5	GigabitEthernet 0/5	Access	96	112	Wireless-Docentes
6	GigabitEthernet 0/6	Access	96	112	Wireless-Docentes
7	GigabitEthernet 0/7	Access	96	112	Wireless-Docentes
8	GigabitEthernet 0/8	Access	96	112	Wireless-Docentes
9	GigabitEthernet 0/9	Access	96	112	Wireless-Docentes
10	GigabitEthernet 0/10	Access	96	112	Wireless-Docentes
11	GigabitEthernet 0/11	Access	96	112	Wireless-Docentes
12	GigabitEthernet 0/12	Access	96	112	Wireless-Docentes
13	GigabitEthernet 0/13	Access	96	112	Wireless-Docentes
14	GigabitEthernet 0/14	Access	96	112	Wireless-Docentes
15	GigabitEthernet 0/15	Access	96	112	Wireless-Docentes
16	GigabitEthernet 0/16	Access	96	112	Wireless-Docentes
17	GigabitEthernet 0/17	Access	96	112	Wireless-Docentes

18	GigabitEthernet 0/18	Access	96	112	Wireless-Docentes
19	GigabitEthernet 0/19	Access	96	112	Wireless-Docentes
20	GigabitEthernet 0/20	Access	96	112	Wireless-Docentes
21	GigabitEthernet 0/21	Access	96	112	Wireless-Docentes
22	GigabitEthernet 0/22	Access	96	112	Wireless-Docentes
23	GigabitEthernet 0/23	Access	96	112	Wireless-Docentes
24	GigabitEthernet 0/24	Access	96	112	Wireless-Docentes
25	GigabitEthernet 0/25	Access	96	112	Wireless-Docentes
26	GigabitEthernet 0/26	Access	96	112	Wireless-Docentes
27	GigabitEthernet 0/27	Access	96	112	Wireless-Docentes
28	GigabitEthernet 0/28	Access	96	112	Wireless-Docentes
29	GigabitEthernet 0/29	Access	96	112	Wireless-Docentes
30	GigabitEthernet 0/30	Access	96	112	Wireless-Docentes
31	GigabitEthernet 0/31	Access	96	112	Wireless-Docentes
32	GigabitEthernet 0/32	Access	96	112	Wireless-Docentes
33	GigabitEthernet 0/33	Access	96	112	Wireless-Docentes
34	GigabitEthernet 0/34	Access	96	112	Wireless-Docentes
35	GigabitEthernet 0/35	Access	96	112	Wireless-Docentes
36	GigabitEthernet 0/36	Access	96	112	Wireless-Docentes
37	GigabitEthernet 0/37	Access	2	6	AP - UTN
38	GigabitEthernet 0/38	Access	96	112	Wireless-Docentes
39	GigabitEthernet 0/39	Access	96	112	Wireless-Docentes
40	GigabitEthernet 0/40	Access	96	112	Wireless-Docentes
41	GigabitEthernet 0/41	Access	96	112	Wireless-Docentes
42	GigabitEthernet 0/42	Access	96	112	Wireless-Docentes
43	GigabitEthernet 0/43	Access	96	112	Wireless-Docentes
44	GigabitEthernet 0/44	Access	96	112	Wireless-Docentes
45	GigabitEthernet 0/45	Access	96	112	Wireless-Docentes
46	GigabitEthernet 0/46	Access	96	112	Wireless-Docentes
47	GigabitEthernet 0/47	Access	96	112	Wireless-Docentes
48	GigabitEthernet 0/48	Access	96	112	Wireless-Docentes
49	GigabitEthernet 0/49	Trunk	-	-	Enlace SW-Rack02
50	GigabitEthernet 0/50	Trunk	-	-	Enlace SW-Rack02

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 155.- *Descripción de las interfaces del Switch 04 del Edificio de Bienestar Estudiantil*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 04 DEL EDIFICO DE BIENESTAR ESTUDIANTIL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	GigabitEthernet 0/1	Access	96	112	Wireless-Docentes
2	GigabitEthernet 0/2	Access	96	112	Wireless-Docentes
3	GigabitEthernet 0/3	Access	96	112	Wireless-Docentes
4	GigabitEthernet 0/4	Access	96	112	Wireless-Docentes
5	GigabitEthernet 0/5	Access	96	112	Wireless-Docentes
6	GigabitEthernet 0/6	Access	96	112	Wireless-Docentes
7	GigabitEthernet 0/7	Access	96	112	Wireless-Docentes
8	GigabitEthernet 0/8	Access	96	112	Wireless-Docentes
9	GigabitEthernet 0/9	Access	96	112	Wireless-Docentes
10	GigabitEthernet 0/10	Access	96	112	Wireless-Docentes
11	GigabitEthernet 0/11	Access	96	112	Wireless-Docentes
12	GigabitEthernet 0/12	Access	96	112	Wireless-Docentes
13	GigabitEthernet 0/13	Access	96	112	Wireless-Docentes
14	GigabitEthernet 0/14	Access	96	112	Wireless-Docentes
15	GigabitEthernet 0/15	Access	96	112	Wireless-Docentes
16	GigabitEthernet 0/16	Access	96	112	Wireless-Docentes
17	GigabitEthernet 0/17	Access	96	112	Wireless-Docentes
18	GigabitEthernet 0/18	Access	96	112	Wireless-Docentes
19	GigabitEthernet 0/19	Access	96	112	Wireless-Docentes
20	GigabitEthernet 0/20	Access	96	112	Wireless-Docentes
21	GigabitEthernet 0/21	Access	96	112	Wireless-Docentes
22	GigabitEthernet 0/22	Access	96	112	Wireless-Docentes
23	GigabitEthernet 0/23	Access	96	112	Wireless-Docentes
24	GigabitEthernet 0/24	Access	96	112	Wireless-Docentes
25	GigabitEthernet 0/25	Access	96	112	Wireless-Docentes
26	GigabitEthernet 0/26	Access	96	112	Wireless-Docentes
27	GigabitEthernet 0/27	Access	96	112	Wireless-Docentes
28	GigabitEthernet 0/28	Access	96	112	Wireless-Docentes
29	GigabitEthernet 0/29	Access	96	112	Wireless-Docentes
30	GigabitEthernet 0/30	Access	96	112	Wireless-Docentes

31	GigabitEthernet 0/31	Access	96	112	Wireless-Docentes
32	GigabitEthernet 0/32	Access	96	112	Wireless-Docentes
33	GigabitEthernet 0/33	Access	96	112	Wireless-Docentes
34	GigabitEthernet 0/34	Access	96	112	Wireless-Docentes
35	GigabitEthernet 0/35	Access	96	112	Wireless-Docentes
36	GigabitEthernet 0/36	Access	96	112	Wireless-Docentes
37	GigabitEthernet 0/37	Access	96	112	Wireless-Docentes
38	GigabitEthernet 0/38	Access	96	112	Wireless-Docentes
39	GigabitEthernet 0/39	Access	96	112	Wireless-Docentes
40	GigabitEthernet 0/40	Access	96	112	Wireless-Docentes
41	GigabitEthernet 0/41	Access	96	112	Wireless-Docentes
42	GigabitEthernet 0/42	Access	96	112	Wireless-Docentes
43	GigabitEthernet 0/43	Access	96	112	Wireless-Docentes
44	GigabitEthernet 0/44	Access	96	112	Wireless-Docentes
45	GigabitEthernet 0/45	Access	96	112	Wireless-Docentes
46	GigabitEthernet 0/46	Access	96	112	Wireless-Docentes
47	GigabitEthernet 0/47	Access	2	6	AP - UTN
48	GigabitEthernet 0/48	Trunk	-	-	Enlace SW-Rack02
49	GigabitEthernet 0/49	Trunk	-	-	Enlace SW-Rack02
50	GigabitEthernet 0/50	Access	96	112	Wireless-Docentes

Fuente: *Dirección de Desarrollo Tecnológico e Informático – UTN*

TABLA 156.- *Descripción de las interfaces del Switch 05 del Edificio de Bienestar Estudiantil*

DESCRIPCIÓN DE LAS INTERFACES DEL SWITCH 05 DEL EDIFICO DE BIENESTAR ESTUDIANTIL					
N°	Interfaz	SwitchPort Mode	Vlan Actual	Vlan Nueva	Descripción
1	FastEthernet 1/1	Access	96	112	Wireless-Docentes
2	FastEthernet 1/2	Access	96	112	Wireless-Docentes
3	FastEthernet 1/3	Access	96	112	Wireless-Docentes
4	FastEthernet 1/4	Access	96	112	Wireless-Docentes
5	FastEthernet 1/5	Access	96	112	Wireless-Docentes
6	FastEthernet 1/6	Access	96	112	Wireless-Docentes

7	FastEthernet 1/7	Access	96	112	Wireless-Docentes
8	FastEthernet 1/8	Access	96	112	Wireless-Docentes
9	FastEthernet 1/9	Access	96	112	Wireless-Docentes
10	FastEthernet 1/10	Access	96	112	Wireless-Docentes
11	FastEthernet 1/11	Access	96	112	Wireless-Docentes
12	FastEthernet 1/12	Access	96	112	Wireless-Docentes
13	FastEthernet 1/13	Access	96	112	Wireless-Docentes
14	FastEthernet 1/14	Access	96	112	Wireless-Docentes
15	FastEthernet 1/15	Access	96	112	Wireless-Docentes
16	FastEthernet 1/16	Access	96	112	Wireless-Docentes
17	FastEthernet 1/17	Access	96	112	Wireless-Docentes
18	FastEthernet 1/18	Access	96	112	Wireless-Docentes
19	FastEthernet 1/19	Access	96	112	Wireless-Docentes
20	FastEthernet 1/20	Access	96	112	Wireless-Docentes
21	FastEthernet 1/21	Access	96	112	Wireless-Docentes
22	FastEthernet 1/22	Access	96	112	Wireless-Docentes
23	FastEthernet 1/23	Access	96	112	Wireless-Docentes
24	FastEthernet 1/24	Trunk	-	-	

Fuente: *Dirección de Desarrollo Tecnológico e Informático - UTN*

ANEXO 04

INSTALACIÓN DE CITRIX XEN-SERVER

Para la instalación de Citrix Xen-Server debemos descargarnos su instalador desde la página oficial de Citrix, para lo cual pide registrarse y es toralmente gratis.

http://www.citrix.es/downloads/xenserver/product-software/xenserver-62.html

Dar click en el botón Download en la opción XenServer 6.2.0 Base Installation ISO, Imagen 58.

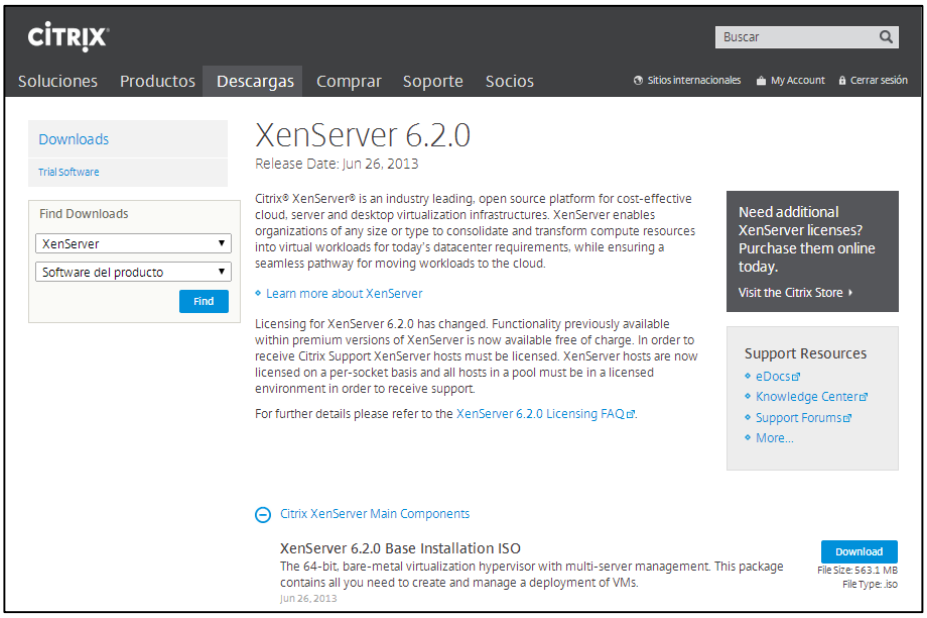


IMAGEN 58.- *Pagina WEB para descargar la ISO de Citrix Xen-Server*

Fuente: *http://www.citrix.es/downloads/xenserver/product-software/xenserver-62.html*

Antes de proceder con la instalación debemos ver que el equipo para ser el servidor Citrix Xen debe cumplir con los siguientes requerimientos:

- ✓ Uno o más CPU de 64bits x86; mínimo CPU de 1.5GHz; recomendado CPU de 2GHz o más.
- ✓ Memoria RAM de 2GB mínimo; 4GB recomendado.
- ✓ Disco Duro de 16GB mínimo; 60GB recomendado.
- ✓ Interfaz de red de 100Mbps mínimo; 1000Mbps recomendado.

Luego de revisar que el equipo donde se instalará Xen-Server cumple con los requerimientos previos y tener nuestro instalador descargado y grabado en un disco, se debe configurar el equipo para que arranque desde el DVD-ROM, lo cual se configura en la BIOS del equipo. Al ingresar y arrancar el disco de instalación se muestra la pantalla de inicio de instalación de Xen-Server, véase Imagen 59.

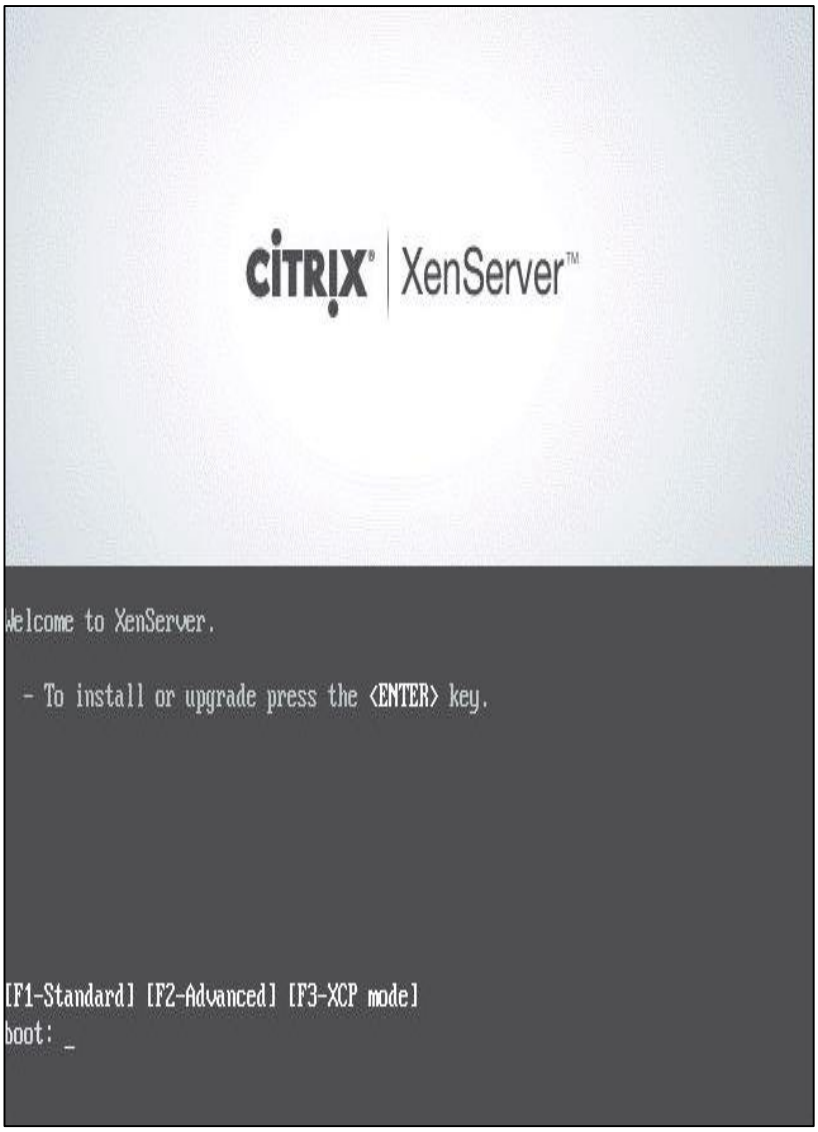


IMAGEN 59.- *Página de bienvenida al instalador de Citrix XenServer*
Fuente: *Instalación de Citrix XenServer*

El asistente de instalación realiza una revisión de hardware y varios componentes del equipo para continuar con la instalación. Seleccionar el idioma del teclado que en este caso será español. Véase Imagen 60.

IMAGEN 60.- *Selección del idioma teclado en español*

Fuente: *Instalación de Citrix XenServer*

Aparece un mensaje de advertencia en el cual se debe confirmar que se borrará todo el contenido del disco duro, para ello seleccionar OK. Véase Imagen 61.

IMAGEN 61.- *Mensaje de advertencia para borrar el contenido del disco duro*

Fuente: *Instalación de Citrix XenServer*

Aceptar el contrato de licencia de instalación EULA, véase Imagen 62.

IMAGEN 62.- *Contrato de Licencia de Usuario Final*

Fuente: *Instalación de Citrix XenServer*

Si al momento de la instalación aparece la pantalla mostrada en la Imagen 63, se debe habilitar la virtualización en el BIOS del equipo.

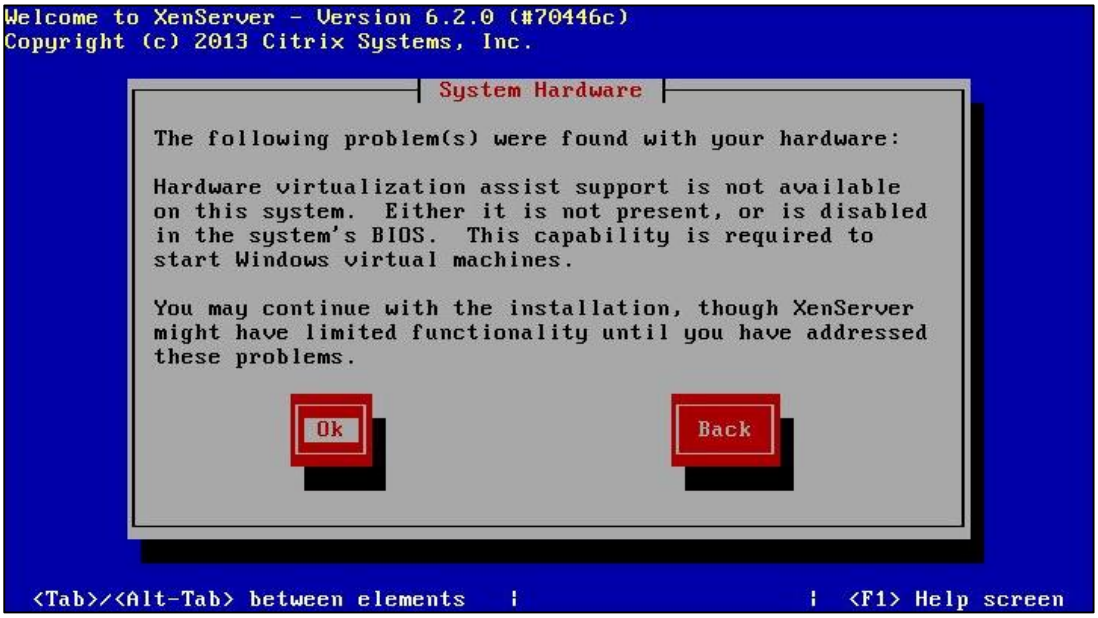


IMAGEN 63.- *Advertencia para la virtualización en el equipo servidor*

Fuente: *Instalación de Citrix XenServer*

Se debe escoger el Disco Duro en el cual se va a guardar las máquinas virtuales, en este caso se deja por defecto el disco existente. Véase la Imagen 64.

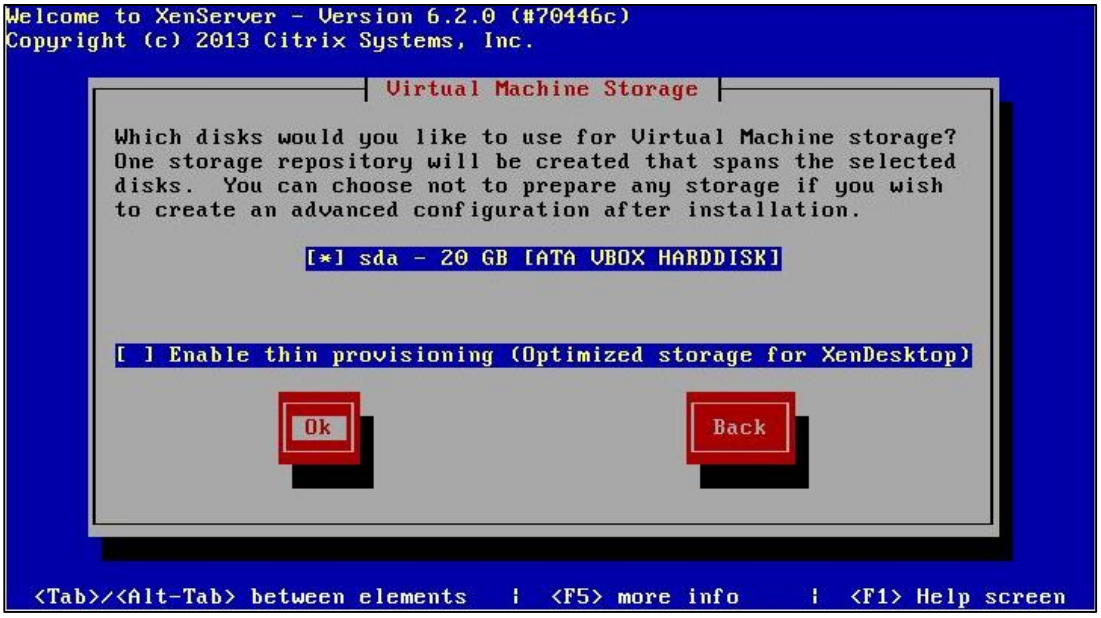


IMAGEN 64.- *Selección del disco duro para storage de las máquinas virtuales*
Fuente: *Instalación de Citrix XenServer*

Seleccionar el disco de instalación, tal como se indica en la Imagen 65.

IMAGEN 65.- *Selección del origen de instalación*
Fuente: *Instalación de Citrix XenServer*

Para que la instalación sea rápida y solo instale XenServer sin ninguna aplicación extra, se escoge la opción no, tal como se observa en la Imagen 66.

IMAGEN 66.- *Selección de los paquetes suplementarios de XenServer*
Fuente: *Instalación de Citrix XenServer*

Cuando se realiza la instalación desde un CD o DVD el asistente siempre preguntará si se desea realizar la revisión del disco para que no existan fallas en la instalación. En este caso obviaremos este procedimiento seleccionando skip. Véase la Imagen 67.

IMAGEN 67.- *Verificación del disco de instalación*
Fuente: *Instalación de Citrix XenServer*

Ingresar la contraseña para el súper usuario root, la cual debe ser de mínimo 6 caracteres. Véase la Imagen 68.

IMAGEN 68.- *Ingreso de la contraseña para el usuario root*

Fuente: *Instalación de Citrix XenServer*

Configurar la tarjeta de red ya sea el caso de usar DHCP o especificar manualmente la IP, en este caso se ha especificado una IP para el servidor XenServer, tal como se indica en la Imagen 69.

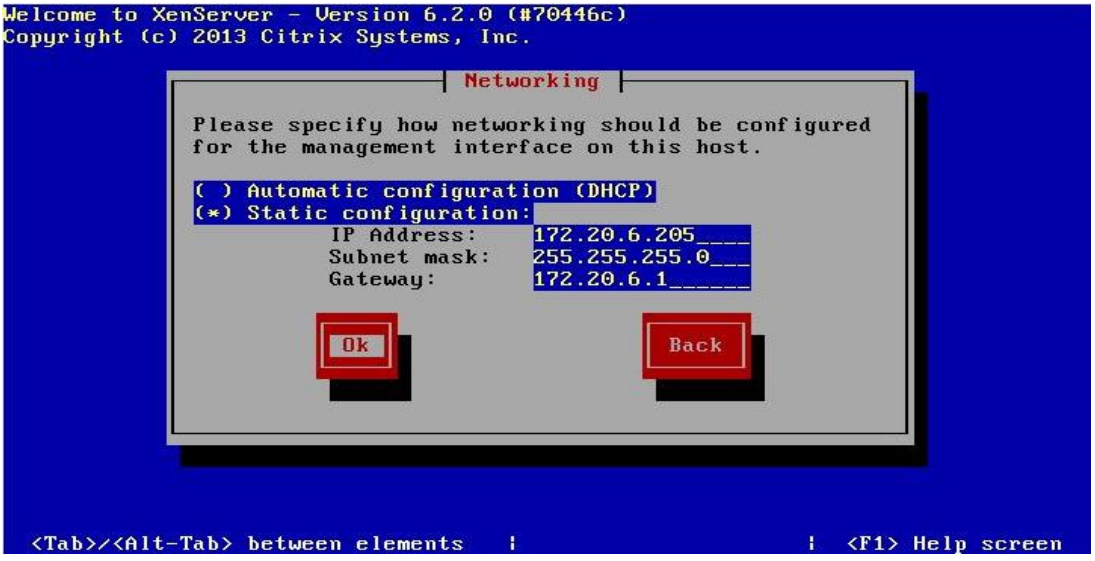


IMAGEN 69.- *Especificación de la IP del servidor*

Fuente: *Instalación de Citrix XenServer*

Se debe configurar el Nombre del Servidor así como su servidor DNS que en este caso se coloca la IP del DNS de la Universidad, tal como se muestra en la Imagen 70.

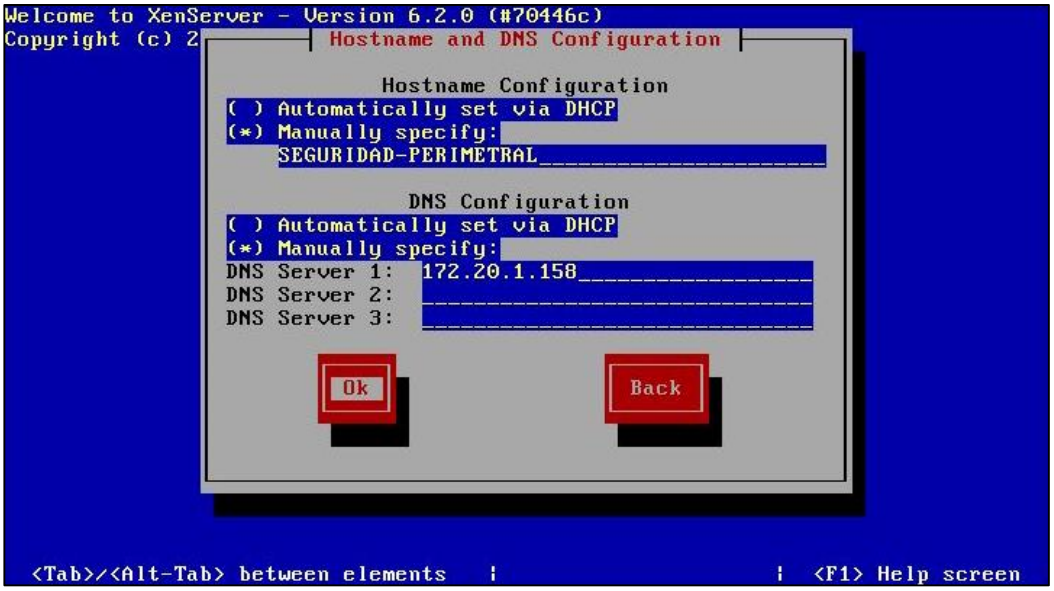


IMAGEN 70.- *Configuración del Nombre y servidor DNS del Servidor XenServer*

Fuente: *Instalación de Citrix XenServer*

Seleccionar el área geográfica donde se encuentra el servidor, en este caso América. Véase la Imagen 71.

IMAGEN 71.- *Selección del área geográfica*

Fuente: *Instalación de Citrix XenServer*

Seleccionar la ciudad más cercana a la localidad en la que se encuentra, dado el caso de que no existe Ibarra (Ciudad en la que me encuentro) ni Quito (Capital de Ecuador) seleccionar Bogotá, ya que se encuentran en el mismo huso horario. Véase la Imagen 72.

IMAGEN 72.- *Selección de la ciudad más cercana a la localidad*

Fuente: *Instalación de Citrix XenServer*

En caso de tener un servidor NTP para la coordinación de la hora en los equipos de red se debe seleccionar la opción Using NTP, en este caso al no poseer el servidor NTP se configurará manualmente la fecha y la hora. Tal como se observa la Imagen 73.

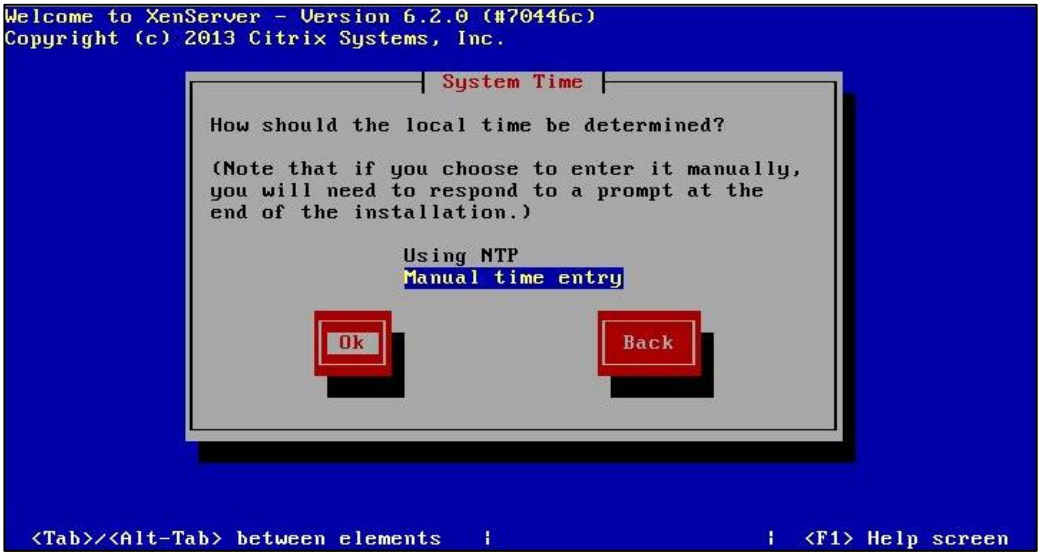


IMAGEN 73.- *Selección del tipo de configuración de la fecha y hora*

Fuente: *Instalación de Citrix XenServer*

Seleccionar la opción para iniciar con la instalación de XenServer en el servidor. Tal como se muestra en la Imagen 74.

IMAGEN 74.- *Inicio de instalación de XenServer*
Fuente: *Instalación de Citrix XenServer*

Durante la instalación el asistente solicitara que se configure manualmente la fecha y hora del servidor, tal como se observa en la Imagen 75.

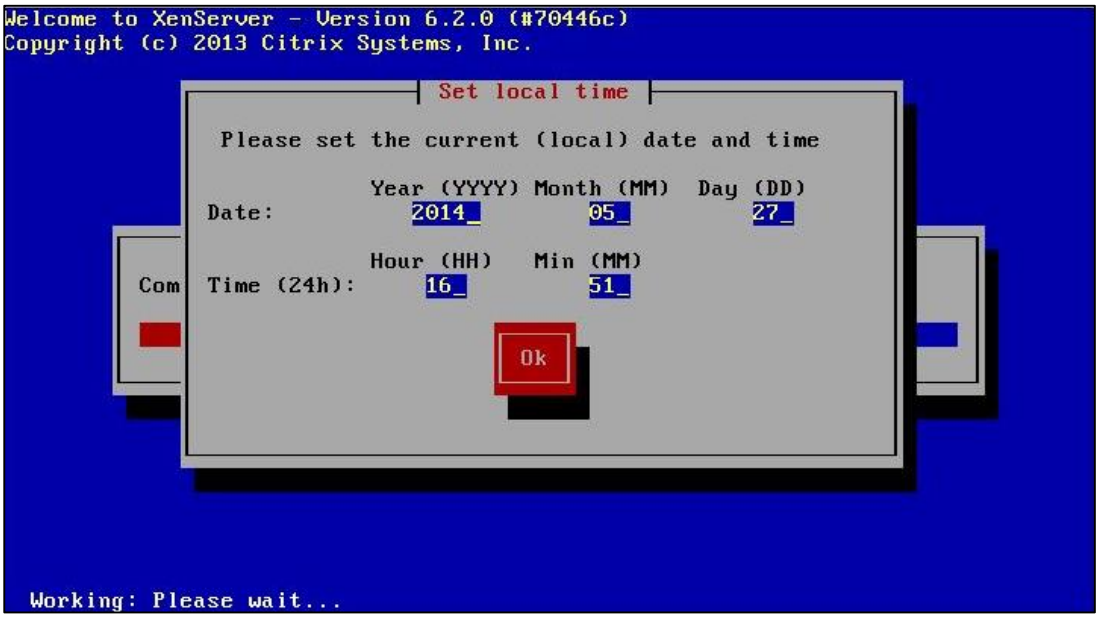


IMAGEN 75.- *Configuración de la fecha y hora del servidor*
Fuente: *Instalación de Citrix XenServer*

Luego de la instalación se muestra la pantalla de finalización tal como en la Imagen 76, se debe retirar el disco de instalación y seleccionar ok.

IMAGEN 76.- *Finalización de la instalación de XenServer*
Fuente: *Instalación de Citrix XenServer*

Posterior a la instalación el servidor se reiniciará automáticamente y al iniciar se mostrara la pantalla que se ve en la Imagen 77.

IMAGEN 77.- *Pantalla de inicio de Citrix XenServer*
Fuente: *Servidor de Virtualización Citrix XenServer*

En la Imagen 78 se muestra la pantalla de inicio y configuraciones del servidor XenServer:

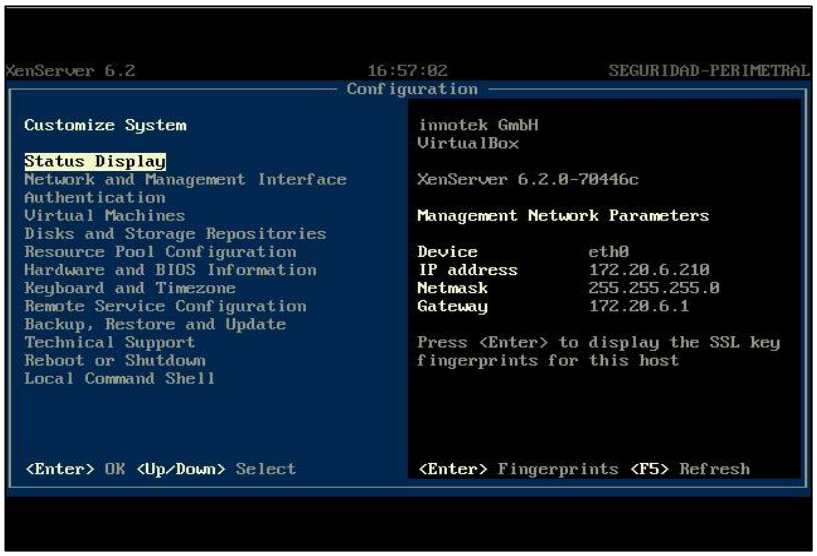


IMAGEN 78.- *Pantalla de inicio del servidor de virtualización XenServer*
Fuente: *Servidor de virtualización Citrix XenServer*

Para la administración del servidor de virtualización Citrix XenServer es necesario realizarlo desde un computador mediante la herramienta XenCenter, la cual permite administrar varios servidores desde un mismo computador. Para ello este computador debe cumplir con varios requisitos:

- ✓ Sistema operativo Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2012, Windows Server 2008, Windows Server 2003
- ✓ .NET Framework versión 3.5
- ✓ CPU de 750 MHz mínimo, recomendado 1GHz o superior
- ✓ Memoria RAM de 1 GB mínimo, recomendado 2GB o más
- ✓ Espacio en el disco de 100MB mínimo
- ✓ Tarjeta de red NIC de 100Mbps o superior
- ✓ Resolución de pantalla de 1024x768 pixeles mínimo

Luego de comprobar que el computador donde se instalará la herramienta XenCenter cumpla con los requerimientos establecidos se debe acceder a un navegador WEB y digitar la IP del servidor XenServer mediante HTTPS. Al momento de ingresar vía web al servidor aparece el mensaje de advertencia de un sitio no seguro para lo cual se debe agregar la verificación de sitio seguro para el navegador, en esta caso Mozilla Firefox, tal como se muestra en la Imagen 79.

IMAGEN 79.- *Verificación de conexión segura en el navegador WEB*
Fuente: *Servidor de virtualización Citrix XenServer*

Luego de verificar la conexión el servidor muestra las opciones de descarga de XenCenter, como se muestra en la Imagen 80. Es necesario descargar XenCenter installer.

IMAGEN 80.- *Opciones de descarga de XenCenter*
Fuente: *Servidor de Virtualización Citrix XenServer*

Posterior a descargar el instalador de XenCenter, se debe instalarlo en la computadora que administrará la virtualización del servidor. La pantalla de Inicio al asistente de instalación será como la que se muestra en la figura 81.

IMAGEN 81.- *Pantalla de inicio a la instalación de XenCenter*

Fuente: *Instalación de Citrix XenCenter*

Seleccionar el directorio donde se guardara el archivo de instalación de XenCenter, véase la Imagen 82.

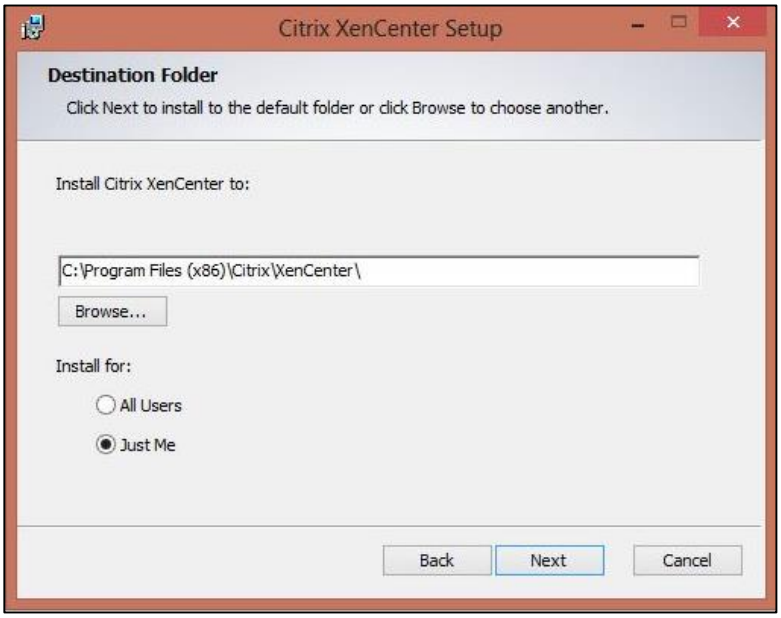


IMAGEN 82.- *Directorio de instalación de XenCenter*

Fuente: *Instalación de Citrix XenCenter*

Seleccionar la opción Install para proceder con la instalación del administrador de servidores de virtualización XenCenter. Véase la Imagen 83.

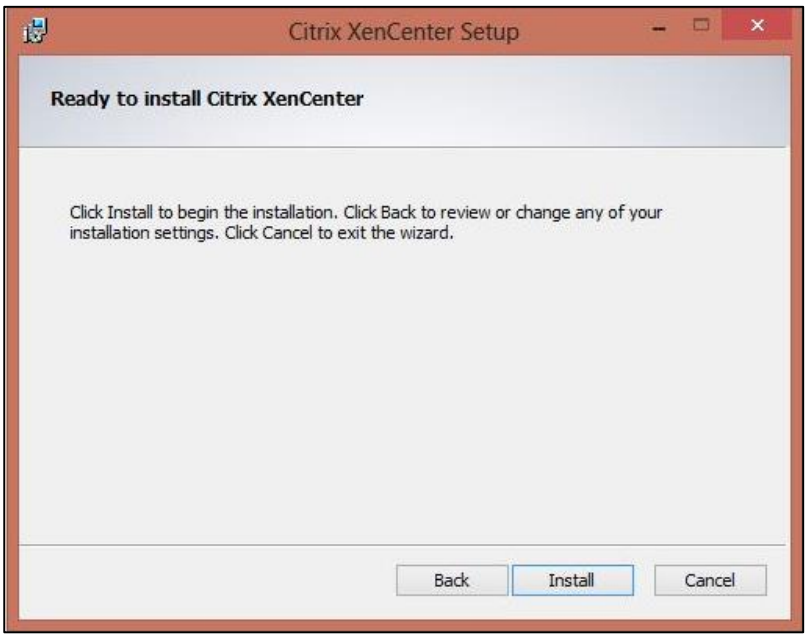


IMAGEN 83.- *Inicio de la Instalación de XenCenter*
Fuente: *Instalación de Citrix XenCenter*

Por último seleccionar finish para dar por terminado la instalación de XenCenter, tal como se ve en la Imagen 84.

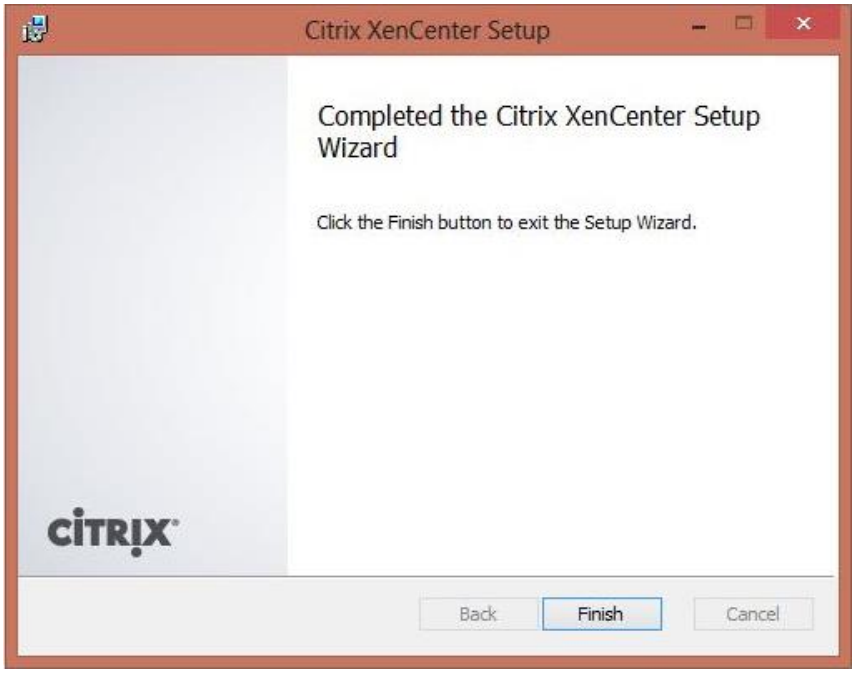


IMAGEN 84.- *Finalización de la instalación de XenCenter*
Fuente: *Instalación de Citrix XenCenter*

Luego de la instalación de la herramienta de administración de servidores de virtualización, se procede a la interconexión entre XenCenter y XenServer. Para ello se abre el administrador, e indicará la pantalla tal cual se muestra en la Imagen 85.

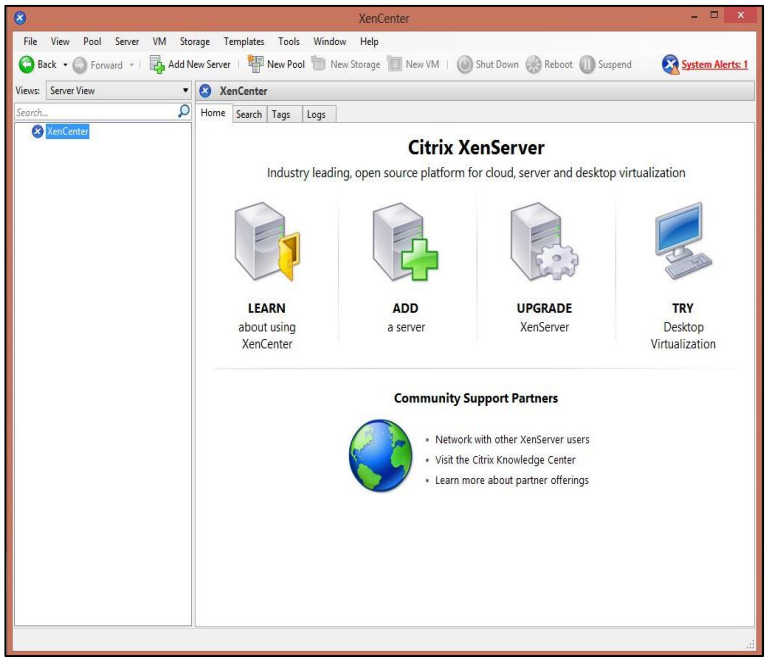


IMAGEN 85.- *Pantalla de inicio de XenCenter*

Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Seleccionar Add New Server, para agregar el servidor en el cual se ha instalado el software de virtualización XenServer, y aparecerá una ventana en la cual se debe agregar la IP del servidor así como su usuario root y la contraseña del mismo. Véase la Imagen 86.

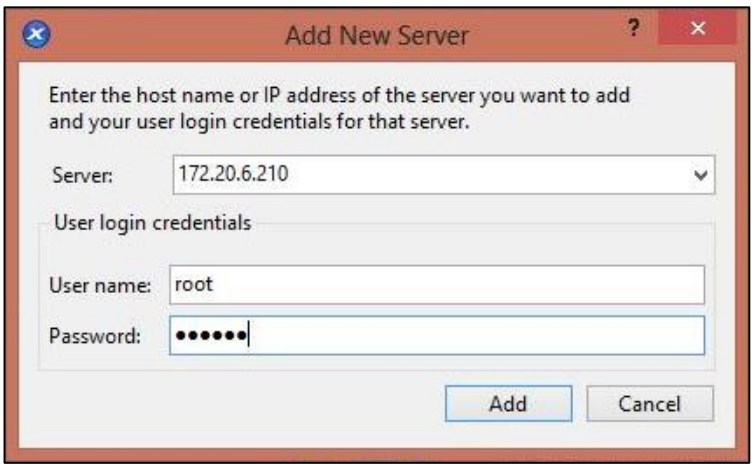


IMAGEN 86.- *Ingreso de IP, usuario y contraseña del servidor XenServer*

Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Luego de realizar una conexión exitosa entre el administrador XenCenter y el servidor XenServer, éste último se mostrará en la pantalla del administrador. En la cual también se muestra la pestaña “Search” en la que indica un resumen de las características de almacenamiento del servidor. Véase Imagen 87.

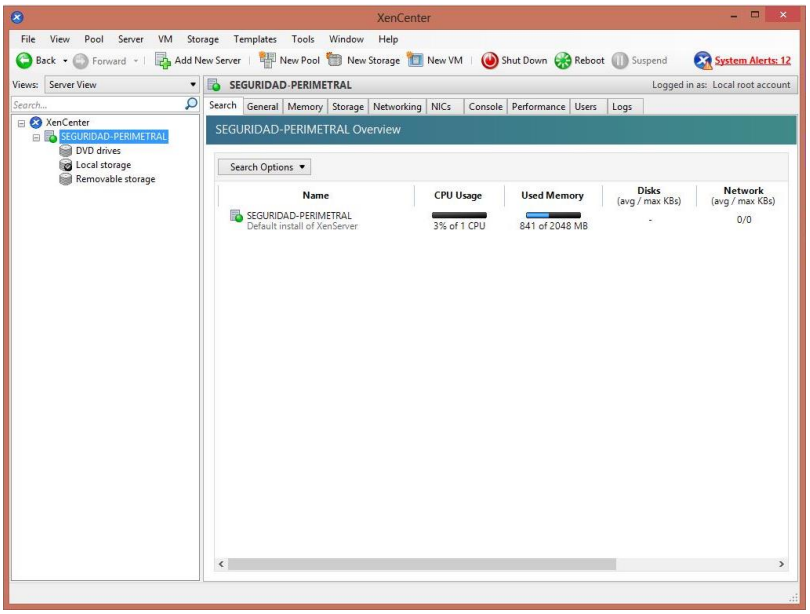


IMAGEN 87.- *Resumen de las características de almacenamiento del servidor*

Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

En la pestaña “General” se muestra la información completa sobre el servidor que se está administrando. Véase la Imagen 88.

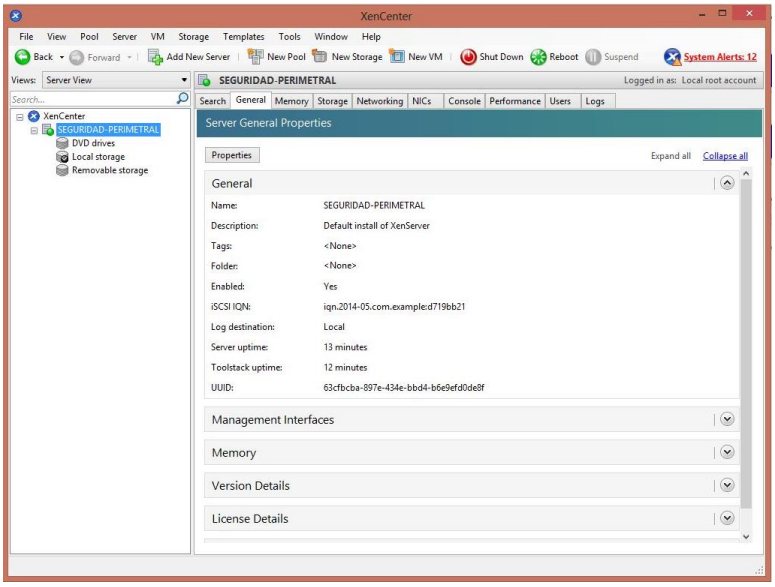


IMAGEN 88.- Información acerca del servidor administrado

Fuente: Administrador de servidores de virtualización Citrix XenServer

En la pestaña “Memory” se muestra la capacidad de la memoria RAM y cuanto de ella ha sido utilizada. Véase la Imagen 89

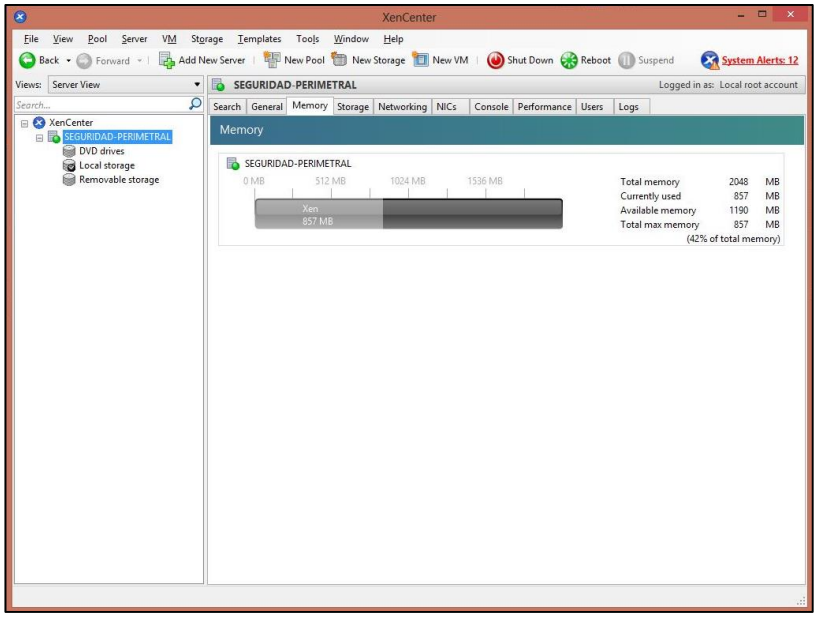


IMAGEN 89.- *Información acerca de la capacidad de la memoria RAM*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

En la pestaña “Storage” se muestra las características del almacenamiento que posee el servidor XenServer y que nos servirá para las máquinas virtuales, tal como se muestra en la Imagen 90.

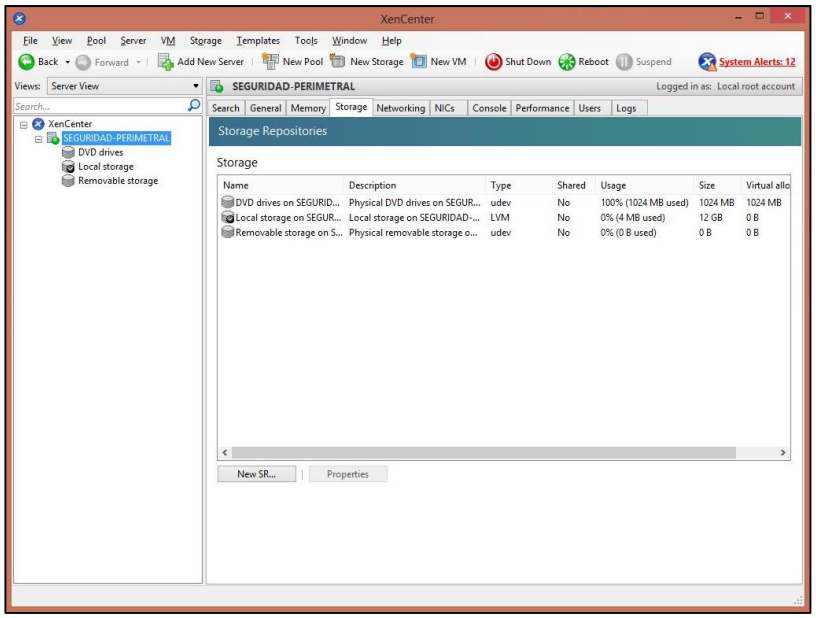


IMAGEN 90.- *Información del disco de almacenamiento del servidor*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

En la pestaña “Networking” se muestra las interfaces de red virtuales que posee el servidor, si un servidor necesita más interfaces es cuestión de agregarlas. Véase la Imagen 91.

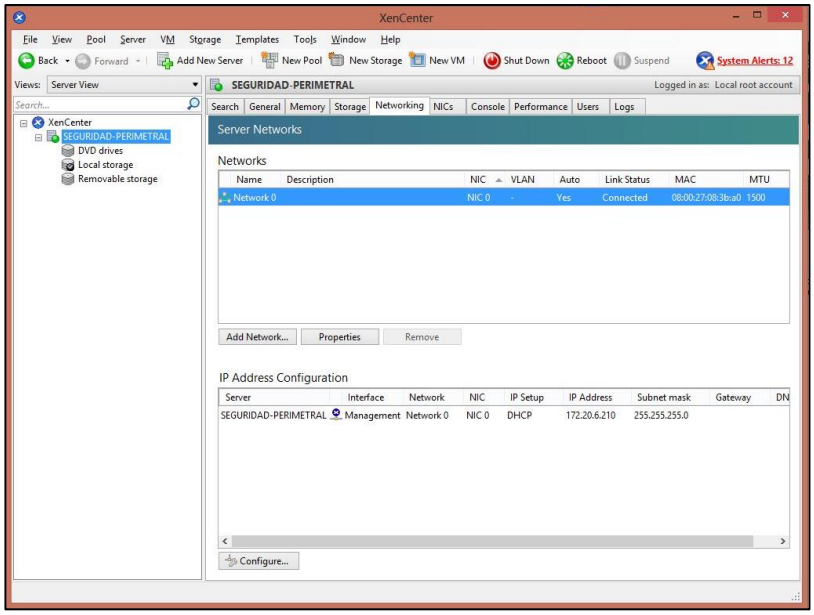


IMAGEN 91.- *Información acerca de las interfaces virtuales de red del servidor*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

En la pestaña “NICs” se muestra los adaptadores de red físicos que posee el servidor. Véase la Imagen 92.

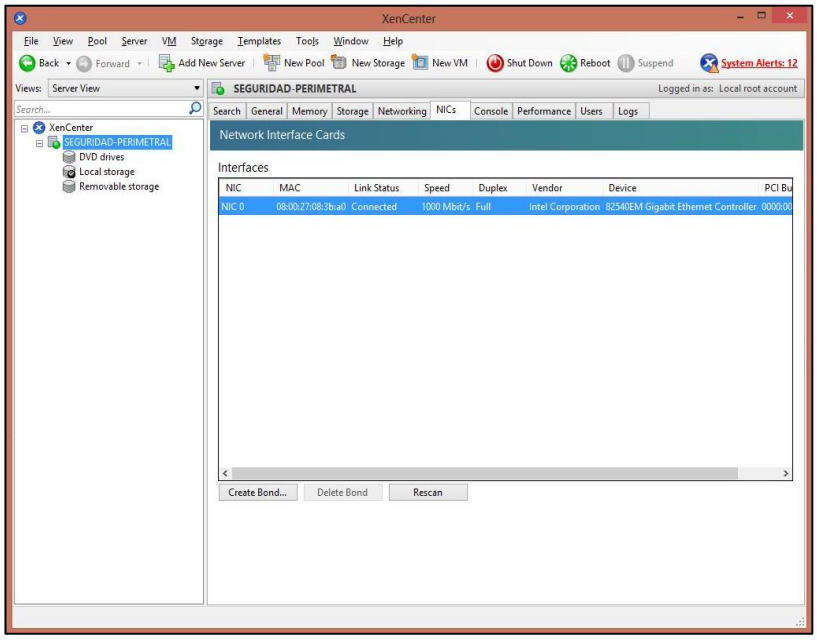


IMAGEN 92.- *Información acerca de los adaptadores de red físicos del servidor*
Fuente: *Administrador de servidores de virtualización Citrix XenServer*

En la pestaña “Console” se puede realizar la conexión hacia el servidor XenServer mediante la consola. Tal como se muestra en la Imagen 93.

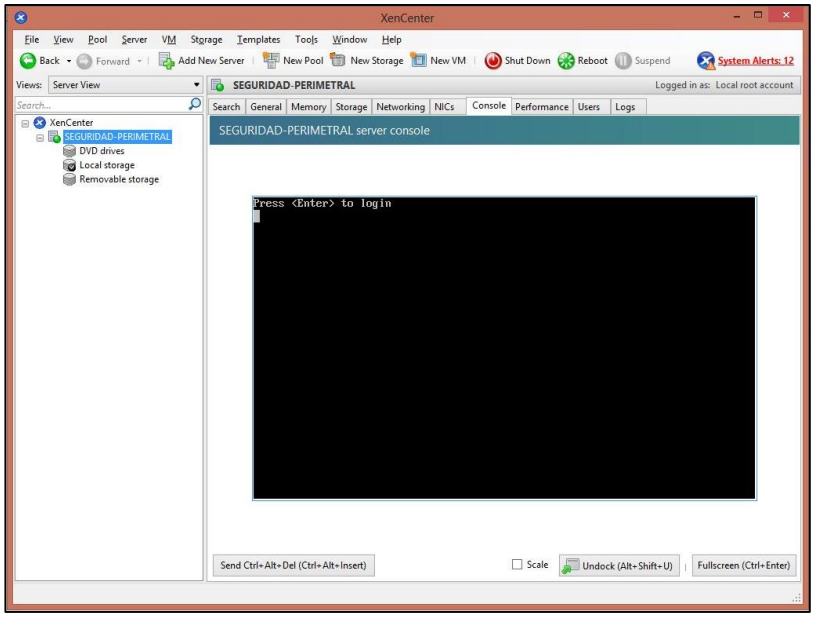


IMAGEN 93.- *Consola para administración del servidor XenServer*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

En la pestaña “Performance” se muestra las gráficas en tiempo real sobre el rendimiento del servidor XenServer, tal como se observa en la Imagen 94.

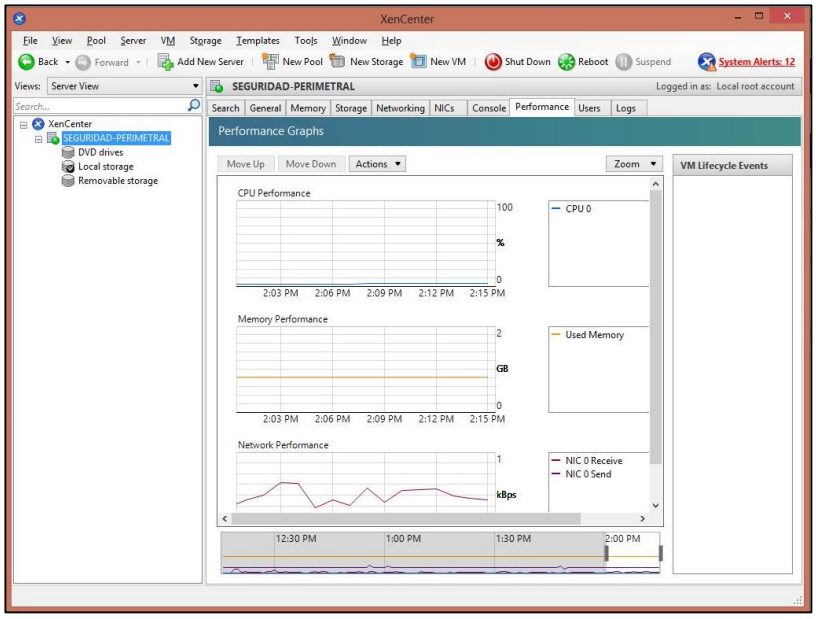


IMAGEN 94.- *Información acerca del rendimiento del servidor*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

En la pestaña “Users” se indica la información acerca de los diferentes usuarios que tienen acceso al servidor XenServer. Véase la Imagen 95.

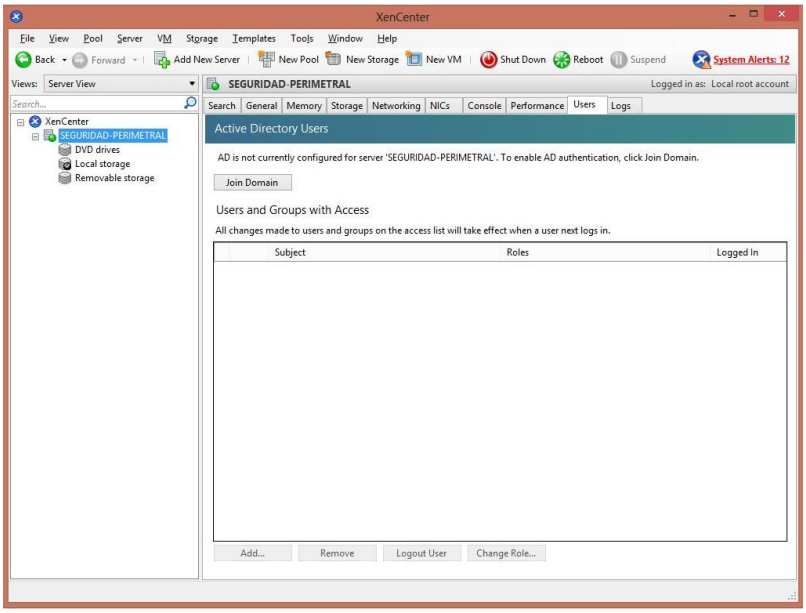


IMAGEN 95.- *Información de los diferentes usuarios que tienen acceso al servidor*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Por último la pestaña “Logs” muestra los diferentes eventos que sucedan en el servidor XenServer, tal como se muestra en la Imagen 96.

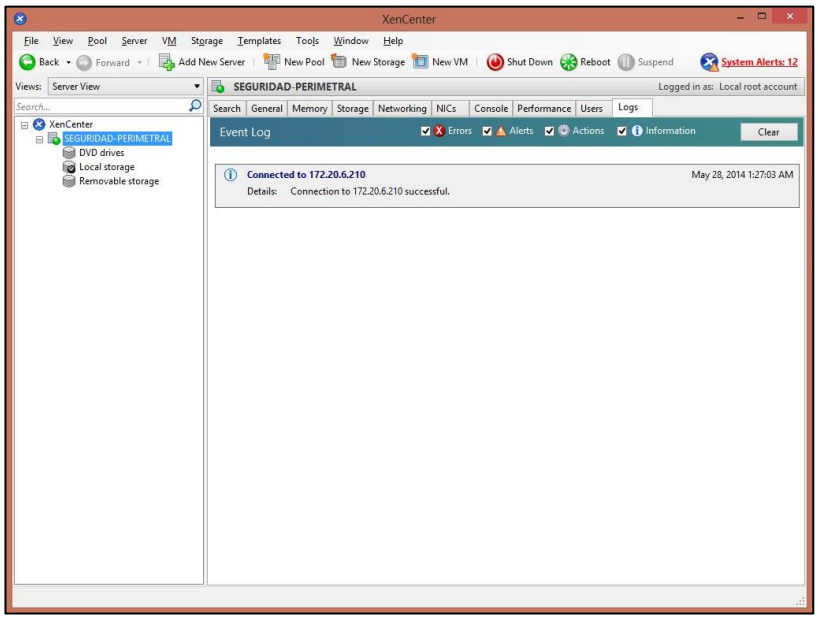


IMAGEN 96.- *Información de los eventos que ocurren en el servidor*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Luego de haber revisado las características del servidor las cuales se presentan en las diferentes pestañas del administrador XenCenter, es necesario la creación de las máquinas virtuales necesarias. Las características de procesamiento, y almacenamiento dependerá de qué tipo de servicio se va a implementar.

Para la creación de la máquina virtual se debe dar click derecho en el servidor XenServer añadido, y seleccionar New VM, tal como se indica en la Imagen 97.

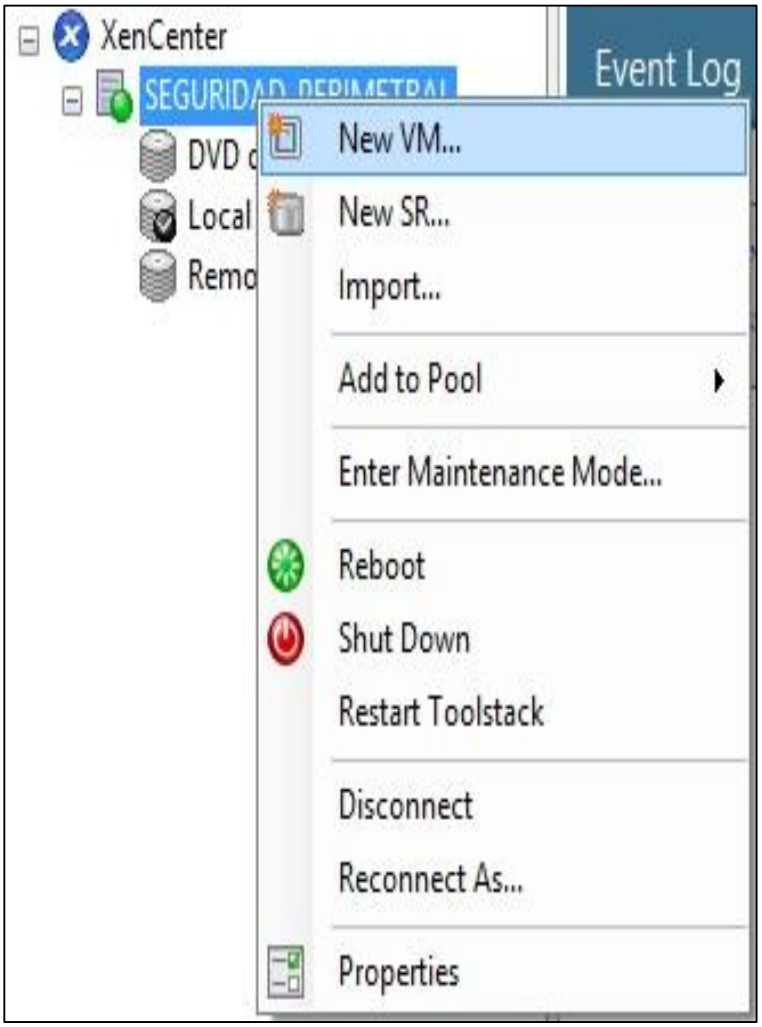


IMAGEN 97.- *Creación de la máquina virtual.*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Al momento de abrir el asistente de creación de máquinas virtuales aparece una pantalla similar a la Imagen 98, en donde se debe seleccionar el tipo de sistema operativo que se va a instalar en dicha máquina virtual, para este caso se escogió la opción CentOS 6.

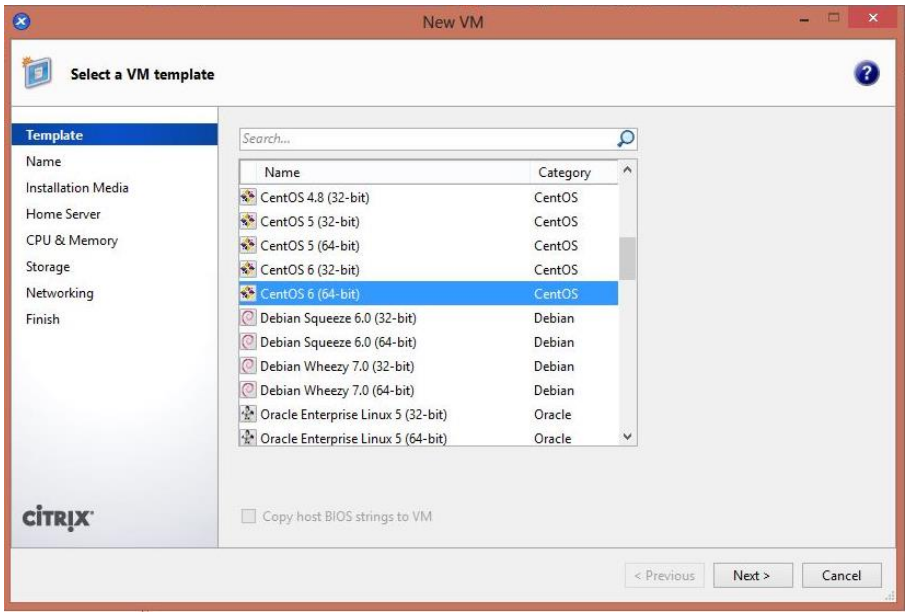


IMAGEN 98.- *Selección del sistema operativo a instalar en la máquina virtual*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Ingresar el nombre a la nueva máquina virtual, para este caso se va a implementar un servidor FIREWALL es por ello que se ingresa este nombre. Véase la Imagen 99.

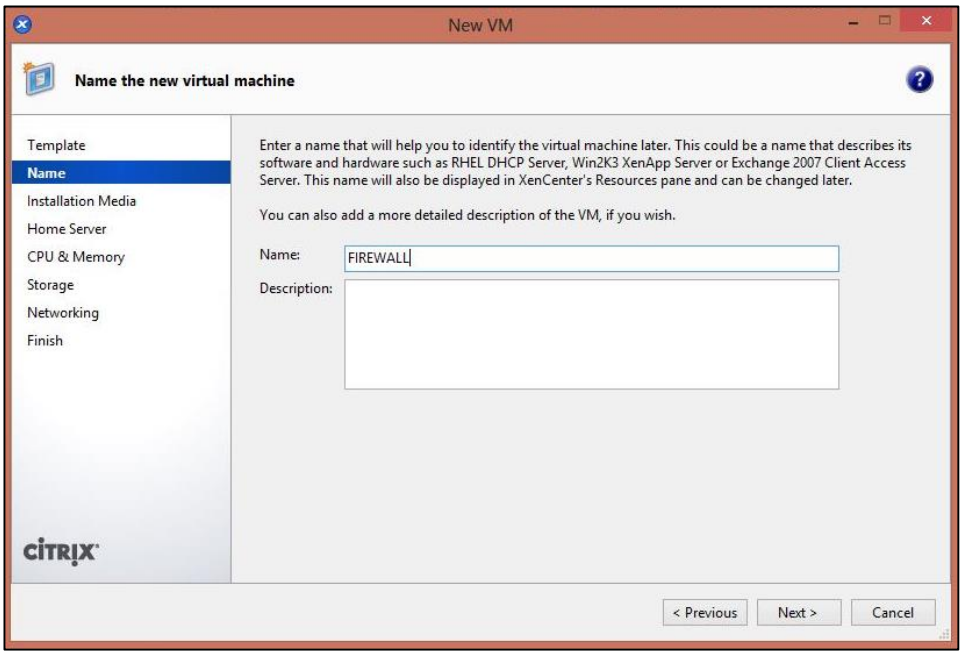


IMAGEN 99.- *Ingreso del nombre de la nueva máquina virtual*
Fuente*: Administrador de servidores de virtualización Citrix XenServer*

Seleccionar la localización del medio de instalación del sistema operativo, para este caso la instalación se la realizara desde el DVD-ROM del servidor por ello la opción a escoger es el drive DVD 0 del servidor XenServer. Véase la Imagen 100.

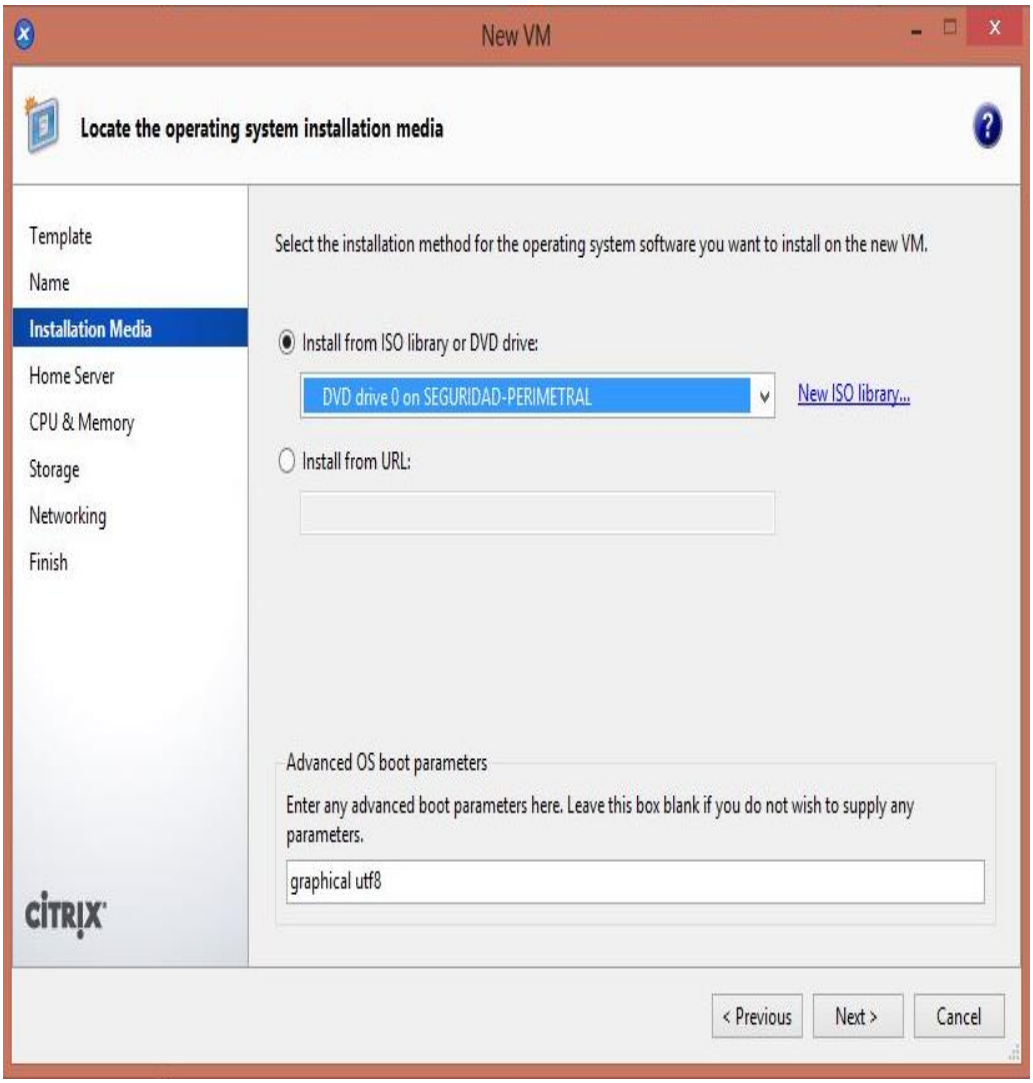


IMAGEN 100.- *Selección del medio de instalación del sistema operativo para la nueva máquina virtual*

Fuente: *Administrador de servidores de virtualización Citrix XenCente*

Cuando se tienen varios servidores XenServer añadidos al administrador XenCenter se debe seleccionar en cuál de los servidores se va a alojar la máquina virtual. En este caso al existir un solo servidor se lo deja por defecto, como se observa en la Imagen 101.

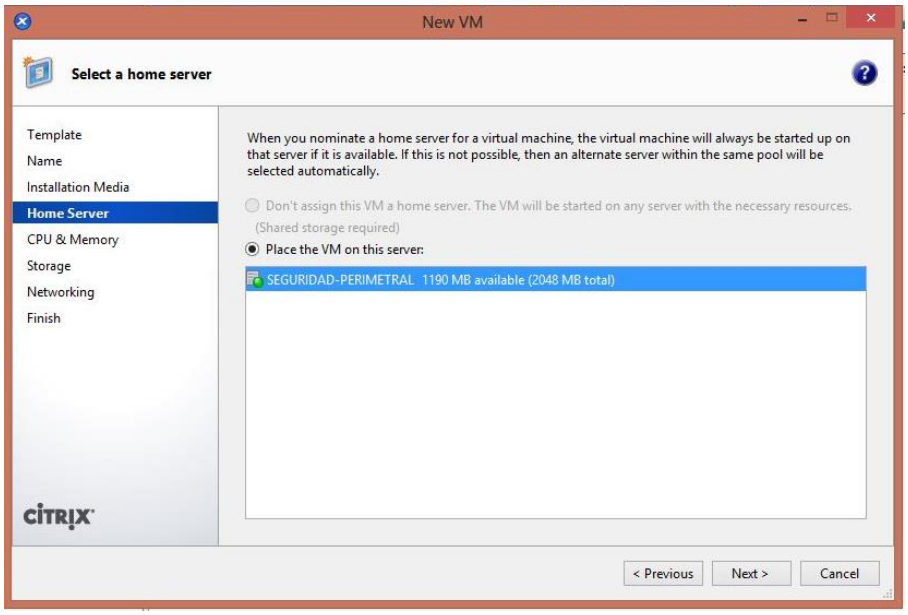


IMAGEN 101.- *Selección del servidor en el que se alojará la nueva máquina virtual*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Seleccionar el número de CPU y la cantidad de memoria que se le asignará a la nueva máquina virtual. Imagen 102.

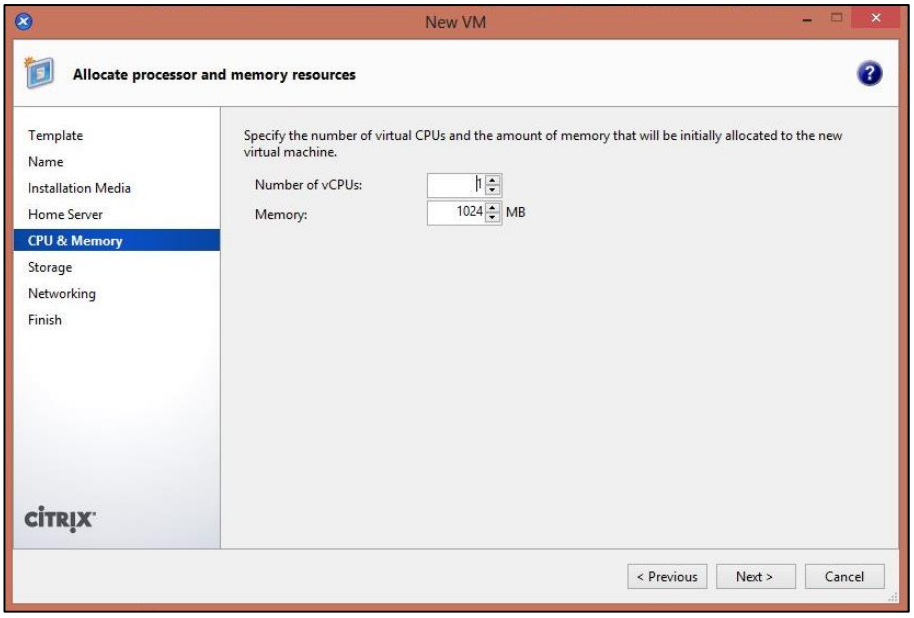


IMAGEN 102.- *Asignación de CPU y memoria para la nueva máquina virtual*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Se debe asignar los discos virtuales para la nueva máquina virtual. Imagen 103.

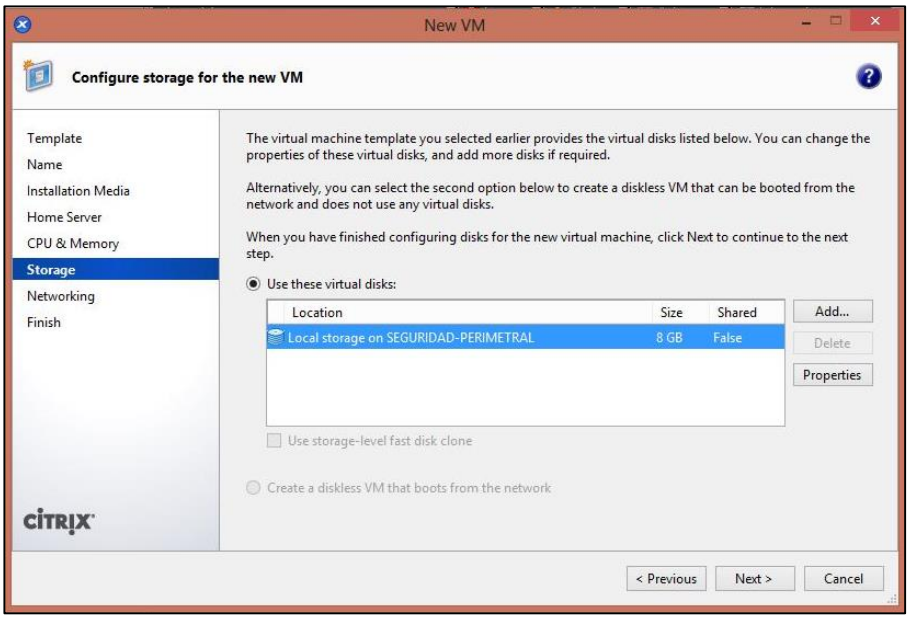


IMAGEN 103.- *Asignación de los discos virtuales para la nueva máquina virtual*

Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Asignar las tarjetas de red virtuales, en este caso práctico es necesario tres tarjetas de red, tal como se indica en la Imagen 104.

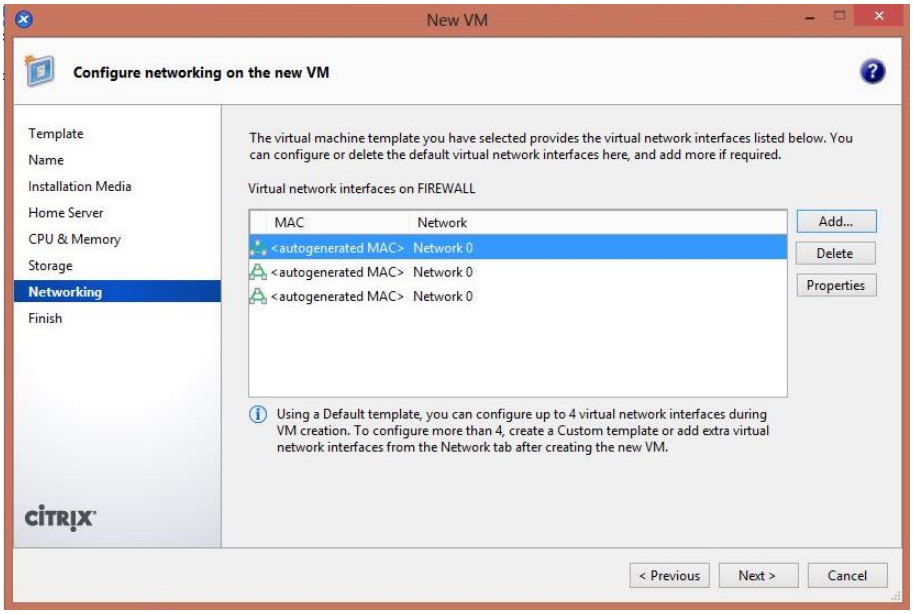


IMAGEN 104.- *Asignación de las tarjetas de red virtuales para la nueva máquina virtual*

Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Finalmente se muestra un resumen de las características de la nueva máquina virtual, selecciona la opción “Create Now”. Imagen 105.

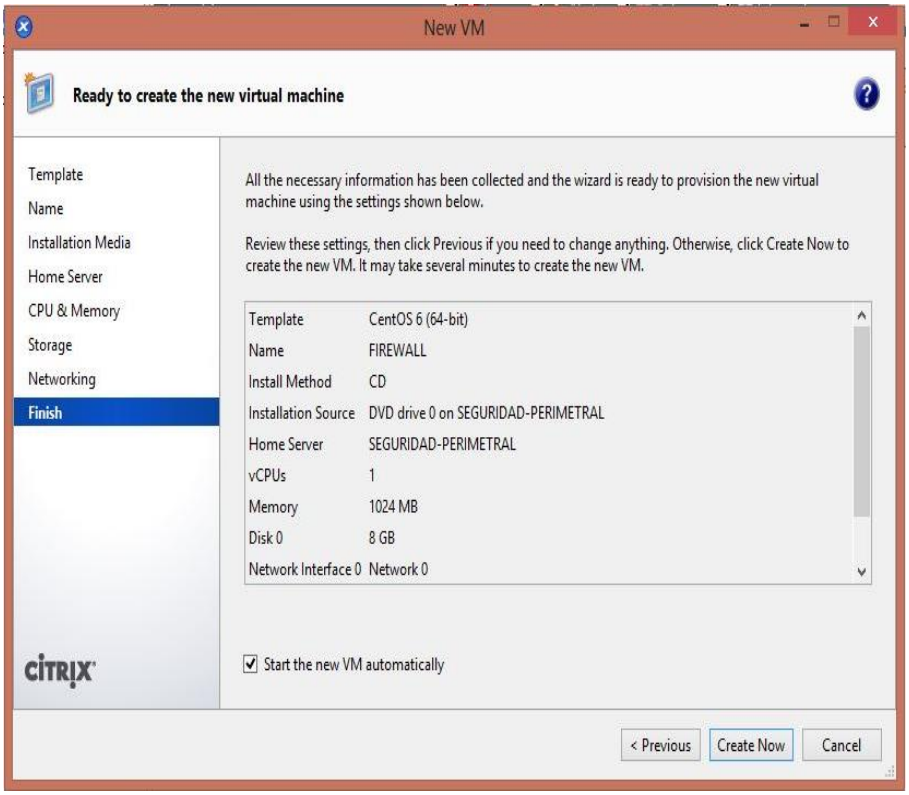


IMAGEN 105.- *Resumen de la nueva máquina virtual a crearse*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

Luego de la creación de la máquina virtual se observa que se ha creado el ícono de la misma. Imagen 106. Ahora ya se puede acceder a la máquina virtual y realizar las configuraciones que se desee.

IMAGEN 106.- *Máquina virtual creada en el servidor XenServer*
Fuente: *Administrador de servidores de virtualización Citrix XenCenter*

ANEXO 05

INSTALACIÓN DEL SISTEMA OPERATIVO “CENTOS”

El sistema operativo CentOS se encuentra en la versión 6,5 y al ser software libre y de código abierto se puede descargar desde la página web, véase la Imagen 107:

http://mirror.centos.org/centos/6/isos/

Seleccione de acuerdo a la arquitectura a utilizarse ya sea i386 o x86_64 y descargue solamente el DVD1.

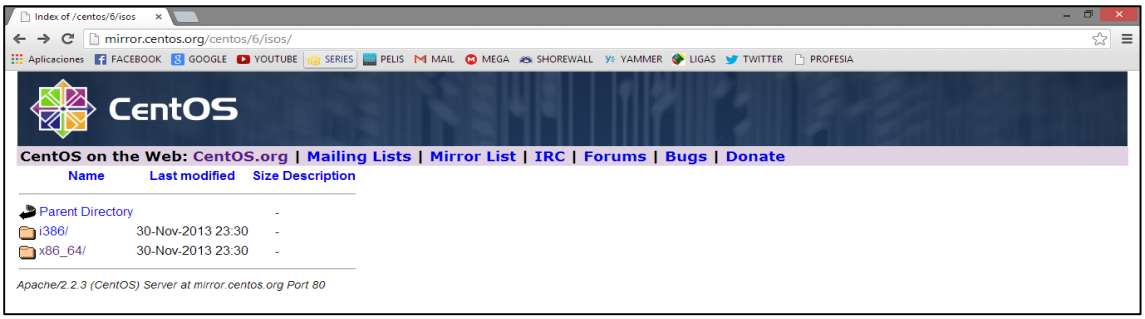


IMAGEN 107.- *Site para descargar las imágenes ISO de CentOS*
Fuente.- *mirror.centos.org/centos/6/isos/*

Si el sistema operativo CentOS se va a instalar en un equipo como sistema anfitrión es necesario que se configure el arranque del equipo y que se lo realice desde el DVD, esto se lo realiza en la BIOS del equipo; si se lo va a instalar en una máquina virtual es necesario conocer el directorio donde se encuentra guardado la imagen iso del DVD de CentOS. Luego de arrancar la imagen iso del instalador aparece la Imagen 108:

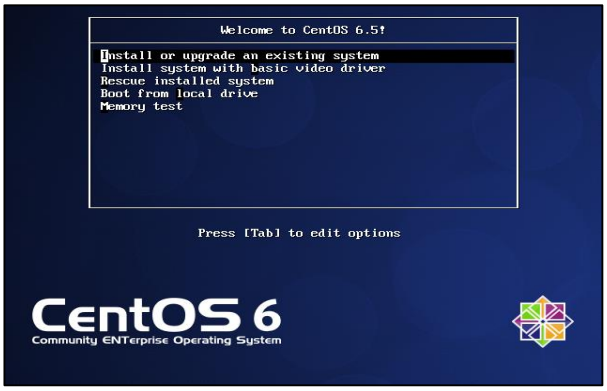


IMAGEN 108.- *Diferentes opciones de instalación de CentOS 6.5*
Fuente: *Instalación del Sistema Operativo CentOS*

Al momento de arrancar el DVD la primera pantalla pregunta si se desea revisar si el disco de instalación se encuentra en óptimas condiciones; si se va a instalar en una máquina virtual se puede omitir este paso pero si se lo realiza en un equipo o servidor es necesario realizarlo, véase Imagen 109.

IMAGEN 109.- *Revisión del disco de instalación*
Fuente: *Instalación del Sistema Operativo CentOS*

Luego de proceder con la revisión del disco o al saltar esta opción, comenzará automáticamente la instalación del Sistema Operativo CentOS, observe la Imagen 110.

IMAGEN 110.- *Inicio de instalación*
Fuente*: Instalación del Sistema Operativo Centos*

Seleccione el idioma en el que se va a instalar el Sistema Operativo, en este caso se lo realiza en *Spanish (Español)*, tal como se indica en la Imagen 111.

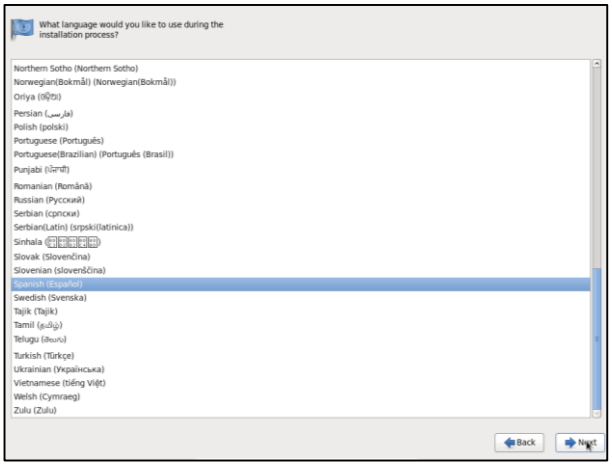


IMAGEN 111.- *Selección del idioma del Sistema Operativo*
Fuente: *Instalación del Sistema Operativo Centos*

Seleccione el idioma del teclado, en este caso se lo realizara con un teclado *Latinoamericano*, véase la Imagen 112.

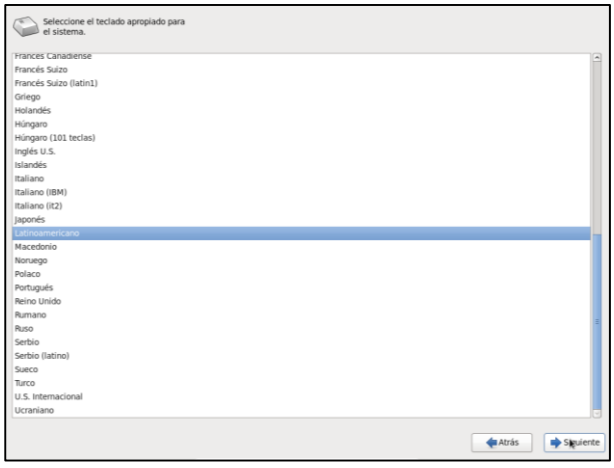


IMAGEN 112.- *Selección del idioma del teclado*
Fuente: *Instalación del Sistema Operativo CentOS*

La instalación se la realizará en discos duros del equipo, es por ello que se selecciona la primera opción *Dispositivos de almacenamiento básicos*, cuando se va a instalar una red de área de almacenamiento (SAN) se selecciona la opción *Dispositivos de almacenamiento especializados*, Imagen 113.

IMAGEN 113.- *Selección del tipo de dispositivo de almacenamiento*
Fuente: *Instalación del Sistema Operativo Centos*

El asistente de instalación despliega un mensaje de advertencia como en la Imagen 114, en el cual indica que pueden existir datos en el disco duro del equipo a instalarse, selecciona *Si, descarte todos los datos*.

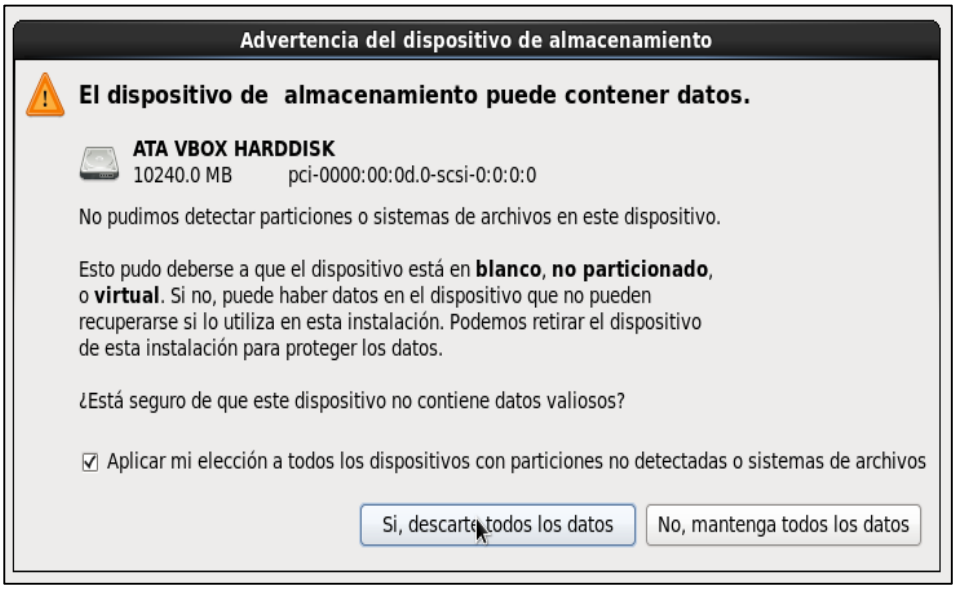


IMAGEN 114.- *Advertencia del dispositivo de almacenamiento*
Fuente: *Instalación del Sistema Operativo Centos*

Digite el nombre del host que tendrá el equipo y será para su identificación en una red. Tal como se muestra en la Imagen 115.

IMAGEN 115.- *Nombre del Host*
Fuente: *Instalación del Sistema Operativo Centos*

Seleccione la zona horaria donde se encuentra el equipo y se recomienda dejar habilitada la opción *El reloj del sistema utiliza UTC* (Tiempo Universal Coordinado). Para este caso se selecciona la zona horaria de *Guayaquil*, como en la Imagen 116.

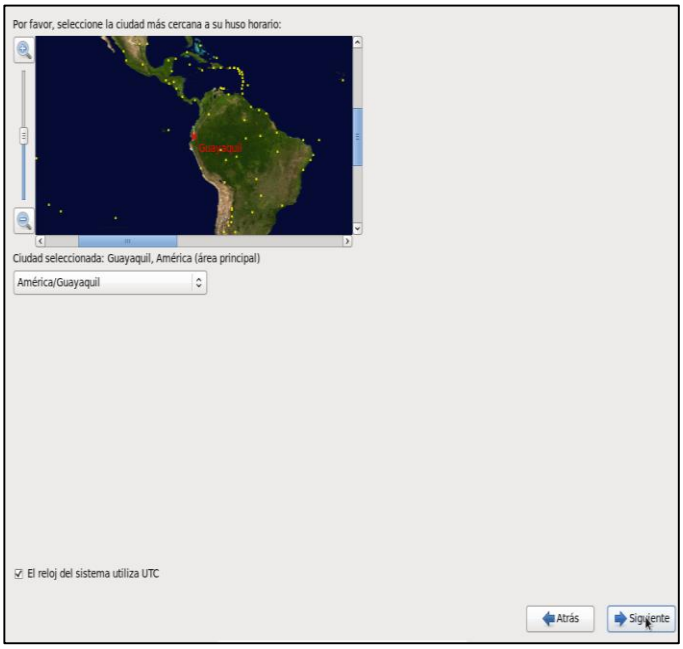


IMAGEN 116.- *Selección de la zona horaria*
Fuente: *Instalación del Sistema Operativo Centos*

Proceder a la configuración y confirmación de la contraseña de la cuenta del usuario *root,* Imagen 117, la cual se utiliza para la administración del sistema.

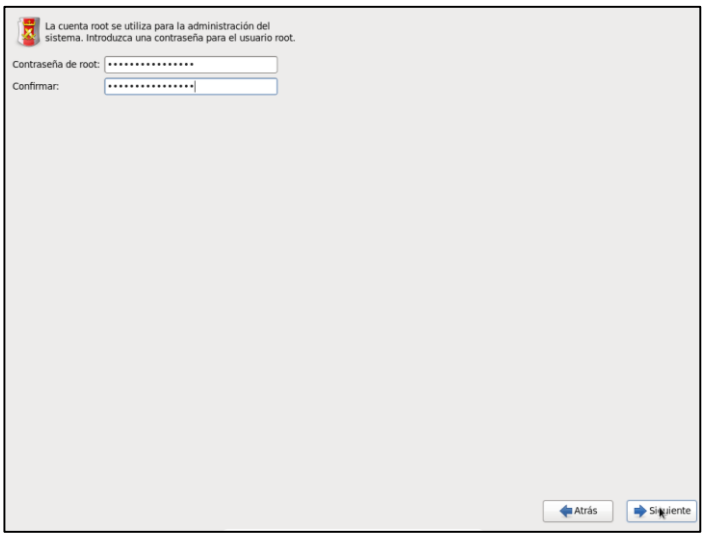


IMAGEN 117.- *Configuración de la contraseña del usuario root*

Fuente: *Instalación del Sistema Operativo Centos*

Seleccione el tipo de instalación que se desea, en este caso se selecciona la opción *Usar todo el espacio*, Imagen 118, lo cual indica al asistente de instalación formatear el disco duro y asignar los espacios necesarios para cada una de las particiones del sistema Operativo.

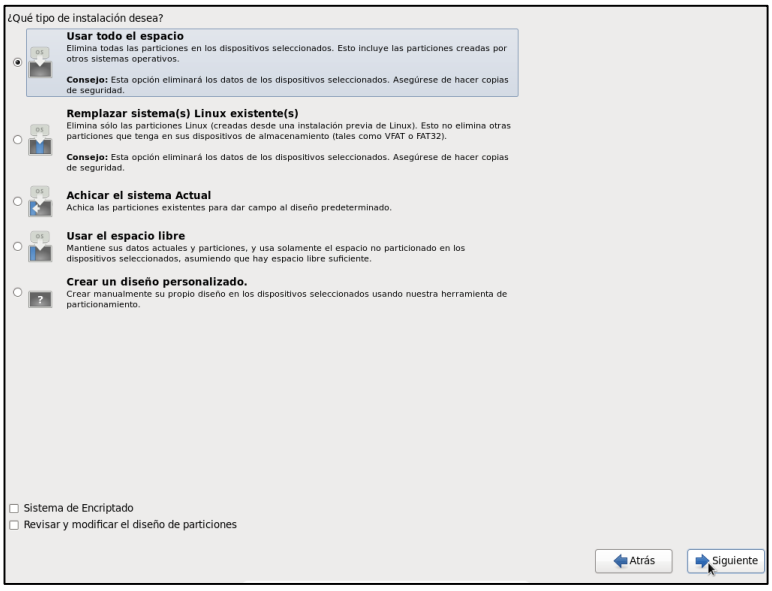


IMAGEN 118.- *Tipo de instalación*

Fuente: *Instalación del Sistema Operativo Centos*

El asistente despliega un mensaje de advertencia en la cual se debe confirmar los cambios en el disco seleccionando la opción *Escribir cambios al disco*, como en la Imagen 119.

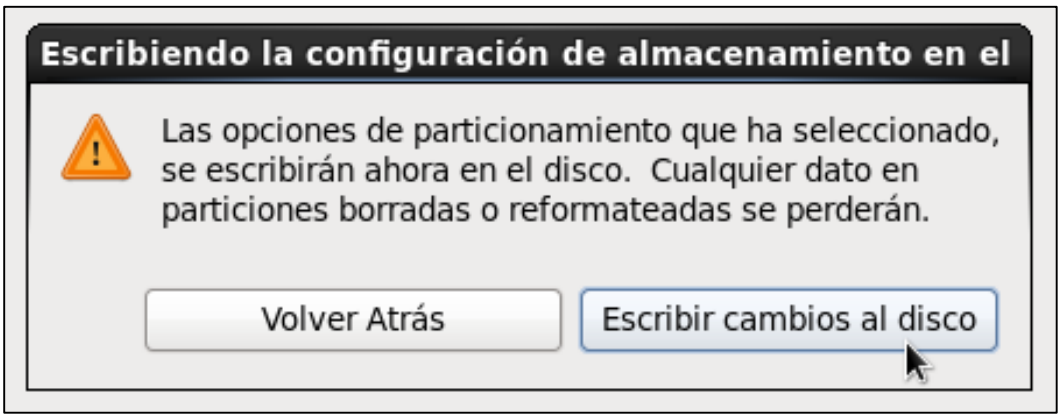


IMAGEN 119.- *Confirmación de escritura en el disco*
Fuente: *Instalación del Sistema Operativo Centos*

Seleccione el tipo de instalación que requiera, en este caso se selecciona la opción *Desktop* en la cual el sistema operativo se instala en el modo visual de escritorio, como se indica en la Imagen 120.

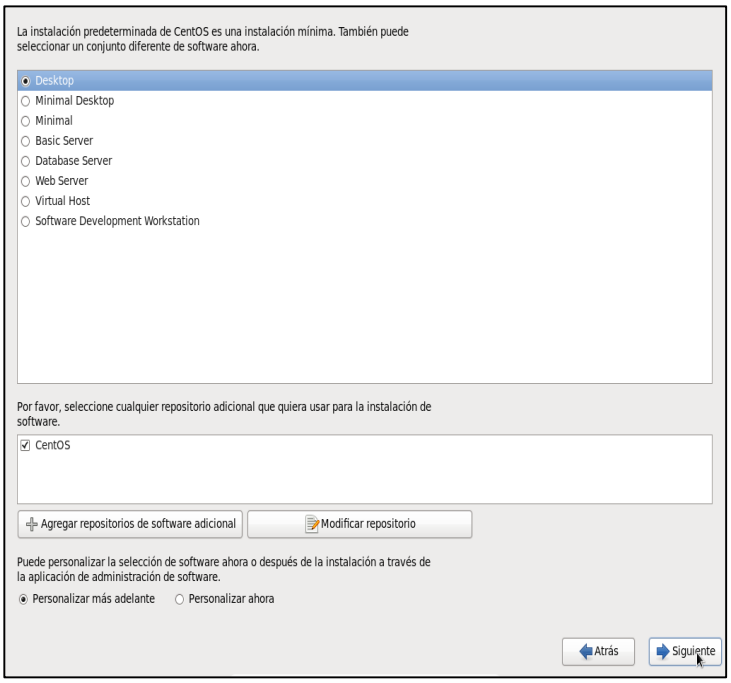


IMAGEN 120.- *Selección del tipo de instalación del sistema operativo*
Fuente: *Instalación del Sistema Operativo Centos*

Luego de realizar todos estos pasos el asistente procederá con la instalación del Sistema Operativo, y simplemente es cuestión de esperar. Imagen 121.

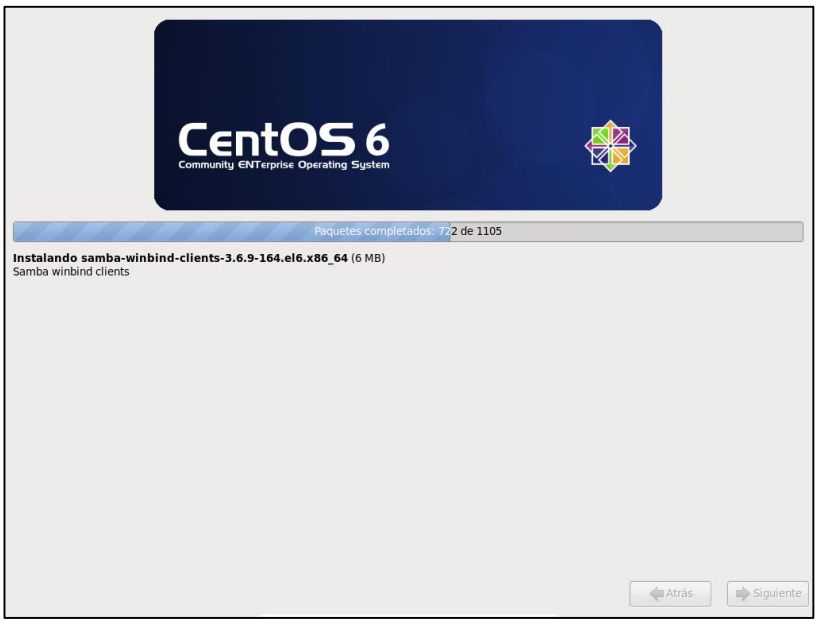


IMAGEN 121.- *Sistema operativo instalándose*
Fuente: *Instalación del Sistema Operativo Centos*

Transcurrido unos minutos el asistente de instalación solicitará que se reinicie el equipo, por lo tanto seleccionamos la opción *Reiniciar* y se retira el DVD de instalación del equipo. Como en la Imagen 122.

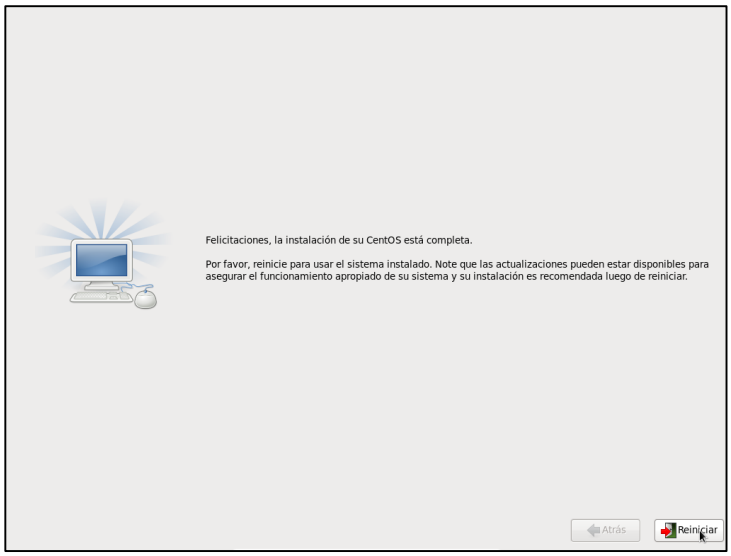


IMAGEN 122.- *Confirmar reinicio de equipo*
Fuente: *Instalación del Sistema Operativo Centos*

Luego de la instalación del Sistema Operativo aparece la pantalla de bienvenida. Imagen 123.

IMAGEN 123.- *Pantalla de bienvenida de Centos*
Fuente: *Instalación del Sistema Operativo Centos*

Seleccione la opción *Sí, Estoy de acuerdo con el Acuerdo de Licencia*, Imagen 124, lo cual indica que se aceptan todos los acuerdos que tiene como licencia el sistema operativo CentOS.

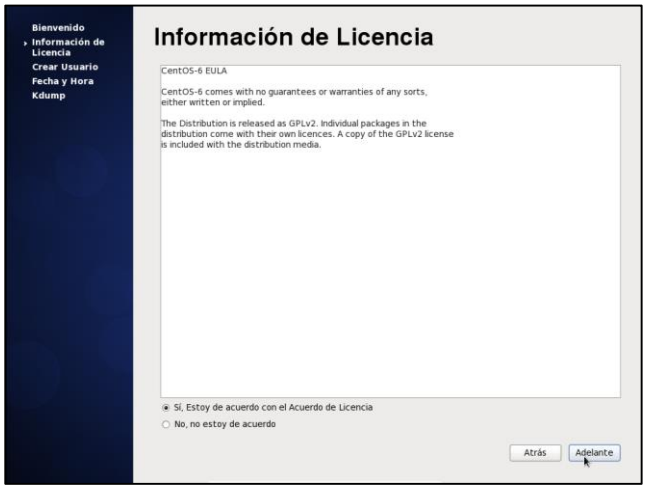


IMAGEN 124.- *Acuerdo de Licencia de Centos*
Fuente: *Instalación del Sistema Operativo Centos*

Se debe registrar el usuario con el cual se accede al sistema operativo, en este caso se deja todo en blanco para que solamente el usuario root se encuentre registrado. Imagen 125.

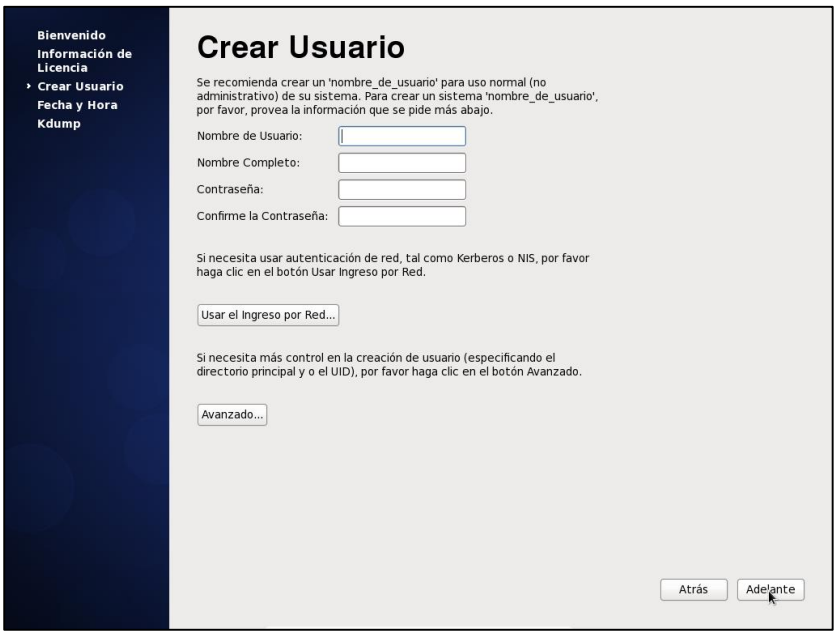


IMAGEN 125.- *Ingreso de usuario*

Fuente: *Instalación del Sistema Operativo Centos*

El asistente muestra una pantalla de advertencia, Imagen 126, en la que indica que no se ha configurado ningún usuario a más de root. Confirmamos esta advertencia.

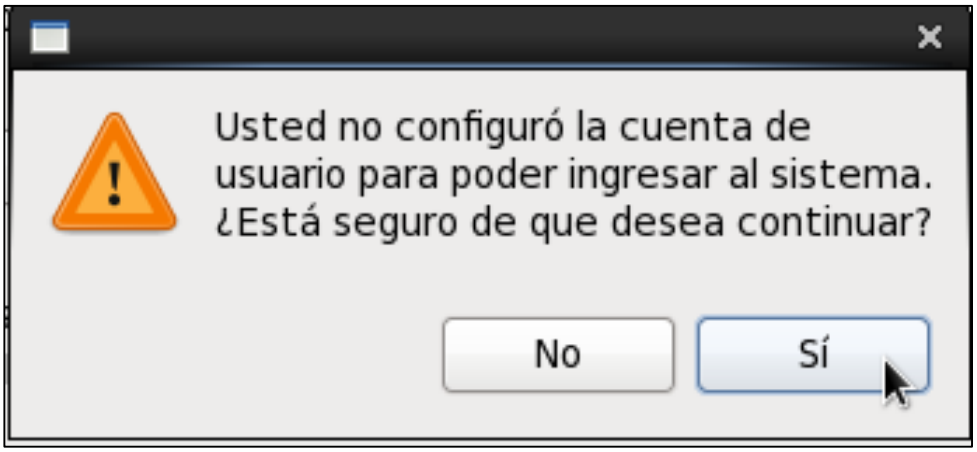


IMAGEN 126.- *Confirmación de las cuentas de usuario*

Fuente: *Instalación del sistema Operativo Centos*

Se configura la hora y fecha del equipo. Imagen 127.

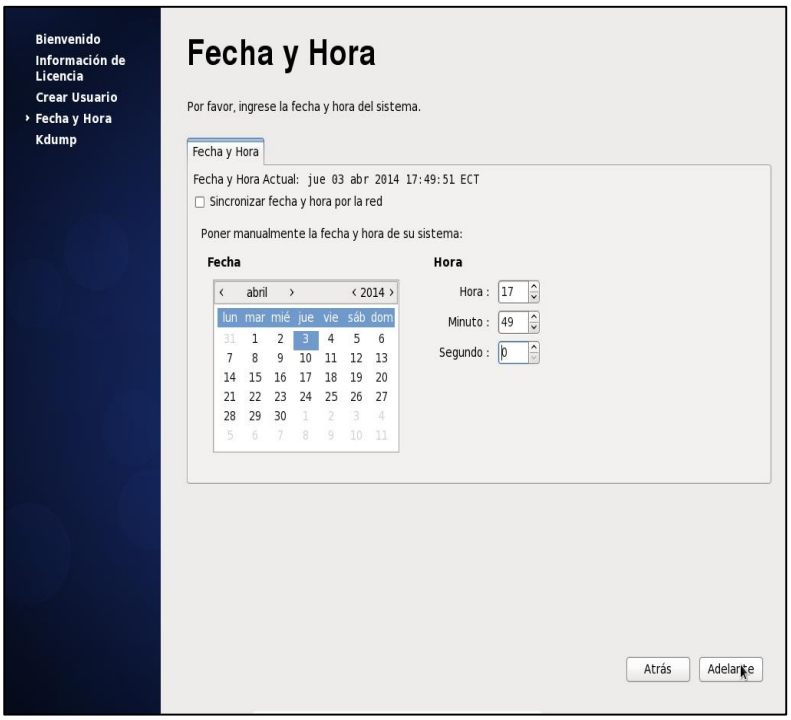


IMAGEN 127.- *Configuración de la fecha y hora del equipo*

Fuente: *Instalación del Sistema Operativo Centos*

Se muestra el error de la memoria *kdump*, solamente se confirma en *Aceptar.* Imagen 128.

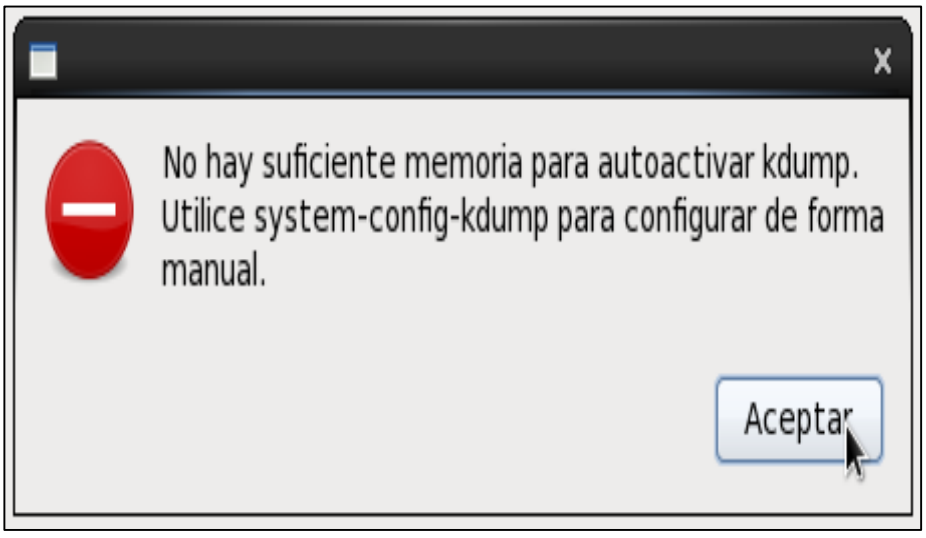


IMAGEN 128.- *Error de la memoria kdump*

Fuente: *Instalación del Sistema Operativo Centos*

Finalmente se muestra el mecanismo de volcado de fallos del kernel, seleccione la opción *Finalizar.* Imagen 129.

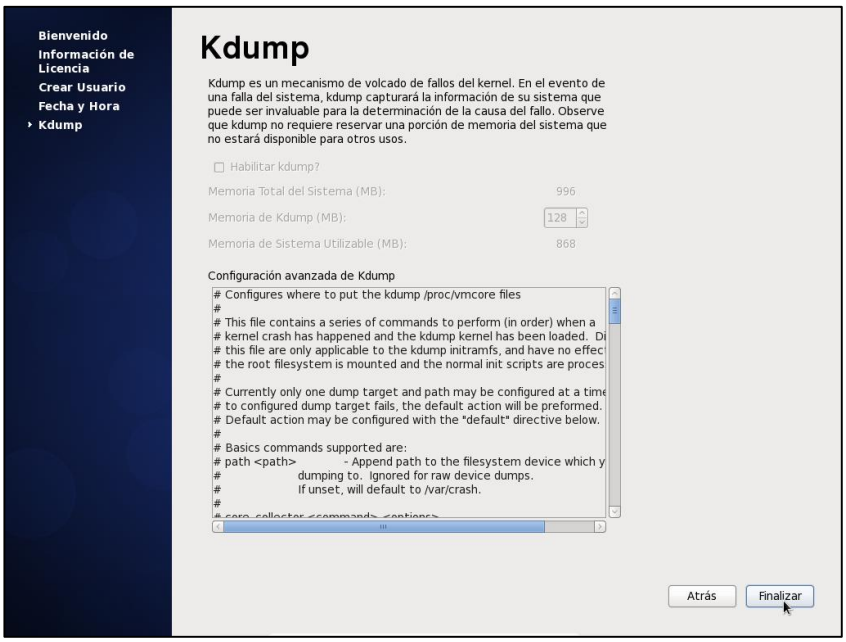


IMAGEN 129.- *Mecanismo de Volcamiento del kernel, Fin de la Instalación*

Fuente: *Instalación del Sistema Operativo Centos.*

Cuando se inicia el sistema operativo se muestra una pantalla indicando el nombre del equipo *snort-pc* y pide la autenticación, ingrese el usuario. Imagen 130.

IMAGEN 130.- *Inicio de sesión con el usuario root*

Fuente: *Instalación del Sistema Operativo Centos*

Ingrese la contraseña del usuario root. Imagen 131.

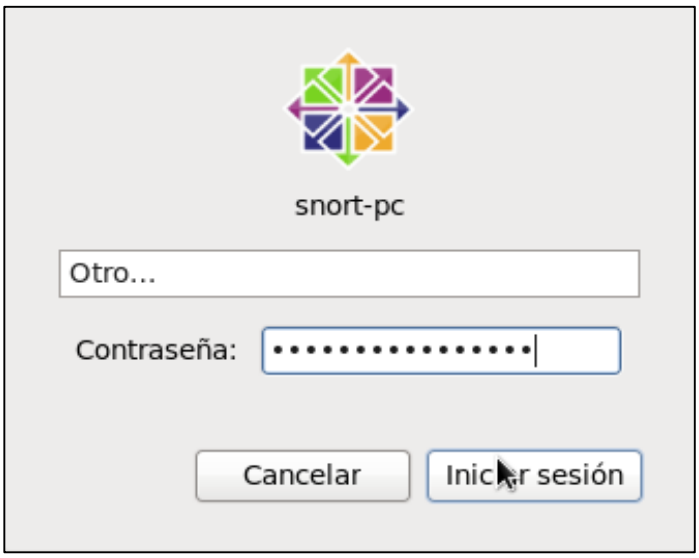


IMAGEN 131.- *Ingreso de la contraseña del usuario root*
Fuente: *Instalación del Sistema Operativo Centos*

El Sistema Operativo muestra una pantalla indicando que ingresa a él con la cuenta de súper usuario root, active la pestaña *No me vuelva a mostrar esto* y seleccionamos *Cerrar*. Imagen 132.

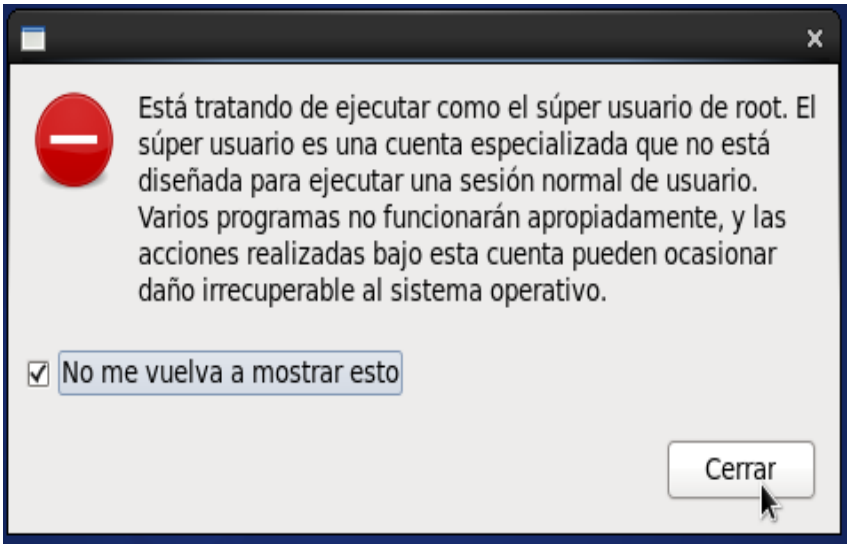


IMAGEN 132.- *Mensaje de acceso con el usuario root*
Fuente: *Instalación del Sistema Operativo Centos*

Listo, ha ingresado al escritorio del Sistema Operativo CentOS en su versión 6.5. Imagen 133.

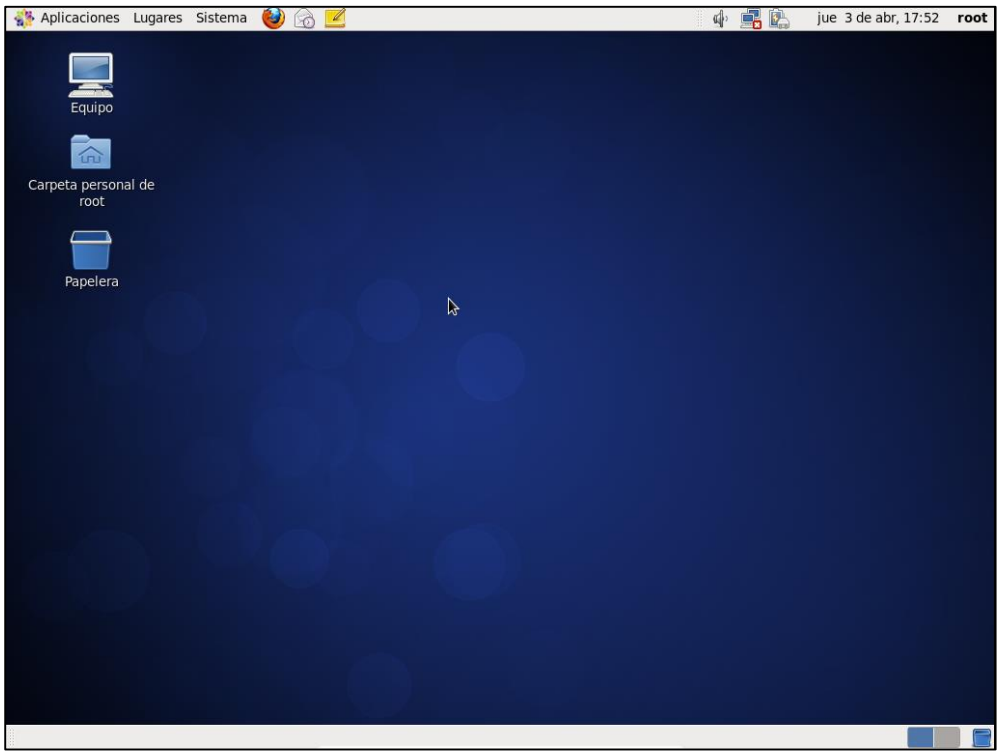


IMAGEN 133.- *Escritorio de CentOS 6.5*

Fuente: *Instalación del Sistema Operativo Centos*

ANEXO 06

INSTALACIÓN DE SHOREWALL Y WEBMIN EN CENTOS 6,5

Para la instalación de Shorewall se puede utilizar los repositorios de *Alcance Libre*, al descargar el archivo *http://www.alcancelibre.org/al/server/AL-Server.repo* y ubicarlo dentro del directorio */etc/yum.repos.d/*, todo esto se lo realiza mediante consola.

cd /etc/yum.repos.d/

wget -N http://www.alcancelibre.org/al/server/AL-Server.repo

cd

El archivo se guarda como */etc/yum.repos.d/AL-Server.repo*, y compruebe mediante el comando:

nano /etc/yum.repos.d/AL-Server.repo

Que el fichero contenga el siguiente contenido:

[AL-Server]

name=AL Server para Enterprise Linux $releasever

mirrorlist=http://www.alcancelibre.org/al/el$releasever/al-server

gpgcheck=1

gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY

Para salir presione la combinación *control + x* y finalmente se procede a la instalación del Shorewall con el comando.

yum –y install shorewall

Luego de la instalación de Shorewall se dirige al directorio */etc/shorewall/shorewall.conf* en el cual se definen los parámetros de configuración del Shorewall pero solo se editará el parámetro STARTUP_ENABLE

START_UP_ENABLE se lo utiliza para activar el servicio Shorewall de tal forma que cada vez que se encienda el equipo arranque automáticamente el servicio, y tan solo se necesita cambiar *No* por *Yes*.

START_UP_ENABLE=Yes

Por último se debe iniciar el servicio de Shorewall.

service shorewall start

Para la instalación de Webmin, tan solo se digita la línea de comando.

yum -y install webmin

Para comprobar el funcionamiento de ambos servicios tanto del Shorewall como del Webmin se utiliza el siguiente comando:

service shorewall status y service webmin status

Y deben dar el reporte de funcionamiento *Service is running.*

Para acceder a las configuraciones del Shorewall mediante el Webmin, en el navegador Web colocan la dirección *https://localhost:10000* y aparece la pantalla de advertencia de sitio no seguro, da click en *Entiendo los riesgos* y *Añadir la excepción.* Imagen 134.

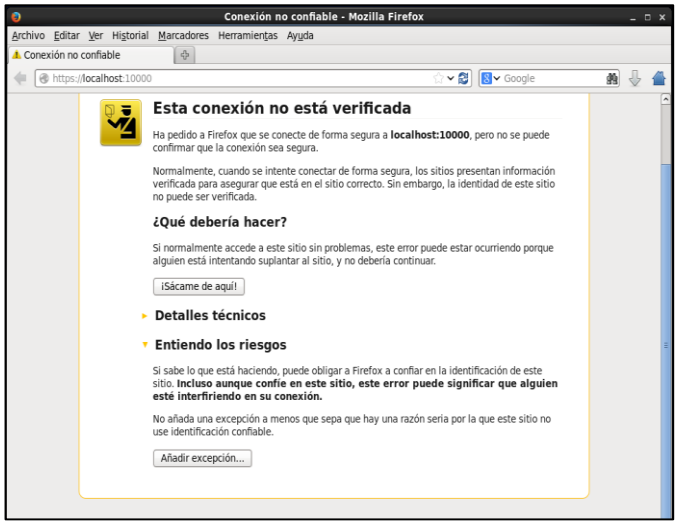


IMAGEN 134.- *Pantalla de advertencia del Webmin*

Fuente: *Servicio Webmin*

Aparece una pantalla donde se puede confirmar la excepción de seguridad para este servicio y de click en *Confirmar excepción de seguridad.* Imagen 135.

IMAGEN 135.- *Añadir excepción de seguridad*

Fuente: *Servicio Webmin*

Luego de confirmar la excepción se abrirá la pantalla de login del servicio Webmin, donde debe ingresar el usuario y contraseña, para ello serán *root* y *la_contraseña_de_root*, respectivamente. Imagen 136.

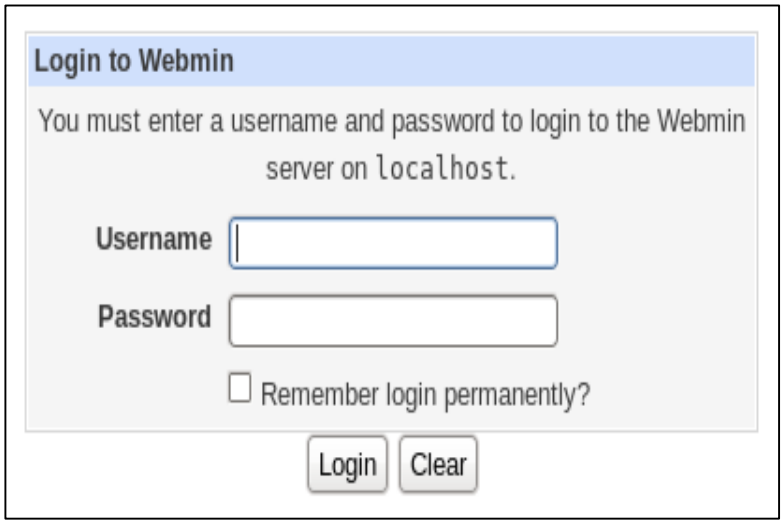


IMAGEN 136.- *Login del servicio Webmin*

Fuente: *Servicio Webmin*

Para acceder a las diferentes configuraciones permitidas en el Shorewall desde el servicio Webmin, diríjase hacia *Networking* > *Shoreline Firewall*, allí se encuentra los diferentes parámetros de configuración para el Firewall Shorewall, como se muestra en la Imagen 137.

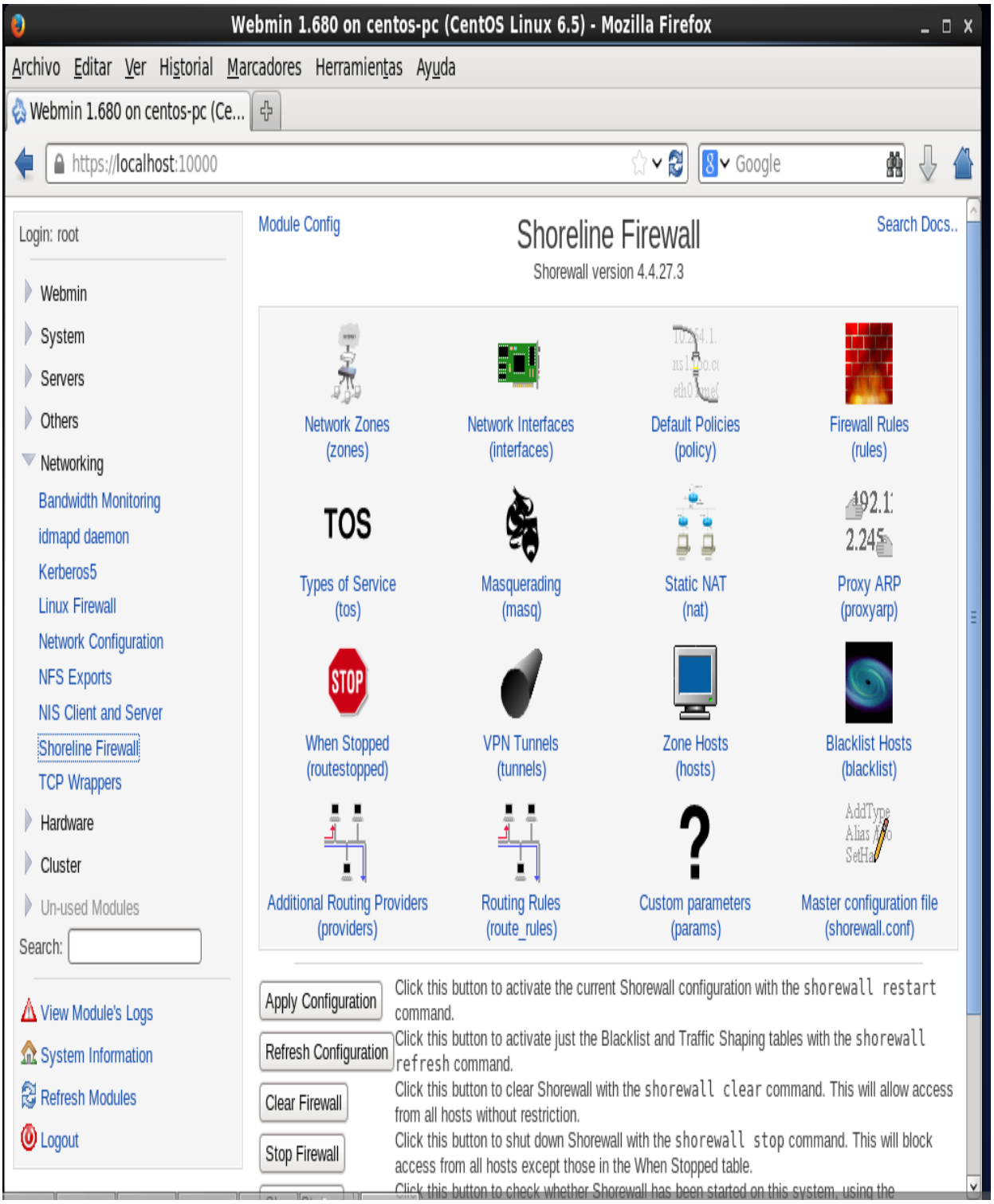


IMAGEN 137.- *Pantalla de configuración de Firewall Shorewall*

Fuente: *Servicio Webmin*

ANEXO 07

INSTALACIÓN DE SURICATA EN CENTOS 6.5

Para la instalación de Suricata es necesario habilitar los repositorios EPEL[29] de Fedora para el sistema x86_64, debido a que se tiene procesador de 64 bits. EPEL es un repositorio completo para la instalación de softwares en las distribuciones de software libre basados en Fedora: RHEL, CentOS y Scientific Linux.

Para habilitar los repositorios EPEL en CentOS 6.5 se ingresa a la terminal del sistema operativo en modo súper usuario y se digita:

wget http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

rpm -ivh epel-release-6-8.noarch.rpm

Uno de los paquetes necesarios para la instalación de Suricata es *magic rpm*, es por ello que se agregara también el siguiente repositorio.

wget http://mirror.nus.edu.sg/Fedora/epel/6/i386/epel-release-6-7.noarch.rpm

rmp –ivh epel-release-6-7.noarch.rpm

El primer paso para instalar Suricata es agregar varias dependencias que son requeridas para la instalación, mediante el comando

yum -y install libpcap libpcap-devel libnet libnet-devel pcre pcre-devel gcc gcc-c++ automake autoconf libtool make libyaml libyaml-devel zlib zlib-devel libcap-ng libcap-ng-devel magic magic-devel file file-devel

Para que Suricata opere en modo IPS necesita los paquetes “libnfnetlink” y “libnetfilter_queue”, pero estos paquetes no vienen dentro del repositorio de EPEL ni en la base de repositorios de CentOS por ello es necesario instalar los paquetes manualmente.

wget http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnetfilter_queue-0.0.15-1.x86_64.rpm
http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnetfilter_queue-devel-0.0.15-1.x86_64.rpm
http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnfnetlink-0.0.30-

[29] EPEL = Extra Packages for Enterprise Linux

1.x86_64.rpm http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnfnetlink-devel-0.0.30-1.x86_64.rpm

rpm -Uvh http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnetfilter_queue-0.0.15-1.x86_64.rpm http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnetfilter_queue-devel-0.0.15-1.x86_64.rpm http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnfnetlink-0.0.30-1.x86_64.rpm http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnfnetlink-devel-0.0.30-1.x86_64.rpm

También es necesaria la instalación de la librería libcap-ng, para ello procedemos con la *siguiente sec*

sudo yum -y install python devel

wget http://people.redhat.com/sgrubb/libcap-ng/libcap-ng-0.6.4.tar.gz

tar -xzvf libcap-ng-0.6.4.tar.gz

cd libcap-ng-0.6.4

./configure

make

sudo make install

Luego de haber ingresado los repositorios necesarios, las librerías y las dependencias que requiere Suricata, se procede con la instalación de Suricata. Para ello se descarga la última versión del software la cual es Suricata 2.0.1.

wget http://www.openinfosecfoundation.org/download/suricata-2.0.1.tar.gz

tar -xvzf suricata-2.0.1.tar.gz

cd suricata-2.0.1

Se utiliza el auto instalación de Suricata para crear todos los archivos de configuración necesaria así como también los últimos set de reglas.

./configure –enable-nfqueue

./configure && make && make install-conf

./configure && make && make install-rules

./configure && make && make install-full

Luego de descargar e instalar Suricata se procede a crear los siguientes directorios.

mkdir /var/log/suricata

mkdir /etc/suricata

En estos directorios que se acaban de crear se procede a copiar los archivos “classification.config”, “reference.config” y “suricata.yaml” desde los archivos orígenes de la instalación.

cd /tmp/suricata-1.4.4

cp classification.config /etc/suricata

cp reference.config /etc/suricata

cp suricata.yaml /etc/suricata

Finalmente para inicializar las funciones de Suricata se debe ingresar el siguiente comando, tomando en cuenta que se deben puentear las dos tarjetas de red del servidor donde se aloja Suricata, y seleccionar la interfaz de red por la que ingresa el tráfico.

suricata -c /etc/suricata/suricata.yaml -i eth0

Para ver si el motor de Suricata se encuentra trabajando correctamente y recibe e inspecciona el tráfico debemos ingresar al directorio de Suricata y digitar:

cd /var/log/suricata

tail http.log

tail -n 50 stats.*log*

Si desea ver la información en tiempo real solo es de agregar la opción *-f* antes de *http.log* y *stats.log.*

cd /var/log/suricata

tail -f http.log

tail -f -n 50 stats.log