UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación y configuración del servidor en el Laboratorio de Geomática y Especialidades de Civiles

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Diego Ramirez Romero

DIRECTORA DE TESIS

M.I. Tanya Itzel Arteaga Ricci

Ciudad Universitaria, Cd. Mx., 2022

Agradecimientos y dedicatorias

A la Universidad Nacional Autónoma de México, por la oportunidad de pertenecer a la máxima casa de estudios, por permitirme crecer como persona y profesionista.

A la Facultad de Ingeniería por acogerme como un hogar, por permitirme la oportunidad de formar parte del gremio de Ingenieros. Por inculcarme que los sueños se pueden lograr. Por cada uno de esos momentos inolvidables en sus instalaciones y recintos.

A mi padre Benjamín por el esfuerzo para otorgarme una educación, por sus enseñanzas y su amor. Por enseñarme el esfuerzo para conseguir lo que uno se propone.

A mi madre Patricia por apoyarme y no dejar a su hijo solo, por educar a un hombre de bien. Por no dejarme jamás, por sus enseñanzas y su amor incondicional.

A mi hermana Fabiola por apoyarme, regañarme cuando es necesario y por quererme tanto. Por ser un ejemplo de superación y constancia. Por estar en las buenas y malas. Por brindarme días de mucha alegría.

A Yuritzi Quintana mi compañera de vida, que ha estado ahí en todos los buenos y malos momentos. Por todos sus consejos y por el simple hecho de escucharme. Por enseñarme el verdadero significado de amor, cariño y lealtad. Por insistir que luche por mis metas.

A mi directora de tesis M. I. Tanya Itzel Arteaga Ricci, por brindarme la oportunidad de crecer profesionalmente, por su paciencia, por sus consejos, por la conducción en este proyecto, por creer en mí y sobre todo por ser mi amiga.

A la Unidad de Cómputo de la DICyG, por enseñarme tantas cosas y adoptarme como uno más. Por todos esas buenas y malas vivencias. Por darme la oportunidad de conocer a personas que han marcado mi vida y siempre las llevare en mi memoria.

A las personas que no creían en mí, porque también son un motivo más para superarme día a día. Por enseñarme la crudeza del mundo.

A mis amigos Gustavo Ortega, Miguel, Julio, Jessica Monserrat, Luis, Pilar, Angie, Sergio, Memo, Paco, Jair, Jesús, Alexa, Marquitos, Armandito, Héctor, Abraham, Monse, Rita y todos aquellos que no alcance a nombrar, pero saben que los aprecio y quiero. Por brindarme su amistar y momentos inolvidables.

A cada uno de mis profesores y profesoras que me brindaron su experiencia y paciencia a lo largo de estos siete años.

A todos ellos muchas gracias y estoy eterna mente agradecido a la vida que los puso en mi camino.

Hay dos formas de sufrimiento:

El trabajo duro, o el arrepentimiento. -NACH

Índice general

Introducción **8**

1. Introducción a las Redes de Datos **10**
1.1. Conceptos básicos de redes . . . 10
1.1.1. Definición de redes de computadoras . . . 10
1.1.2. Servicios que ofrecen las redes de datos . . . 10
1.1.3. Equipo activo de red . . . 11
1.1.4. Servidores . . . 11
1.1.5. Herramientas para la virtualización . . . 14
1.2. Clasificación de las redes por su cobertura geográfica . . . 16
1.3. Clasificación de redes por su topología . . . 17
1.3.1. Segmentación de red . . . 20
1.4. Modelos de referencia y protocolos . . . 21
1.5. Medios de transmisión . . . 25
1.5.1. Medios de transmisión guiados . . . 25
1.5.2. Medios de transmisión no guiados . . . 29
1.6. Estándares y organismos reguladores . . . 30
1.6.1. ANSI/TIA/EIA . . . 31
1.6.2. Normalización y Certificación Electrónica (NYCE) . . . 35

2. Situación *actual* de la red en los Laboratorios de Geomática y Especialidades de Civiles **37**
2.1. Antecedentes de estructura lógica del laboratorio . . . 37
2.2. Equipo con el que se contaba . . . 38
2.2.1. Sistema de gestión de calidad . . . 40
2.2.2. Diagnóstico lógico . . . 41
2.2.3. Seguridad en el laboratorio qué tipo de seguridad ofrece . . . 41
2.2.4. Necesidades reales . . . 41

3. Configuración del Servidor **43**
3.1. Servicios Necesarios . . . 43
3.2. Instalación del Sistema Operativo . . . 47
3.2.1. Instalación del Servidor . . . 47
3.2.2. Configuración del Servidor ESXi . . . 51
3.2.3. Creación de Servidores Virtuales . . . 56
3.2.4. Seguridad del Servidor . . . 72
3.2.5. Creación de las VLAN . . . 76
3.2.5.1. Configuración de las VLAN . . . 76
3.2.6. Cambio de equipo de red y servidores a VLAN 1000 . . . 84
3.2.7. Creación de VPN . . . 85
3.2.7.1. Configuración . . . 85

4. Implementación de herramientas especializadas **93**
4.1. Herramientas de monitoreo 93
4.1.1. NTOPNG 93
4.1.2. TCPDUMP 96
4.2. Puesta en marcha del portal WEB 96
4.2.1. Accesos y Seguridad 98
4.2.2. Servicios 99
4.3. Pruebas 99
4.4. Programa de mantenimiento 109

5. Manual de operaciones **112**
5.1. Manual de Administrador 112
5.2. Esquema general de red 115

Conclusiones **118**

Glosario **120**

Referencias **123**

Referencias de Figuras **125**

Índice de figuras

1.1. Modelo Cliente-Servidor . . . 12
1.2. Servidor de Correo . . . 12
1.3. Servidor Web . . . 13
1.4. Servidor de Archivos . . . 14
1.5. Herramientas para la virtualización . . . 15
1.6. Topología Estrella . . . 17
1.7. Topología Bus . . . 18
1.8. Topología Árbol . . . 18
1.9. Topología Anillo . . . 19
1.10. Topología Malla . . . 19
1.11. Capas del modelo OSI . . . 21
1.12. Capas del modelo TCP/IP . . . 22
1.13. Datagrama de TCP . . . 23
1.14. Datagrama UDP . . . 23
1.15. Datagrama IP . . . 24
1.16. Vista seccionada de un cable coaxial . . . 25
1.17. Cable UTP . . . 26
1.18. Cable STP . . . 26
1.19. Cable FTP . . . 27
1.20. Elementos de la fibra óptica . . . 27
1.21. Conectores de fibra óptica . . . 28
1.22. Propagación de baja y alta frecuencia . . . 29
1.23. Conexión extremo a extremo de microondas . . . 29
1.24. Antena repetidora de microondas . . . 30
1.25. Subsistemas del Cableado Estructurado . . . 31
1.26. (a) Cable Cruzado y (b) Directo . . . 33

2.1. Topología inicial de red . . . 37
2.2. Rack con equipo de red . . . 38
2.3. Cableado horizontal . . . 39
2.4. Detalle de cable UTP . . . 39
2.5. *Switch* NETGEAR . . . 39
2.6. Equipo de Cómputo . . . 40

3.1. Colocación de piso falso . . . 43
3.2. Detalle de cable UTP . . . 44
3.3. Tendido de cableado de red y electricidad . . . 44
3.4. Cableado horizontal . . . 45
3.5. Cableado horizontal dirección SITE . . . 45
3.6. Aire acondicionado . . . 46
3.7. Cuadra rack con todo el equipo de red . . . 46
3.8. Compatibilidad con ESXi . . . 48
3.9. Términos de licencia . . . 48
3.10. Elección de disco duro para la instalacion . . . 49
3.11. Distribución del teclado . . . 49

3.12. Contraseña de *root* . . . 49
3.13. Configuración de instalación . . . 50
3.14. Reinicio del servidor . . . 50
3.15. Detalles del servidor . . . 51
3.16. Ingreso a personalizacion del sistema . . . 51
3.17. Configuración de red . . . 51
3.18. Selección de interfaz de red para LAN . . . 52
3.19. Datos de red . . . 52
3.20. Dirección de los DNS . . . 53
3.21. Creación de almacenamiento . . . 53
3.22. Tipo de creación . . . 54
3.23. Selección de dispositivo y asignación de nombre . . . 54
3.24. Espacio a utilizar y tipo de partición . . . 55
3.25. Información de la partición . . . 55
3.26. Confirmacion en la creación de la partición . . . 56
3.27. Almacenamiento creado . . . 56
3.28. Especificaciones de imagen ISO de pfSense . . . 57
3.29. Carga de imagen ISO en datastore1 . . . 57
3.30. ISO en datastore1 . . . 58
3.31. Configuración de *switch* para la WAN . . . 58
3.32. Configuración de *switch* para la LAN . . . 59
3.33. Configuración de grupo de puertos para la WAN . . . 59
3.34. Configuración de grupo de puertos para la LAN . . . 60
3.35. Sección Máquinas virtuales . . . 60
3.36. Especificaciones para la máquina virtual . . . 61
3.37. Almacenamiento para la máquina virtual . . . 61
3.38. Configuración de interfaces de red e imágen ISO de pfSense . . . 62
3.39. Instalación de pfSense . . . 63
3.40. Partición guiada de pfSense . . . 63
3.42. Interfaces de red configuradas . . . 64
3.41. Configuraciones de interfaz de red para WAN y LAN . . . 64
3.43. Consola pfSense . . . 65
3.44. Página de login de pfSense . . . 65
3.45. Vista de primer inicio de pfSense . . . 66
3.46. Información general de pfSense . . . 67
3.47. Zona horaria pfSense . . . 67
3.48. Configuración de interfaz WAN . . . 68
3.49. Bloqueo de redes privadas y bogon . . . 68
3.50. Configuración de interfaz LAN . . . 69
3.51. Actualización de contraseña para pfSense . . . 69
3.52. Configuración DHCP LAN . . . 70
3.53. DNS de la UNAM . . . 70
3.54. Reglas NAT . . . 71
3.55. Reglas en *Firewall* . . . 71
3.56. Generación de llaves pública-privada . . . 72
3.57. Directorio de las llaves pública-privada . . . 72
3.58. Copia de clave pública al servidor web . . . 73
3.59. Conexión al servidor web . . . 73
3.60. Conexión con el servidor web sin confirmar contraseña . . . 74
3.61. Especificaciones de SSH en pfSense . . . 74
3.62. Llave pública en pfSense . . . 75
3.63. Conexión SSH a pfSense . . . 75
3.64. Desbloqueo de llave pública en cliente . . . 75
3.65. Conexión con pfSense sin confirmar contraseña . . . 76
3.66. Agregar VLANs . . . 77
3.67. Detalles de VLAN . . . 77

3.68. Listado de VLANs . . . 77
3.69. Asignación de VLANs . . . 78
3.70. Configuración de VLAN . . . 78
3.71. Listado de interfaces asignadas . . . 79
3.72. Configuración de DHCP para cada VLAN . . . 79
3.73. Reglas de paso . . . 80
3.74. Creación de grupo de puertos para cada VLAN . . . 80
3.75. Grupo de puertos LAN . . . 80
3.76. Sección para crear VLAN . . . 81
3.77. Agregar VLAN . . . 81
3.78. Asignación y creación de VLAN . . . 81
3.79. Editar configuración de VLAN . . . 82
3.80. Asignación de puertos de manera *untagged* . . . 82
3.81. Configuración de puertos troncales . . . 83
3.82. Configuración de puertos . . . 83
3.83. Configuración de puerto para AP . . . 84
3.84. Topología Final de Red. . . . 84
3.85. Grupo de puertos VLAN100 . . . 85
3.86. Instalación de paquete para exportar clientes VPN . . . 85
3.87. Proceso de instalación de paquete . . . 86
3.88. Instalación finalizada . . . 86
3.89. Asistente de configuración de OpenVPN . . . 87
3.90. Tipo de Servidor a implementar . . . 87
3.91. Creación de CA . . . 88
3.92. Servidor de certificados . . . 88
3.93. Configuraciones generales del Servidor . . . 89
3.94. Configuraciones criptográficas . . . 89
3.95. Configuración de algoritmos criptográficos . . . 89
3.96. Configuraciones del túnel . . . 90
3.97. Configuraciones de clientes . . . 90
3.98. Creación de reglas en *Firewall* . . . 90
3.99. Creación de certificado para usuario local . . . 91
3.100. Configuración del certificado para usuario local . . . 91
3.101. Certificado para usuario local . . . 91
3.102. Cliente OpenVPN . . . 91

4.1. Paquete *ntopng* . . . 94
4.2. Instalación de paquetes necesarios para *ntopng* . . . 94
4.3. Instalación exitosa de ntopng . . . 94
4.4. Configuraciones generales *ntopng* . . . 95
4.5. Estatus de *ntopng* . . . 95
4.6. Login para *ntopng* . . . 96
4.7. Versión de tcpdump y libpacp . . . 96
4.8. Estatus de ufw . . . 97
4.9. Permisos al usuario encargado . . . 97
4.10. Versión de mysql . . . 97
4.11. Estado de mysql . . . 97
4.12. Versión de php . . . 98
4.13. Página principal del LGyEC . . . 98
4.14. Página de *cerbot* . . . 99
4.15. Asignación de IP y velocidad de internet VLAN 10 . . . 100
4.16. Asignación de IP y velocidad de internet VLAN 20 . . . 100
4.17. Asignación de IP y velocidad de internet VLAN 30 . . . 101
4.18. Asignación de IP y velocidad de internet VLAN 40 . . . 101
4.19. Asignación de IP y velocidad de internet VLAN 1000 . . . 102
4.20. DHCP *Leases* . . . 102
4.21. Icono OpenVPN . . . 103

4.22. Login OpenVPN . . . 103
4.23. Estado de conexión VPN . . . 104
4.24. Equipo conectado a VPN . . . 104
4.25. Conexión a ESXi . . . 105
4.26. Conexión a página web . . . 106
4.27. Conexión pfSense . . . 106
4.28. Conexión NTOPNG . . . 107
4.29. VLAN 20 loal *hosts* . . . 108
4.30. VLAN 20 MAC *list* . . . 108
4.31. VLAN 20 *Active Flows* . . . 109

5.1. Conexiones Físicas del equipo de red . . . 112
5.2. Especificaciones de NIC VMkernel . . . 113
5.3. Interfaces físicas en ESXi . . . 113
5.4. Grupo de puertos y *switch Management Network* . . . 114
5.5. Grupo de puertos y *switch* WAN . . . 114
5.6. Grupo de puertos y *switch* LAN . . . 115
5.7. Diagrama de red lógico del LGyEC . . . 116

Introducción

Introducción

Actualmente los servicios de TI(Tecnologías de la Información) ya dejaron de ser un lujo que unos cuantos pueden tener, se han convertido en herramientas de uso diario y multidisciplinario. En materia de educación se ha vuelto indispensable contar con las herramientas informáticas, para el apoyo y desarrollo del aprendizaje, con esta premisa, surge la necesidad de proveer de servicios e instalaciones tecnológicas de calidad, con las normas y estándares necesarios para su correcto funcionamiento.

Por lo que, la División de Ingenierías Civil y Geomática(DICyG), a través de la Unidad de Cómputo, tiene el compromiso de gestionar de la mejor manera la infraestructura de red provista por la Facultad. A lo largo de este trabajo se describirán las buenas prácticas junto con los estándares necesarios para la puesta en marcha del site del Laboratorio de Geomática y Especialidades de Civiles (LGyEC), así como la instalación y configuración de las herramientas que se utilizarán para proveer los servicios. Cabe mencionar que a lo largo del todo el trabajo, por motivos de seguridad se ocultaran datos de red.

En el primer capítulo, se abordarán los conceptos básicos de las redes de datos, así como algunos estándares y organismos reguladores necesarios para el desarrollo del cualquier proyecto de infraestructura de red.

En el segundo capítulo, se hablará de las condiciones reales de la infraestructura y estructura lógica de red en el Laboratorio de Geomática y Especialidades de Civiles (LGyEC), así como el objetivo que se tiene que cubrir en el laboratorio para una posible certificación.

El tercer capítulo hablará de toda la nueva implementación del proyecto mostrando la infraestructura y el equipo de red que se usará. La instalación del sistema base y los servicios requeridos, así como las configuraciones pertinentes para la administración.

El cuarto capítulo abarca la instalación de herramientas que se utilizarán para la administración de la red, puesta en marcha del portal web, pruebas de segmentación y de monitoreo, así como el programa de mantenimiento que se tendrá en el laboratorio.

En el quinto capítulo se hablará de manera general de cómo se tienen las configuraciones relevantes del proyecto tanto en el servidor host y los virtuales.

Por último, se establecerán las conclusiones al proyecto donde se estará validando el objetivo y el alcance de toda la implementación y mejoras sustanciales del proyecto.

Objetivo

Proveer de un servidor que ofrezca seguridad, administración, disponibilidad de servicios y herramientas de control de red, para los laboratorios de Geomática y Especialidades de Civiles(LGyEC).

Objetivos específicos

- Ofrecer herramientas adecuadas para la administración de los servicios de red.
- Implementar una segmentación de la red para cada área de trabajo que existe en el LGyEC.
- Otorgar redireccionamiento de servicios.
- Proveer un monitoreo de red eficaz y eficiente.
- Administrar los servicios de manera remota.
- Dar la posibilidad de escalabilidad y crecimiento futuro.

Capítulo 1 Introducción a las Redes de Datos

Capítulo 1

Introducción a las Redes de Datos

1.1. Conceptos básicos de redes

1.1.1. Definición de redes de computadoras

Es un sistema de comunicación que está conformado por dos o más equipos interconectados a través de un medio de transmisión, para poder comunicarse y compartir recursos sin importar la naturaleza de cada equipo.

1.1.2. Servicios que ofrecen las redes de datos

A continuacion se listan algunos servicios que ofrecen las redes de datos:

1. Acceso: Comprende la verificación de la identidad del cliente para determinar qué recursos puede o no manejar. En el control de acceso el cliente tiene que conectarse a un servidor el cual le pedirá un usuario y una contraseña de acceso, en dado caso que los dos sean correctos el usuario puede conectarse a la red. El acceso remoto le permitirá al usuario tener acceso a uno o varios recursos en red.

2. Almacenamiento de Archivos: Ofrece una gran cantidad de almacenamiento para poder guardar o eliminar fuera del equipo del cliente. Permitiendo almacenar aplicaciones y datos en un lugar centralizado, reduciendo los requerimientos de almacenamiento en las estaciones de los clientes.

3. Impresión: Permite compartir impresoras entre múltiples usuarios quitando la limitante de la conexión fisica con el dispositivo de impresión, ya que toda la conexión es por medio de la red. En dado caso que el servicio pueda contar con almacenamiento este mismo puede mantener la cola de impresión de los clientes.

4. Correo: Es uno de los servicios con mayor demanda, ya que es un medio de comunicación entre clientes. Este servicio incrementa mucho lo que se puede enviar a través de un correo electrónico, ya que además de texto pueden enviarse cualquier tipo de archivo digital.

5. Manejo de Información: Comparte archivos en función de su contenido como es el hipertexto. O pueden proveer de información que necesita un tratamiento por alguna aplicación en un cliente, como lo es en el caso de las bases de datos.

6. Gestión remota: Permite el acceso y control remoto de un dispositivo sin ninguna conexión fisica, habitualmente se localiza en otra región geográfica.

7. Comunicación: Otorga la infraestructura de hardware que es la base sobre la cual se puede desarrollar algún ortro servicio.

8. Flujo de datos: Es la forma en las tramas se propagan a través de la red. Es el movimiento de datos a través de los dispositivos y a la manera en que la información debe de encapsularse para poder viajar de la forma correcta.

1.1.3. Equipo activo de red

Son aquellos equipos de red que necesitan energía eléctrica para poder funcionar, permitiendo distribuir la información por la red. A continuación se mencionan algunos equipos activos.

- **Tarjeta de red PCI**. Elemento de hardware que necesita una computadora para poder conectarse a la red, se conecta directamente a la placa madre.
- **Puentes o Bridges**. Conecta dos o más segmentos de red para formar una sola red. Funciona mediante una tabla de direcciones MAC, de esta manera el puente permite filtrar tramas para permitir el paso sólo de aquellas cuyas direcciones de destino corresponda con un equipo ubicado en alguna de las dos redes que conecta.
- **Switch**. Es un dispositivo que permite que la conexión entre equipos de cómputo y periféricos a la red para que puedan comunicarse entre sí y con otras redes. Existen dos tipos de switches:
  1. Switches administrados: son aquellos programables. Se puede ajustar de forma remota o local para controlar el tráfico y los accesos a la red.
  2. Switches no administrados: funcionan automáticamente y no permiten cambios. Estos son los switchs más comúnmente usados en las redes domésticas.
- **Router**. El enrutador (del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware (o software) para interconexión de red. Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. El router asegura que la información no va a donde no es necesaria.
- **AP o WAP**. Punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un dispositivo que interconecta a equipos con tecnología inalámbrica (equipos de cómputo, impresoras, etc.) para formar una red inalámbrica.

1.1.4. Servidores

Un servidor es un equipo de cómputo que pertenece a una red y se encarga de proveer servicios a otros equipos. Dicho equipo de cómputo debe contar con una aplicación específica capaz de atender las peticiones de los distintos clientes y brindarles respuesta oportuna, por lo que en realidad dentro de una misma computadora física (hardware) pueden funcionar varios servidores simultáneos (software), siempre y cuando cuenten con los recursos logísticos necesarios. Los servidores dedicados son aquellos que especializan todos sus recursos a atender peticiones de otros equipos clientes. En contraparte el servidor compartido es usado para trabajar de forma local y atender clientes en la red al mismo tiempo. Los servidores se basan en el modelo cliente-servidor véase en la Figura 1.1.

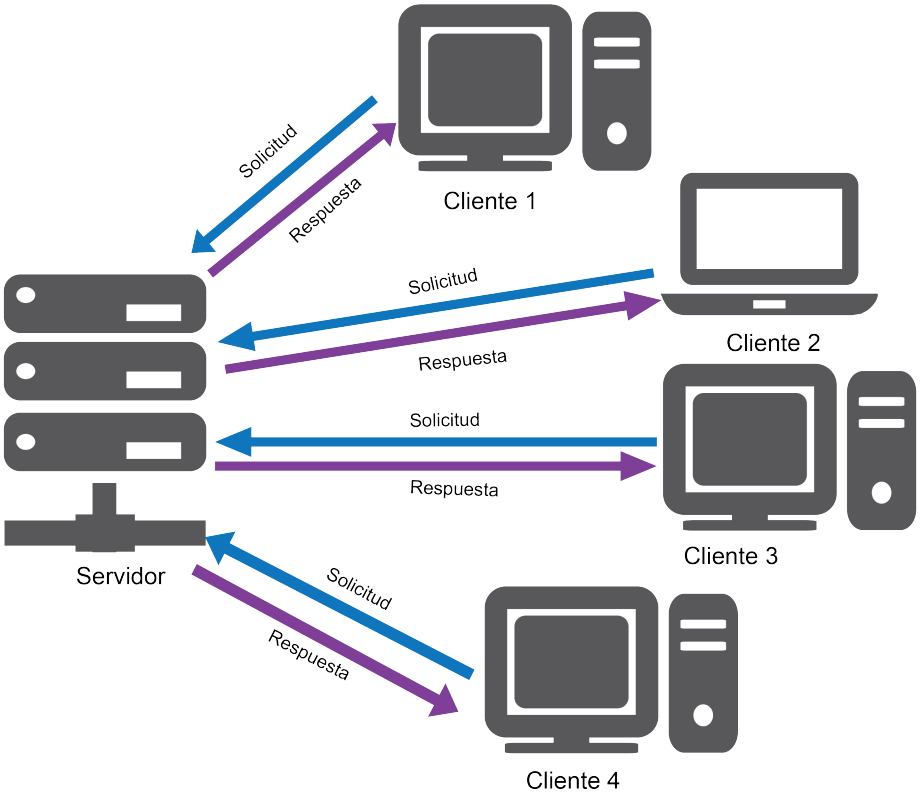

Figura 1.1: Modelo Cliente-Servidor

Existen diversos tipos de servidores, algunos de los más demandados son los siguientes:

(a)Servidor de Correo. Permite la recepción, envío y reenvío de correos electrónicos, así como mantenerlos disponibles para el usuario. Funciona mediante el protocolo SMTP (*Simple Mail Transfer Protocol*). Para poder tener la comunicación entre el servidor y el usuario, es necesario contar con un cliente de correo electrónico para que administre la comunicación con el servidor de correos. Para esta comunicación se implementan los protocolos IMAP (*Internet Message Access Protocol*) o POP (*Post Office Protocol*) véase la Figura 1.2.

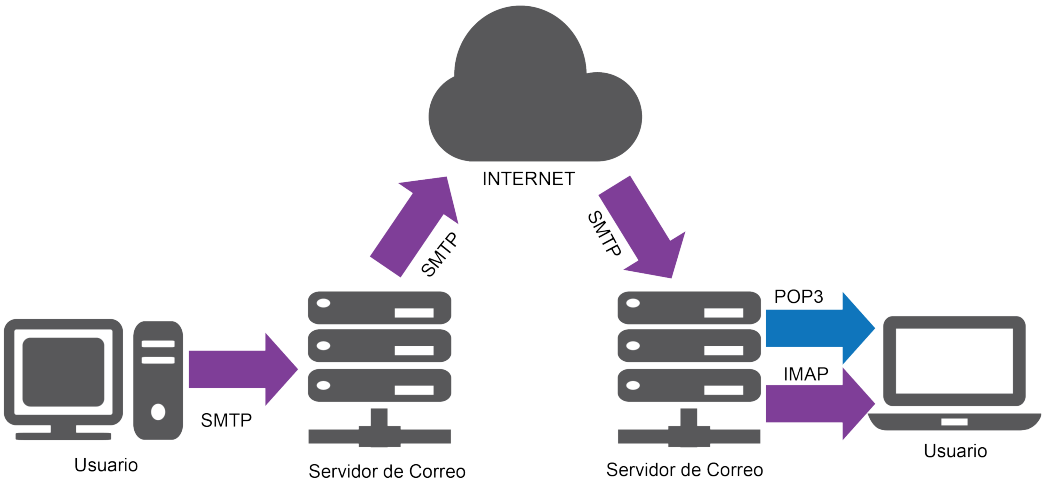

Figura 1.2: Servidor de Correo

(b)Servidor WEB. Guarda y organiza páginas web con la posibilidad de mostrarlas a un cliente, ya sea navegador web o *crawlers*[1]. La comunicación entre este servidor y los clientes se basa en HTTP (*Hypertext Transfer Protocol*) o en HTTPS (*HyperText Transfer Protocol Secure*). El servidor envía solo archivos HTML (*HyperText Markup Language*) y sus elementos integrados. Apache es un ejemplo de servidor web véase Figura 1.3.

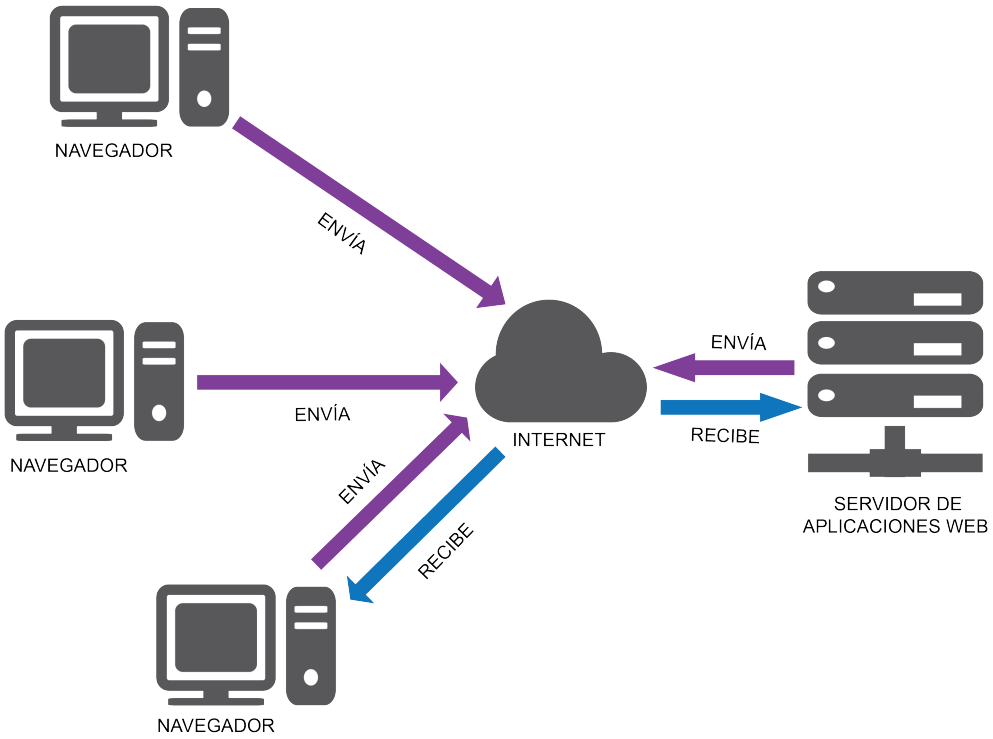

Figura 1.3: Servidor Web

(c)Servidor de Archivos. Provee de un lugar de almacenamiento centralizado disponible para todos los clientes autorizados de una red, así como su gestión. El administrador de dicho servidor puede configurar quién tiene acceso y a qué archivos en específico, si la configuración lo permite los clientes pueden tener acceso a sus archivos fuera de la red local. Para esto se implementan protocolos de transmisión como lo son FTP (*File Transfer Protocol*), SFTP(*SSH File Transfer Protocol*), FTPS (*SSL File Transfer Protocol*) o SCP (*Secure Copy Protocol*), sin olvidar que los protocolos SMB (*Server Message Block*) y NFS (*Network File System*) habitualmente funcionan en la red local. Este tipo de servidor también puede emplearse como servidor de respaldo o repositorio de programas que deben de estar disponibles para distintos miembros de la red, véase Figura 1.4.

[1]Conocidos como rastreadores, son programas que analizan los documentos de los sitios web.

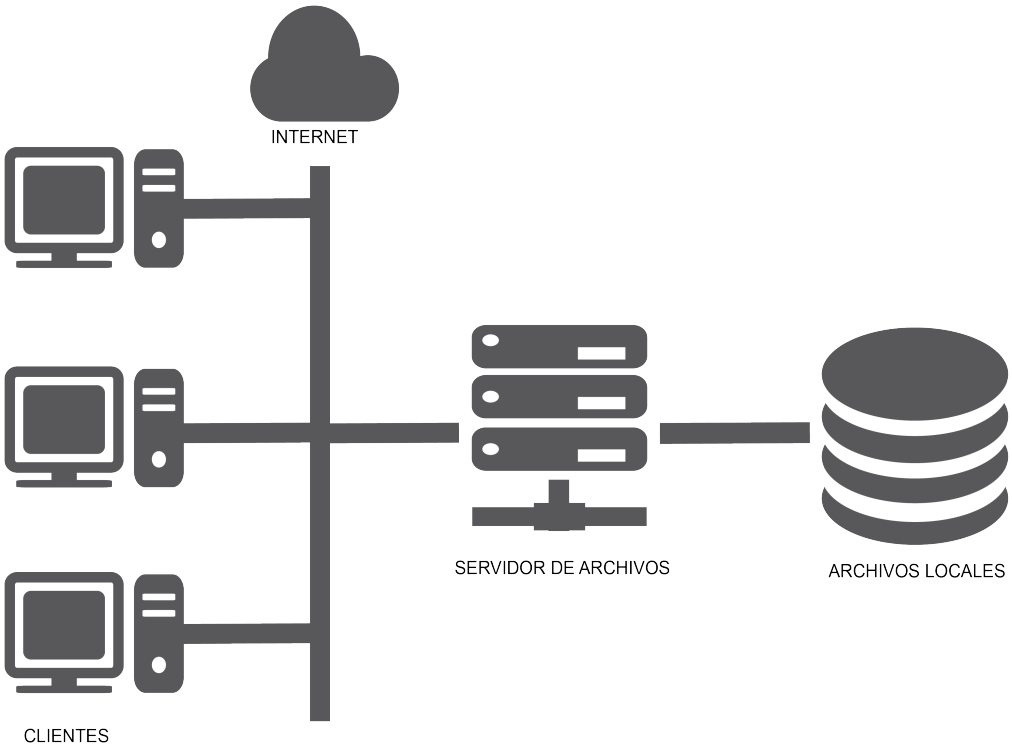

Figura 1.4: Servidor de Archivos

(d)Servidor Virtual. La virtualización consiste en la creación de una versión no física de algún recurso de Tecnologias de la Información(TI), como lo son los sistemas operativos, servidores, recursos de red, dispositivos de almacenamiento entre otros. Como ejemplo tenemos la partición de un disco duro en dos unidades distintas separadas por el software, pero unidas por un mismo hardware. En la virtualización tenemos tres áreas de interés: redes, almacenamiento y servidores. Esta última permite mediante software, ejecutar más de un sistema operativo como invitado en un host con hardware de servidor. De esta manera cada sistema operativo invitado se convierte en una máquina virtual[2].

1.1.5. Herramientas para la virtualización

A continuacion se listan algunas herramientas que se pueden implementar para la virtualización, cada una de ellas tiene sus caracteristicas que se pueden observar en la Tabla 1.1.

(a)QEMU. Es un emulador y virtualizador de máquinas genérico y de código abierto. Al implementarlo como un emulador de máquina, puede ejecutar sistemas operativos y programas creados para una máquina. Y al usarlo como virtualizador, logra un rendimiento casi nativo, admite la virtualización cuando se ejecuta bajo el hipervisor Xen. QEMU puede virtualizar x86, servidor y PowerPC incorporado, POWER de 64 bits, S390, ARM de 32 y 64 bits, e invitados MIPS.

(b)VirtualBox. Es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Está disponible de manera gratuita como software de código abierto bajo los términos de la versión 2 de la GPL de GNU. Actualmente, VirtualBox se ejecuta en un hosts Windows, Linux, Macintosh y Solaris. Y puede tener como sistemas invitados a Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS / Windows 3.x, Linux (2.4, 2.6, 3.xy 4.x), Solaris y OpenSolaris, OS / 2 y OpenBSD.

(c)VMware. ESXi. Es un hipervisor de tipo ***bare-metal***. No se ejecuta sobre un sistema operativo externo sino que está incrustado en el núcleo del mismo. Para su ejecución, ESXi se apoya en un sistema Linux basado

[2]Entorno virtual que funciona con su propio cpu,memoria,interfaz de red y almacenamiento que gestiona el hypervisor.

en Red Hat Enterprise modificado para la ejecución del hipervisor y los componentes de virtualización de VMware. Puede configurar máquinas virtuales de hasta 128 CPU virtuales, 6 TB de memoria RAM y 120 dispositivos. ESXi forma parte del paquete de soluciones de WMware vSphere, junto a vSphere cliente y vCenter.

(d)KVM. Es una solución de virtualización completa para Linux en hardware x86 que contiene extensiones de virtualización (Intel VT o AMD-V). Consiste en un módulo de kernel cargable, kvm.ko, que proporciona la infraestructura de virtualización principal y un módulo específico del procesador, kvm-intel.ko o kvm-amd.ko. Permite la ejecución de sistemas operativos desde imágenes de disco, por ejemplo, en formato ISO o MDS con sistemas operativos ejecutables. Solamente podremos virtualizar sistemas operativos Linux.

Figura 1.5: Herramientas para la virtualización

Tabla 1.1: Comparativa herramientas de virtualización

Característica	VirtualBox	QEMU	KVM	VMWare ESXi
Tipo de Hipervisor	hosted	hosted	hosted	bare-metal
Tipo de Licenciamiento	Gratuito	Gratuito	Código abierto	Gratuito / Paga
Virtualización	Hardware + Software	Hardware	Hardware	Hardware
Sistema Operativo Host	Linux, Windows, Solaris, macOS	Windows, Solaris, Linux, FreeBSD, NetBSD, OpenBSD, macOS	Linux	Ninguno
Sistema Operativo Invitado	Linux, Windows, Solaris, macOS, FreeBSD	Linux, Windows, DOS, OpenBSD, FreeBSD	Linux, Windows, entre otros	Linux, Windows, Solaris, FreeBSD
Migración viva de MV	Si (Teletrans-portación)		Si	Si (vMotion)

Hypervisor.

El hipervisor es el elemento del sistema operativo o de software que administra y hace que funcionen las máquinas virtuales sobre un hardware virtual. El hipervisor tiene varias tareas, por un lado, presentan a los sistemas virtualizados, también proveen de un hardware virtual a las máquinas virtuales y de monitorizar a estas máquinas, véase Figura 1.5.

Existen tres tipos principales de hipervisores en el mercado:

- Hipervisores de tipo 1 (También llamados nativos, unhosted o bare-metal): en ellos el hipervisor se ejecuta directamente sobre el hardware físico; el hipervisor se carga antes que ninguno de los sistemas operativos invitados, y todos los accesos directos a hardware son controlados por él.
- Hipervisores de tipo 2 (también llamados hosted): en ellos el hipervisor se ejecuta en el contexto de un sistema operativo completo, que se carga antes que el sistema operativo. Las máquinas virtuales se ejecutan en un tercer nivel, por encima del hipervisor. Son típicos de escenarios de virtualización orientada a la ejecución multiplataforma de software, como en el caso de Common Language Runtime de .NET o de las máquinas virtuales de Java.
- Hipervisores híbridos en este modelo tanto el sistema operativo anfitrión como el hipervisor interactúan directamente con el hardware físico. Las máquinas virtuales se ejecutan en un tercer nivel con respecto al hardware, por encima del hipervisor, pero también interactúan directamente con el sistema operativo anfitrión.

Contenedores

Es la ejecución de un sistema operativo, siendo el mismo para los sistemas hosts y huésped. Se aprovecha la intervención directa del sistema operativo con el hardware eliminando el uso de un hypervisor. El sistema que fungirá como anfitrión mantendrá separado los servicios que se necesiten configurar. Una de la principales características que tienen los contenedores es el consumo bajo de recursos, ya que cualquier otro método de virtualización ocupará algunos recursos, aún estando inactiva.

1.2. Clasificación de las redes por su cobertura geográfica

Según su cobertura o su extensión geográfica, las redes de datos se pueden clasificarse de la siguiente manera:

I.-Redes de área local. Usualmente llamadas LAN (Local Area Networks), son redes que funcionan dentro de un solo edificio (casa, oficina o fábrica). Las LAN son implementadas para la conexión de computadoras personales así como cualquier equipo de cómputo, con la finalidad de compartir recursos e intercambiar información.

II.-Redes de área local inalámbricas. WLAN (Wireless Local Area Network) implementa un sistema flexible de comunicación de datos, usa radiofrecuencias para transmitir y recibir datos, minimizando la necesidad de conexiones cableadas. Permiten también la interconexión de dos equipos que se encuentran cercanos entre sí para establecer una conexión sin necesidad de tener salida a internet. Su principal estándar es el IEEE 802.11[3].

III.-Redes de área metropolitana. Mejor conocida como MAN (Metropolitan Area Network) su cobertura es para toda una ciudad teniendo mayor alcance que una red LAN pero menos que las WAN. El principal medio para mantener conexión es mediante fibra óptica, permitiendo que las conexiones sean mucho más rápidas y reduciendo los errores en la misma.

IV.-Redes de área amplia. Comúnmente llamada WAN (Wide Area Network) abarca una área geográfica mucho más extensa. Los nodos pueden estar separados por distancias muy grandes pudiendo abarcar continentes, con lo que no siempre se interconectan con medios físicos; es aquí donde intervienen los medios aéreos por ejemplo los satélites o las microondas.

1.3. Clasificación de redes por su topología

Son las distintas maneras en que una red puede organizarse, para lograr una intercomunicación entre todos los dispositivos que pertenecen a una red. Toda topología de red cuenta con la parte física y lógica.

Topología Física

Es la manera en que se disponen el medio de transmisión para interconectar los elementos de la red.

(a)Estrella. Los nodos se conectan a un nodo central, el cual se encarga de la comunicaciones en la red (véase Figura 1.6). Adquiriendo una gran importancia el nodo central ya que él es único que puede comunicar a los equipos y si este presenta algún fallo la red colapsaría.

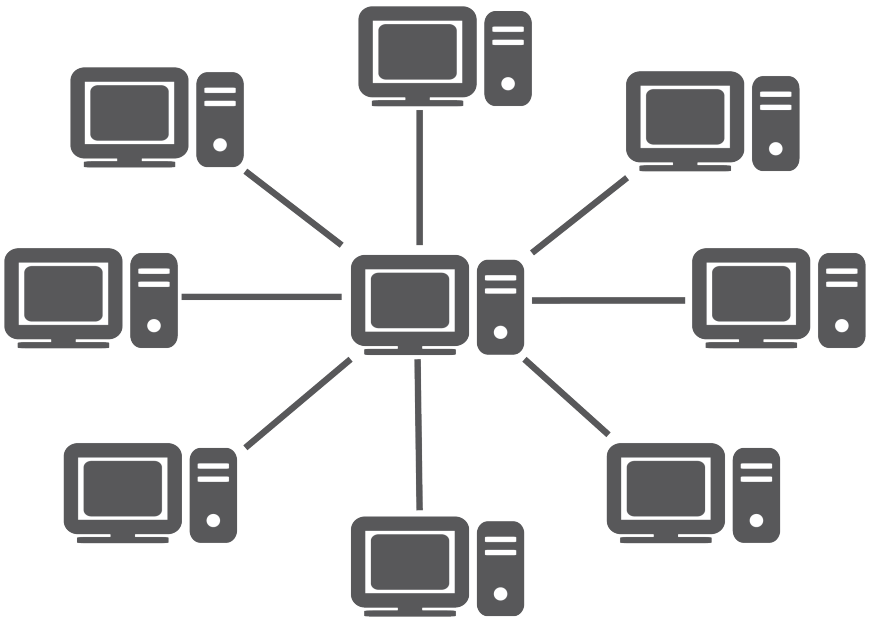

Figura 1.6: Topología Estrella

[3]Estándar IEEE 802.11-2007 IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. https://standards.ieee.org/standard/802_11-2007.html

(b)Bus. Todos los nodos se conectan a un único canal de transmisión. Los mensajes son escuchados por todos los nodos pero solo son aceptados por el nodo receptor de ese mensaje. Con un fallo en el medio común toda la comunicación en la interconexión es perdida, véase Figura 1.7.

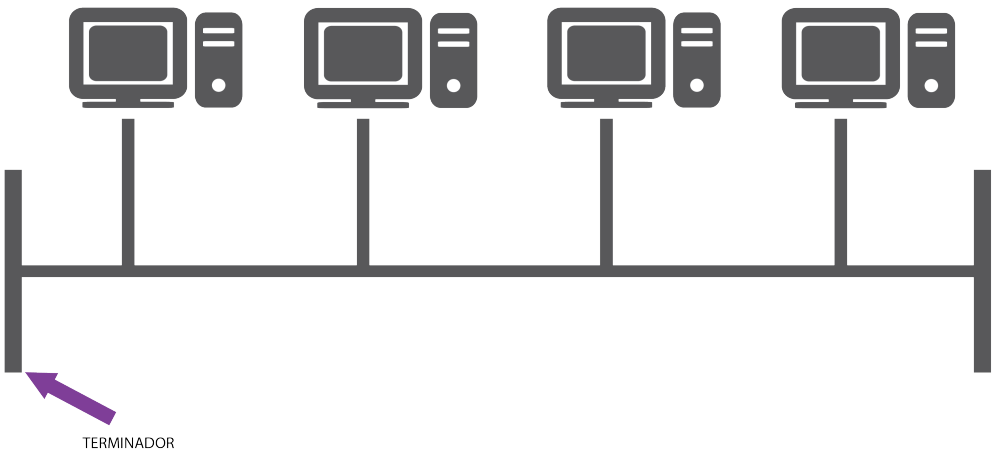

Figura 1.7: Topología Bus

(c)Árbol. Podemos considerar a esta topología como el encadenamiento de diferentes interconexiones en bus con diferentes longitudes, las cuales constituyen las ramas de interconexión. En esta topología resalta la importancia de cada uno de los nodos que funge como nodo central para los nodos más cercanos. Cabe mencionar que la interconexión en árbol sigue una jerarquía ya que la raíz es la que comunica a todas las hojas y ramas del árbol, véase Figura 1.8.

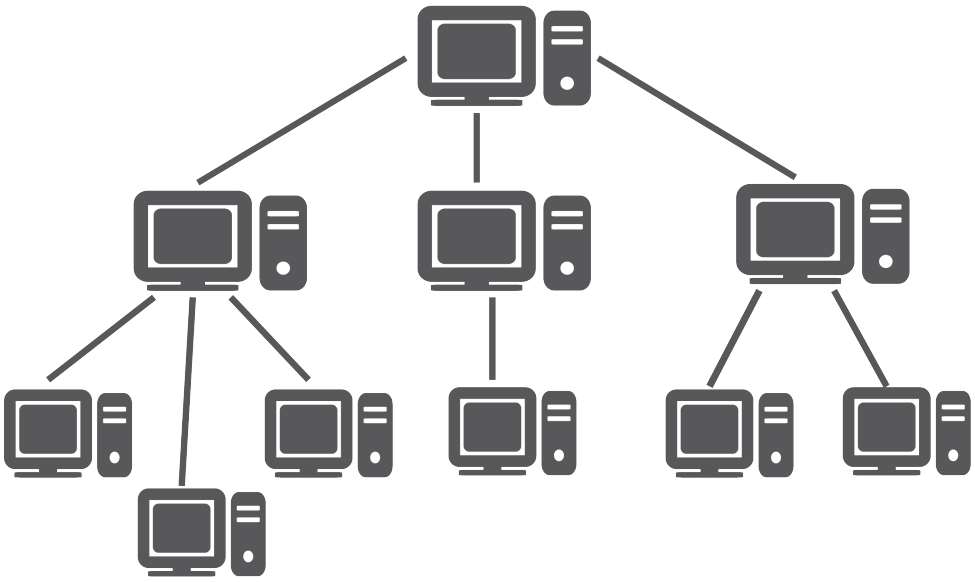

Figura 1.8: Topología Árbol

(d)Anillo. Todos los nodos se conectan en serie uno tras otro aparentando una conexión de Bus pero conectando el primer nodo con el último nodo de la red. En esta interconexión los mensajes solo tiene una dirección, por lo que un mensaje es transmitido por todos los nodos hasta llegar al nodo destino. Si un nodo de todo la red es comprometido la red queda incomunicada, véase Figura 1.9.

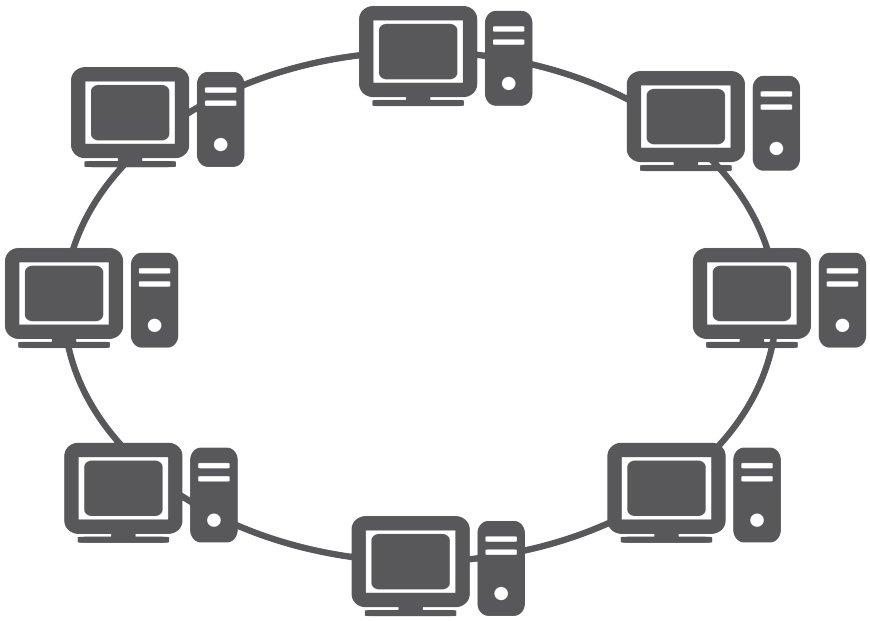

Figura 1.9: Topología Anillo

(e)Malla. Esta interconexión proporciona múltiples conexiones entre los nodos, es decir todos contra todos.Concibiendo múltiples canales de comunicación entre dos nodos. Malla completa se presenta cuando todos los nodos de la red están conectados con todos los demás, y malla parcial cuando existen varias rutas de comunicación, pero no se cubren todos los nodos, véase Figura 1.10.

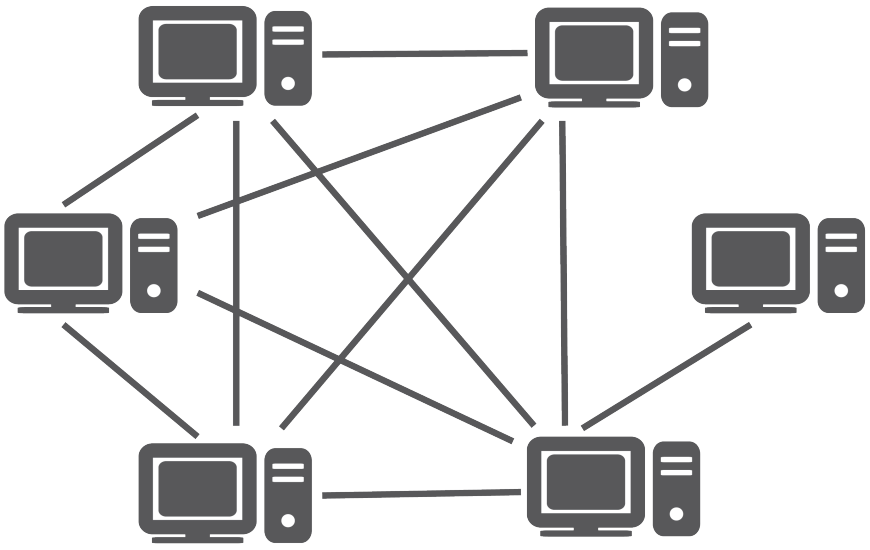

Figura 1.10: Topología Malla

Topología lógica

Conjunto de reglas que define la manera en que se transmiten los datos en la red. Un ejemplo, es la implementación de tokens para poder tener acceso a la red, el token se distribuye de equipo a equipo; si un equipo no tiene nada que enviar, pasa el token al siguiente equipo, esto es utilizado en *token ring*[4]. También tenemos el

[4]Token ring está basado en el estándar de red IEEE 802.5, todas las computadoras de la red LAN están conectadas de mane de un anillo lógico y fue descontinuado a finales de los 90.

acceso múltiple donde los equipos utilizan el mismo medio de transmisión, donde se escuchan todas las peticiones de los equipos y para mejorar la comunicación entre estos cada equipo tiene una MAC[5] que sirve para identificar al emisor y receptor.

1.3.1. Segmentación de red

Una segmentación de red es una forma de incrementar la seguridad y además poder otorgar diferentes grados, de dicha seguridad, al crear distintas redes, en este caso, subreredes. Además, se logra una mejor gestión, debido a que se puede tener menos dominios de colisión y se puede contar con un mejor control.

VLAN. Acrónimo Virtual Local Área Network (Red de Área Local Virtual), es una o varias redes dominio de broadcast en varios más chicos, también por seguridad, se utilizan para tener separadas las redes que son prioritarias de otras redes.

Las ventajas que proporcionan las VLANs son entre otras:

1. Mayor flexibilidad y mejor gestión de recursos, al facilitar el cambio y movimiento de los dispositivos en la red.
2. Facilidad de localización y aislamiento de fallas.
3. Mejora en cuanto a seguridad, debido a la separación de dispositivos en distintas VLANs.
4. Control de tráfico de broadcast.
5. Separación de protocolos.

Clasificación de VLAN

- **VLAN de nivel 1** (por puerto). También conocida como port switching. Se especifica que puertos del switch pertenecen a la VLAN, los equipos de dicha VLAN son los que se conectan a esos puertos. Los puertos se configuran tagged y untagged lógicas que coexisten dentro de una única red física, su principal utilidad es dividir un único dependiendo del puerto, ya que los puertos que sirven como troncales se taggean a cada VLAN existente.
- **VLAN de nivel 2** (por dirección MAC). Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que configurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se podría conectar a otro puerto de ese u otro dispositivo y no se pierde el servicio. El principal inconveniente es que si hay cientos de usuarios habría que asignar los equipos uno a uno.
- **VLAN de nivel 3** (por direcciones de subred). La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones de trabajo quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red estarán en múltiples VLAN.

VPN

Acrónimo del inglés Virtual Private Network, es una red super puesta que implementa mecanismos de seguridad para la conexion entre dos puntos. Puede implementarse para la conexion a recursos de una red que se encuentran en una localizacion geografica diferente, ademas que toda la informacion trasmitida entre los puntos es totalmente cifrada.

Las ventajas que proporciona una VPN son entre otras:

- Comunicación cifrada
- Acceso a contenido regional
- Transferencia segura de datos

[5] El control de acceso a medios (MAC) se refiere al método utilizado para asignar el uso del medio entre las computadoras y dispositivos en la red.

Clasificación de VPN

- **VPN de acceso remoto.** Permite que los usuarios se conecten a una red privada para que tengan acceso a servicios y recursos de forma remota, avitualmente es de uso comercial o personal.
- **VPN site-to-site.** Permite que areas de trabajo u organizaciones puedan conectarse a otras areas de trabajo localizadas en otro punto geografico, con la finalidad de compartir recursos o servicios entre si. Este tipo de VPN habitualmente lo implementan las empresas, pero pueden ser empleadas por organizaciones pequeñas.

1.4. Modelos de referencia y protocolos

Modelo de referencia OSI

Del inglés Open Systems Interconnection[?], el modelo OSI se basa en la comunicación abierta entre sistemas. Este modelo cuenta con siete capas, véase Figura 1.11:

- Capa Física. Esta capa se encarga de la transmisión de bits a través del medio físico. Se definen las características eléctricas y mecánicas de la línea de transmisión.
- Capa de Enlace. Asegura la transmisión de los datos entre dos nodos. Imponiendo los métodos de direccionamiento, detección y recuperación de errores.
- Capa de Red. Controla la ruta de la comunicación de datos entres los nodos, determinando la ruta a seguir por los paquetes de emisor a receptor.
- Capa de Transporte. Su función básica es aceptar datos de la capa superior, así como asegurar el envío de paquetes de un extremo a otro.
- Capa de Sesión. Permite a los usuarios establecer sesiones entre ellos, ofreciendo el control del diálogo de la comunicación, el manejo de tokens y la sincronización.
- Capa de Presentación. Se enfoca en la sintaxis y semántica de la información transmitida.
- Capa de Aplicación. Proporciona servicios de información distribuida.

Figura 1.11: Capas del modelo OSI

Modelo de referencia TCP/IP

Como su nombre lo indica este modelo de referencia está constituido principalmente por sus dos protocolos. Este modelo se definió por primera vez en 1974 por Vint Cerf y Robert Kahn[6]; después se refinó y definió como estándar en la comunidad de Internet (R. Braden, 1989)[7]. Este modelo define las siguientes cuatro capas, véase Figura 1.12:

- Capa de Enlace. Describe los enlaces que se deben de llevar a cabo para la conexión entre los hosts y los enlaces de transmisión.
- Capa de Internet. Su función es proveer procedimientos que permitan que la información viaje a través de la red, con la finalidad de entregar los paquetes IP donde deben de llegar. En esta capa se implementa el protocolo de internet y el protocolo de mensajes de control de internet.
- Capa de Transporte. Implementa los protocolos TCP y UDP para establecer una conexión entre el origen y destino.
- Capa de Aplicación. Contiene la lógica necesaria para traducir los datos enviados a las distintas aplicaciones finales de usuario.

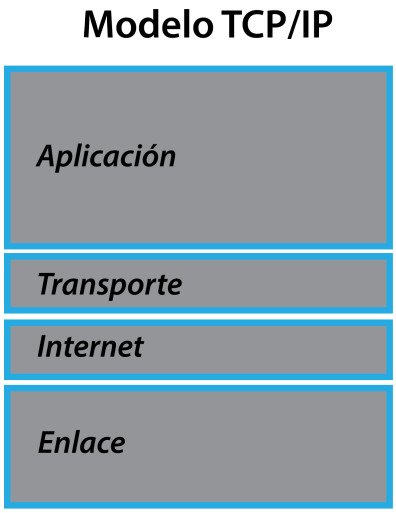

Figura 1.12: Capas del modelo TCP/IP

Protocolo TCP

Del inglés Transmission Control Protocol, es un protocolo orientado a la conexión el cual está especificado en el RFC 793[**?**]. El propósito de TCP es proveer un flujo en la comunicación de extremo a extremo de manera confiable. El encabezado TCP consiste en 20 octetos como mínimo véase Figura 1.13, los campos son los siguientes:

- Puerto origen: Usuario TCP origen.
- Puerto destino: Usuario TCP destino.
- Número de secuencia: Número de secuencia del primer octeto excepto si el indicador SYN está presente. En dado caso que SYN esté presente el número de secuencia es ISN + 1.
- Número de confirmación: Contiene el número de secuencia del siguiente octeto que la entidad TCP espera recibir.
- Longitud de la cabecera: Número de palabras de 32 bits en la cabecera. Reservados: Bits reservados para un uso futuro.

[6]S.Tanenbaum, Andrew y J.Wetherall, David. (2012). Redes de computadoras. México: Pearson Educación.

[7]R. Braden. (1989). Requirements for Internet Hosts -- Communication Layers. 10/04/2020, de Internet Engineering Task Force Sitio web: https://tools.ietf.org/html/rfc1122\#section-4.2

- Indicadores: URG: El campo puntero urgente es válido. ACK:el campo de confirmación es válido. PSH: función de carga. RST: puesta a cero de la conexión. SYN: sincronizar los números de secuencia. FIN: emisor no tiene más datos.
- Ventana: Asignación de créditos de control de flujo, medido en octetos.
- Suma de verificación: Complemento a uno de la suma módulo 216-1de todas las palabras de 16 bits en el segmento más una pseudo-cabecera. Puntero urgente: señala un octeto que sigue a los datos urgentes llegan.
- Opciones: Si está presente, solamente se define una opción que especifica el tamaño máximo del segmento que será aceptado.

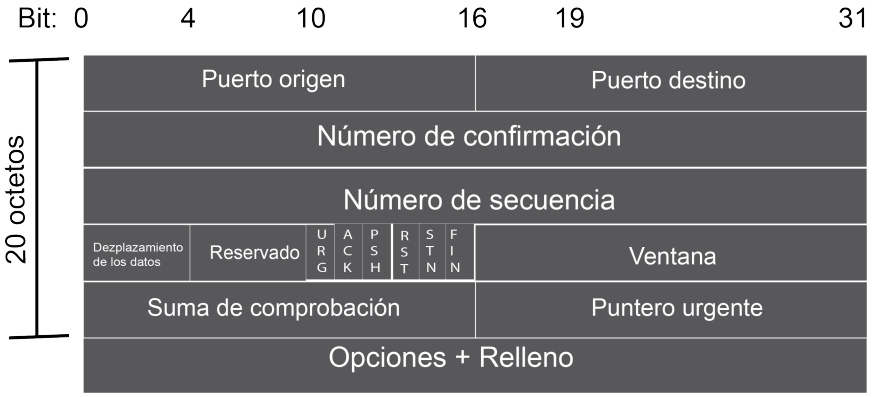

Figura 1.13: Datagrama de TCP

Protocolo UDP

Del inglés Use Datagram Protocol, este protocolo de transporte sin conexión proporciona una forma para que las aplicaciones envíen datagramas IP sin la necesidad de estar conectados a internet. El protocolo UDP se describe en el RFC 768[**?**]. Básicamente este protocolo no garantiza la entrega y la protección, no hace más que enviar paquetes entre aplicaciones. UDP envía encabezado de 8 bytes seguido de la carga útil. La cabecera UDP está incrustada por encima de la cabecera de IP incrementando los puertos de origen y destino. Gracias a estos dos puertos la capa de transporte no sabria que hacer con cada paquete que es enviado. El encabezado UDP está constituida como se muestra en la Figura 1.14.

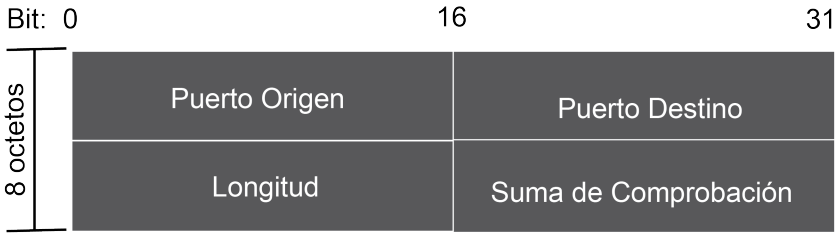

Figura 1.14: Datagrama UDP

La cabecera incluye un puerto origen y un puerto destino. Longitud contiene el tamaño del segmento UDP entero, incluyendo la cabecera y los datos. La suma de comprobación es el mismo algoritmo utilizado para IP y TCP, este campo es opcional.

Protocolo IP

El protocolo IP (Internet Protocol) es utilizado como base del internet. Este protocolo proporciona un servicio de distribución de paquetes (datagramas) de información orientado a la no conexión, por lo que los paquetes pueden

viajar por diferentes trayectorias para llegar a su destino sin garantizar la recepción del mismo. Algunas de las principales características de este protocolo son las siguientes:

- Protocolo orientado a no conexión. Fragmentación de paquetes de necesitarlo.
- Direccionamiento a través de direcciones lógicas IP.
- El tiempo de un paquete no recibido en la red es finito.
- El tamaño máximo del datagrama es de 65635 bytes.

Un datagrama tiene el formato mostrado en la Figura 1.15. Con los campos siguientes:

- Versión: Indica que versión del protocolo se está empleando.
- Longitud de la cabecera Internet: Expresada en palabras de 32 bits.
- Tipo de servicio: Contiene los parámetros de seguridad, prioridad, retardo y rendimiento. Longitud total: Tamaño total del datagrama, expresado en octetos.
- Identificador: Número de secuencia que, junto a la dirección origen, destino y protocolo usado, se emplea para identificar de forma única un datagrama.
- Indicadores: Constituido por 3 bits, solo dos bits están definidos. El primero es para segmentación y reensamblado. Y el otro bit prohíbe o no el fragmentado.
- Desplazamiento del Fragmento: Muestra el lugar donde se sitúa el fragmento dentro del datagrama original.
- Tiempo de vida: Tiempo en segundos, que se le permite a un datagrama permanecer en la red. Cada dispositivo de encaminamiento que procese el paquete modificará el tiempo de vida en al menos una unidad, notando que el tiempo de vida está relacionado con los saltos que lleva en el transporte del datagrama.
- Suma de comprobación de la cabecera: Contiene un código de detección de errores que solo es aplicado a la cabecera, esto por los cambios posibles durante el transporte del datagrama. Este valor es calculado y verificado por cada dispositivo de encaminamiento.
- Dirección origen y destino: Codificada para permitir asignación variable de bits para poder especificar la red y sistema final.
- Opciones: Contiene las opciones solicitadas por el usuario.
- Relleno: Asegura el tamaño de la cabecera del datagrama. Datos: Este campo debe de tener una longitud múltiplo de 8 bits. Un datagrama tiene la longitud máxima de 65.5355 octetos.

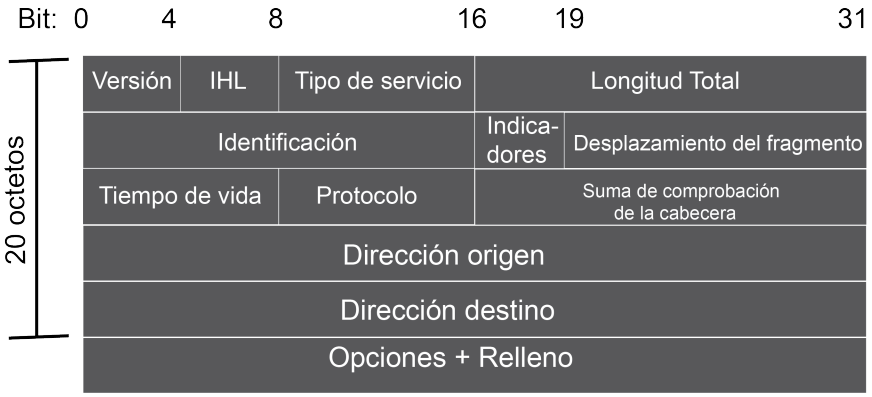

Figura 1.15: Datagrama IP

1.5. Medios de transmisión

El medio de transmisión es el camino por el cual viaja el mensaje de emisor a receptor, estos se clasifican en dos tipos guiados y no guiados. En ambos casos, la información viaja a través de ondas electromagnéticas.

1.5.1. Medios de transmisión guiados

En este medio de transmisión las ondas electromagnéticas viajan por un medio sólido.

(a)Cable coaxial. Está formado por un alambre de cobre o aluminio rígido como su núcleo, rodeado por un material aislante (dieléctrico) que a su vez está forrado por una pantalla conductora fuertemente trenzada. La malla conductora está cubierta por una funda protectora de plástico. Véase Figura 1.16.

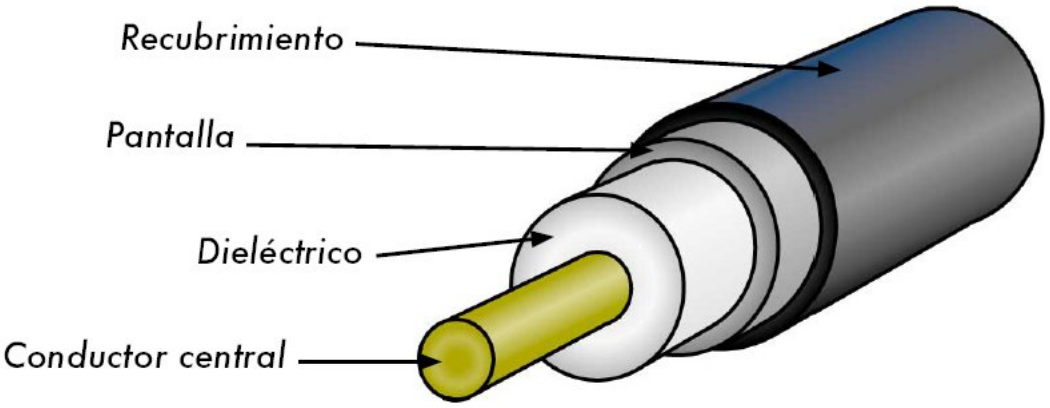

Figura 1.16: Vista seccionada de un cable coaxial

Gracias a los elementos que lo constituyen, el cable coaxial tiene un alto ancho de banda e inmunidad al ruido eléctrico, véase Tabla 1.2. Este tipo de medio era muy utilizado para las líneas de larga distancia, pero fue sustituido por fibra óptica en largas distancias. Sin embargo en la actualidad el cable se sigue empleando para la televisión por cable y las redes de área metropolitana.

Tabla 1.2: Características de cable coaxial

Cable	Caracteristicas
10-BASE-5 Cable coaxial grueso	Velocidad de transmisión: 10 Mbs/seg Segmentos: Máximo de 500 metros
10-BASE-2 Cable coaxial fino	Velocidad de transmisión: 10 Mbs/seg Segmentos: Máximo de 185 metros
10-BROAD-36	Velocidad de transmisión: 10 Mbs/seg Segmentos: Máximo de 3600 metros

(b)Cable de par trenzado. Actualmente es el tipo de cable más utilizado en redes de área local, su origen fue una solución para el reuso del cableado existente de redes telefónicas. Cada uno de los hilos del cable par trenzado está hecho de cobre y con una cubierta de aislante. Las normativas del cableado estructurado clasifican los diferentes tipos de cable de pares trenzados en categorías dependiendo de sus características, véase Tabla 1.3.

- **No apantallado.** El UTP (Unshielded Twisted Pair) es un cable de par trenzado que está constituido tan sólo de los alambres y aislante. Tal como se muestra en la Figura 1.17.

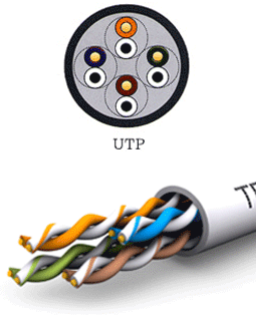

Figura 1.17: Cable UTP

No posee ninguna protección adicional al recubrimiento de PVC, teniendo una impedancia de 100 Ohm. Su conector es el RJ45 pero también puede usarse otros (RJ11,DB25,DB11,etc.) dependiendo del adaptador de red. El segmento máximo de longitud de cable es de 100 metros.

Tabla 1.3: Categorías y características de cable UTP

Tipo	Velocidad	Ancho de Banda
Categoría 1	Cable Telefónico	$<$ 0.5 MHz
Categoría 2	Hasta 4 Mbps	4 MHz
Categoría 3	Hasta 10 Mbps	16 MHz
Categoría 4	Hasta 20 Mbps	20 MHz
Categoría 5	Hasta 100 Mbps	100 MHz
Categoría 5E	Hasta 1000 Mbps	100 MHz
Categoría 6	Hasta 1000 Mbps	250 MHz
Categoría 6A	Hasta 10Gbps	500 MHz
Categoría 7	Hasta 10 Gbps	600 MHz
Categoría 7A	Hasta 100 Gbps	1000 MHz

- **Blindado o apantallado.** El cable STP (Shielded Twisted Pair), este cable tiene una malla conductora por cada par trenzado que apantalla las interferencias y ruidos eléctricos véase en la Figura 1.18.

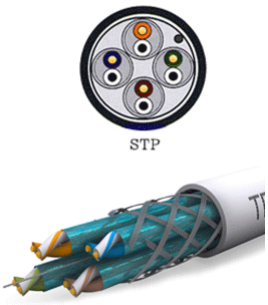

Figura 1.18: Cable STP

La impedancia es de 150 Ohms, el STP tiene mayor protección contra perturbaciones externas que el UTP, pero tiene un mayor costo y su instalación no es tan sencilla. Para que la pantalla protectora sea más eficaz requiere una configuración de interconexión con tierra. Los conectores usualmente utilizados en este tipo de par trenzado es el RJ49.

Cable FTP (Foiled Twisted Pair) este tipo de cable no tiene un apantallado por cada par de cables sino que usa un apantallado global para mejora sus nivel de protección a interferencias véase en la Figura 1.19. Tiene una impedancia de 120 Ohm y los conectores que puede usar son los RJ45.

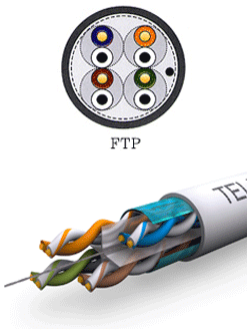

Figura 1.19: Cable FTP

Principales Tipos de Fibra Óptica

La fibra óptica tiene forma cilíndrica y está constituida por tres secciones: el núcleo, el revestimiento y la cubierta como se muestra en la Figura 1.20.

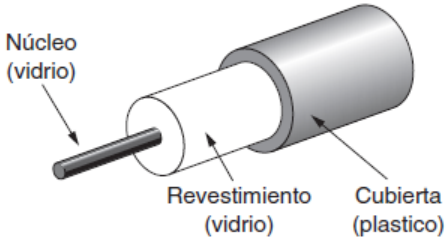

Figura 1.20: Elementos de la fibra óptica

El núcleo es la sección más interna por la cual se hace pasar un haz de luz, está constituido por una o varias hebras muy finas de cristal y tiene un diámetro entre 8 y 100 [mm]. El revestimiento cubre al núcleo y actúa como reflector confinado el haz de luz del núcleo, su recubrimiento le proporciona protección. La fibra óptica puede manejar mayores anchos de banda, gracias a la baja atenuación solo es necesario repetidores aproximadamente cada 50 [km] en líneas extensas contra los 5 [km] que necesitan los repetidores para el uso de cobre.

La fibra se puede conectar de tres formas diferentes:

1. Termina en conectores e insertarse en clavijas de fibra. Se pierde entre 10 y 20 % de luz por el uso de conectores, pero se puede reconfigurar los sistemas mucho más fácil.

2. Se puede empalmar en forma mecánica, simplemente se acomodan dos extremos cortados uno junto a otro en un manguera especial y se sujetan en su lugar, con una pérdida del 10 % de luz.

3. La fusión de dos piezas de fibra para formar una conexión sólida.Este empalme es tan bueno como una sola fibra, pero también se produce un poco de atenuación.

Las dos principales fuentes de luz para producir las señales son con LED o diodos emisores de luz y láseres semiconductores.

(a)Monomodo. Esta fibra óptica sólo emplea un modo de propagación, tiene solamente una longitud de onda de luz permitiendo únicamente un haz de luz, no rebota en las paredes del cable de la fibra sino que viaja longitudinalmente al cable. Por esto mismo las pérdidas por reflexión son menores, por lo que la fibra puede

ser mucho más larga que en el multimodo alcanzando una distancia máxima de 20 [km]. Existen dos tipos de fibras monomodo:

- OS1 Presenta una protección interna ajustada, está constituida por un cable multifibra de 900 micras y una fibra ajustada de nylon, hytrel o PVC, esto permite su aplicación en interiores. Su atenúa es ligeramente superior a la del tipo OS2 y tiene 2 [km] -10 [km] como distancia máxima para la transmisión.
- OS2 Este tipo de fibra presenta un tubo suelto, es muy usado en exteriores donde puede moverse libremente gracias a su tubo holgado. Tiene una atenuación de 0.4[dB/km] y 200[km] como distancia máxima.

(b)Multimodo de índice de gradiente gradual. Utiliza variaciones en la composición del vidrio del núcleo para poder compensar las diferentes longitudes de las trayectorias de los haces de luz. Este tipo de fibra ofrece un ancho de banda mucho mayor que la de índice escalonado. La principal implementación de esta fibra es en las redes de área local, CCTV y otros sistemas de seguridad.

(c)Multimodo de índice escalonado. En este tipo de fibra, el núcleo y el revestimiento son construidos de distintos materiales ópticos. Teniendo una mayor atenuación, generando que la información que es trasmitida por este medio sea lenta, la dispersión que presenta por las diferentes distancias que recorren los distintos modos del haces de luz reduce la implementación de este tipo de fibra, las fibras de plástico implementan este tipo de índice y son utilizadas para la transmisión de radio y televisión.

A continuación se describen los tipos de fibra multimodo:

- OM1 Tiene un núcleo de 62.5 [µm], permite distancias de 100[m] a 1Gbps. Está optimizada para su uso con emizores de luz basadas en LED que se encuentran en sistemas de velocidad lenta.
- OM2 Su núcleo es de 50[µm], no se encuentra optimizada para emisores con láser. Fue creada en los años 80.
- OM3 Su núcleo es de 50[µm], es optimizada para emisores con láser. Permite 40Gbps en 240[m] y 100Gbps en 75[m], frecuentemente implementada en centro de datos.
- OM4 Tiene un núcleo de 50[µm], permite 40Gbps en 350[m] y 100Gbps en 100[m].
- OM5 Su núcleo es de 50[µm], permite 40Gbps en 440[m] y 100Gbps en 100[m].

Conectores de fibra óptica

Los conectores se encuentran en los extremos de la fibra óptica, permitiendo la conexión y desconexión de la fibra sin la necesidad de tener un empalme. Garantizando que la fibra se encuentre alineada para que la conexión sea la correcta. Existen los conectores ST(Straight Tip), FC (Conector de Furrele), LC (Conector Pequeño) y SC (Conector Cuadrado); en donde, estos dos últimos, son los más utilizados, gracias a su tamaño, así como el soporte para fibras multimodo y monomodo, véase Figura 1.21.

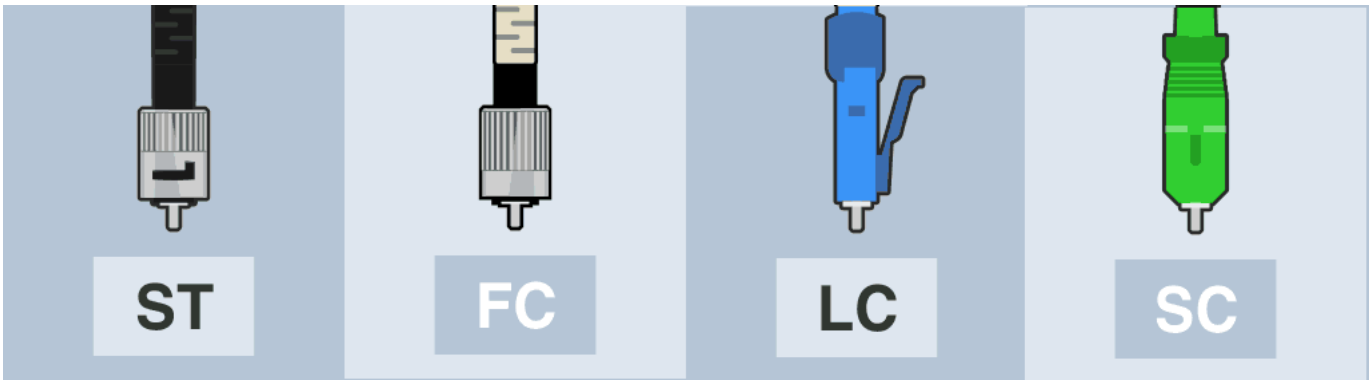

Figura 1.21: Conectores de fibra óptica

1.5.2. Medios de transmisión no guiados

En este tipo de medios, la transmisión y recepción se realiza por medio de una antena, gracias a la transmisión de ondas electromagnéticas que se propagan a través del aire; esto es una gran ventaja en la movilidad de los dispositivos que necesitemos interconectar, pero también presentan desventajas, ya que el medio es compartido por distintas ondas, así como la reflexión que presentan dichas ondas en los obstáculos físicos.

(a)Radiotransmisión. Las ondas de radio frecuencia (RF) son fáciles de generar y pueden recorrer distancias largas así como penetrar edificios, por lo que son implementadas en la comunicación. Gracias a que las ondas son omnidireccionales, el transmisor y el receptor no tienen que estar alineados perfectamente para que la información vaya de un punto a otro. Las ondas de radio de baja frecuencia tienden a seguir el recorrido de la geodesia de la tierra (véase Figura 1.22), pudiendo atravesar obstáculos físicos pero con velocidades de transmisión bajas. En el caso de las ondas de alta frecuencia, estas son absorbidas por la tierra por lo que se tiene que mandar con dirección a la ionosfera para que esta la rebote (véase Figura 1.22), y se pueda transmitir a mayor distancia.

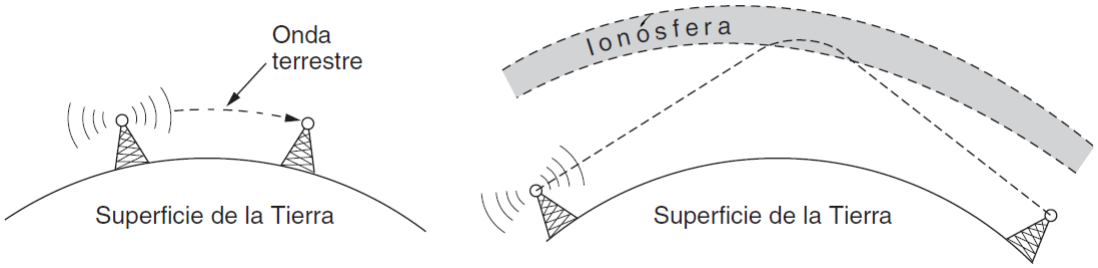

Figura 1.22: Propagación de baja y alta frecuencia

(b)Transmisión de Microondas. Las microondas son un tipo de onda que viajan en línea recta por lo que se podría enfocar un haz. Esto es posible concentrando toda la energía por medio de una antena parabólica, la alineación entre las dos antenas, emisora y receptora, debe de ser precisa. Gracias a la direccionalidad de estas ondas, se puede tener varios receptores o emisores alineados, sin tener interferencia entre las antenas (véase Figura 1.23).

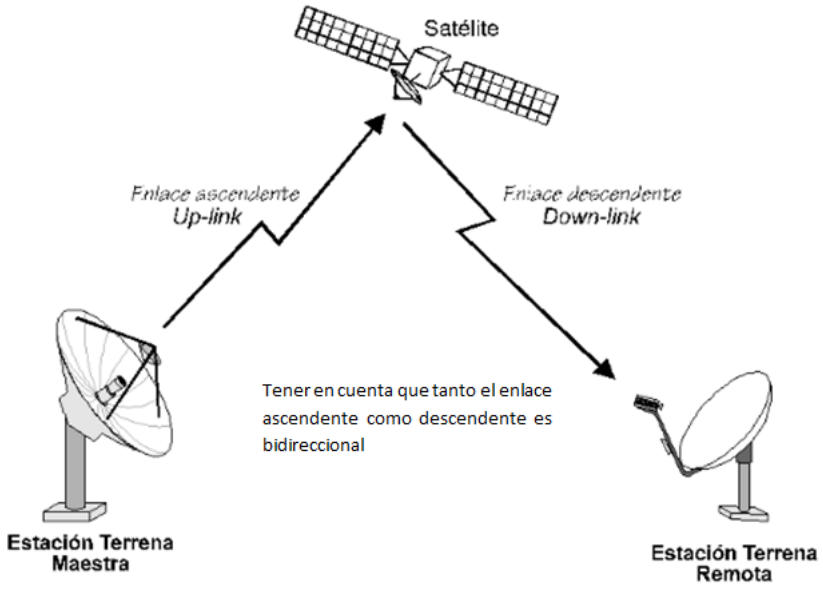

Figura 1.23: Conexión extremo a extremo de microondas

La comunicación por microondas se utiliza tanto para la comunicación telefónica de larga distancia, teléfonos móviles, televisión, entre otros. Una de las principales desventajas que tienen las microondas, es que no pueden atravesar bien los obstáculos. Por lo que es necesario la instalación de una antena repetidora véase (véase Figura 1.24).

Figura 1.24: Antena repetidora de microondas

1.6. Estándares y organismos reguladores

(a)ISO.

De las siglas en inglés International Organization for Standardization(ISO), y se dedica a la creación de normas y/o estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios. Fue fundada en 1926 como Federación Internacional de Asociaciones de Normalización Nacionales (ISA), con sede en Ginebra, Suiza.

ISO es una organización internacional no gubernamental independiente con una membresía de 164 organismos nacionales de normalización. A través de sus miembros, reúne a expertos para compartir conocimientos y desarrollar estándares internacionales, basado en el consenso y relevantes para el mercado que apoyan la innovación y brindan soluciones a los desafíos mundiales.

Actualmente se cuentan con 23126 normas internacionales que cubren casi todos los aspectos de la tecnología y la fabricación.

(b)IEEE.

El Instituto de Ingenieros en Electricidad y Electrónica(IEEE) fue fundada en New York, el 13 de mayo de 1884, por un grupo de profesionales en el área, como Thomas Alva Edison, Alexander Graham Bell y Franklin Leonard Pope. La contribución científica del IEEE, constituye el 30 % de la información técnica escrita sobre los avances tecnológicos a nivel mundial, que promueven la teoría y la práctica de la electrotecnología, fomentando la innovación tecnológica y la excelencia, para el beneficio de la humanidad.

(b.1)IEEE Sección México.

Se registró en enero de 1904 y, constituida el 29 de junio de 1922 en el AIEE (American Institute of Electrical Engineers) en Estados Unidos. Es la tercera sección más antigua y la fundadora de la región 9. Cuenta con una membresía de 1200 Ingenieros y estudiantes de Ingeniería. Tiene 12 capítulos técnicos y 76 ramas estudiantiles, así como dos grupos de afinidad: La mujer en la Ingeniería y Jóvenes profesionales.

Desarrolla actividades técnicas, educacionales y profesionales que promuevan la teoría y la práctica de la electrotecnología para el desarrollo personal y profesional en sus integrantes.

(c)ANSI.

El Instituto Nacional Estadounidense de Estándares, es una organización privada sin fines de lucro dedicada a apoyar los estándares voluntarios de Estados Unidos. Esta organización es miembro de la ISO y la IEC (Comisión Electrónica Internacional). Fue fundado el 19 de octubre de 1918. Compuesto por agencias gubernamentales, organizaciones, empresas, organismos académicos e internacionales y particulares.

1.6.1. ANSI/TIA/EIA

(i)ANSI/TIA/EIA-568 Cableado de telecomunicaciones para edificios comerciales.

Este estándar junto con sus actualizaciones especifican los requerimientos del cableado para los edificios comerciales, independientemente de las aplicaciones y el proveedor del servicio de internet. Se estima que la vida productiva del sistema de cableado de un edificio comercial debe estar entre 15 a 25 años, con escalabilidad y compatibilidad con la actualización de las tecnologías, véase Figura 1.25.

Los subsistemas que conforman el cableado estructurado son:

1. Entrada del edificio.
2. Cuarto de equipos.
3. Cableado Vertical (backbone).
4. Cuarto de Telecomunicaciones.
5. Cableado Horizontal.
6. Área de trabajo.

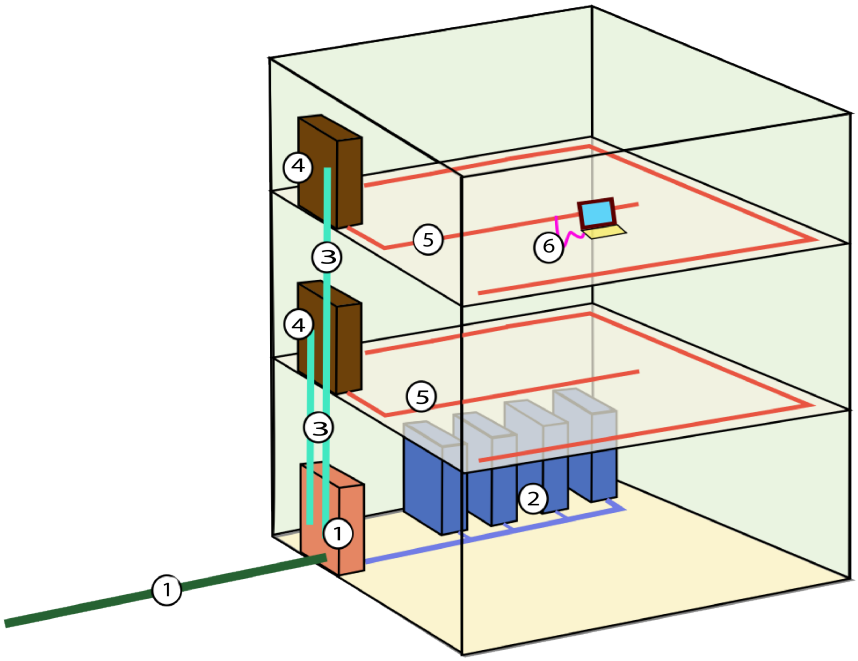

Figura 1.25: Subsistemas del Cableado Estructurado

I.-Entrada del edificio. Está constituida por cables, hardware de conexión, dispositivos de protección y otros para interconectar al proveedor (ISP locales, otro edificio en el caso de ser un campus o ambos) y el cableado del cliente. Su diseño debe de estar basado en la norma ANSI/TIA/EIA-569-A. Este estándar recomienda que la entrada del edifico sea en un lugar seco y cerca del backbone.

II.-Cuarto de Equipos. Contiene el equipo que administra los servicios en todo el edificio, pueden ser conmutadores PBX, servidores de red, servidores web, centrales de video, etc., así como el cableado necesario para distribuir los servicios a todo el edificio.

En su diseño y ubicación, se deben considerar:

- Posibilidades de actualizar y agregar más equipos, así como el posible crecimiento del cuarto de equipos.
- Facilidad de acceso para los equipos de gran tamaño.

- Estar cerca del cableado vertical.
- Estar lejos de fuentes de interferencias electromagnética.
- La estimación de espacio para el cuarto es de $0.7[m^2]$por cada $10[m^2]$ de área utilizable del edificio (véase la Tabla 1.4).
- La temperatura se debe mantener entre los 18 y 24 grados centígrados.

Tabla 1.4: Estimación del cuarto de equipos

Número de Estaciones de Trabajo	Dimensiones del Cuarto de Equipos$[m^2]$
1-100	10
101-400	20
401-800	40
801-1200	70

III.-Cableado Vertical (*backbone*). El propósito principal de este subsistema es proporcionar las interconexiones necesarias entre los cuartos de telecomunicaciones, el cuarto de equipos y la conexión con otros edificios. Es necesario que soporte las demandas de conexión en un lapso aproximado de 3 a 10 años, tomando en cuenta la actualización y escalabilidad del cableado.

IV.-Cuarto de Telecomunicaciones. Es el encargado de realizar la interconexión del cableado horizontal y vertical. Existirá un cuarto de telecomunicaciones en cada piso donde se encuentre una área de trabajo funcionales con el suficiente espacio para alojar el equipo y el cableado para la interconexión con el cableado horizontal, garantizando la escalabilidad y/o actualización del equipo para las conexiones.

V.-Cableado Horizontal. Es el cableado que se extiende desde el área de trabajo, los cables de conexión o puentes con el cuarto de telecomunicaciones, la recomendación es implementar una topología en estrella. El término horizontal se emplea ya que, actualmente el cable se extiende horizontalmente por el suelo o techo del edificio. Para el diseño de este cableado se recomienda contemplar la escalabilidad de la organización y el mantenimiento del mismo ya que el cableado horizontal habitualmente es un difícil acceso, esto para reducir el posible cambio o eliminación del cableado.

VI.-Área de trabajo. Es la zona donde están ubicados los distintos puestos de trabajo en la red. Comprende todo aquello que se conecta desde la toma de telecomunicaciones, como computadoras, terminales de datos y teléfonos, así como adaptadores, filtros o acopladores en caso de ser requeridos. El cableado que se extiende a partir de la roseta de conexión no es permanente, por lo que los cambios en esta zona son rápidos y sencillos.

(i)Tipos de cable de conexión (cable UTP). Los cables de conexión son aquellos que se implementan en el área de trabajo, cableado horizontal, cuarto de telecomunicaciones y cuarto de equipos. Para interconectar los equipos activos y pasivos que conforman a la red. Existen dos tipos de cables: los cruzados y los directos, para construir estos cables se utiliza las normas T-568A y/o T-568B (véase configuración en Figura 1.26), proporcionan el esquema para la terminación de los cables de red en las rosetas y RJ45.

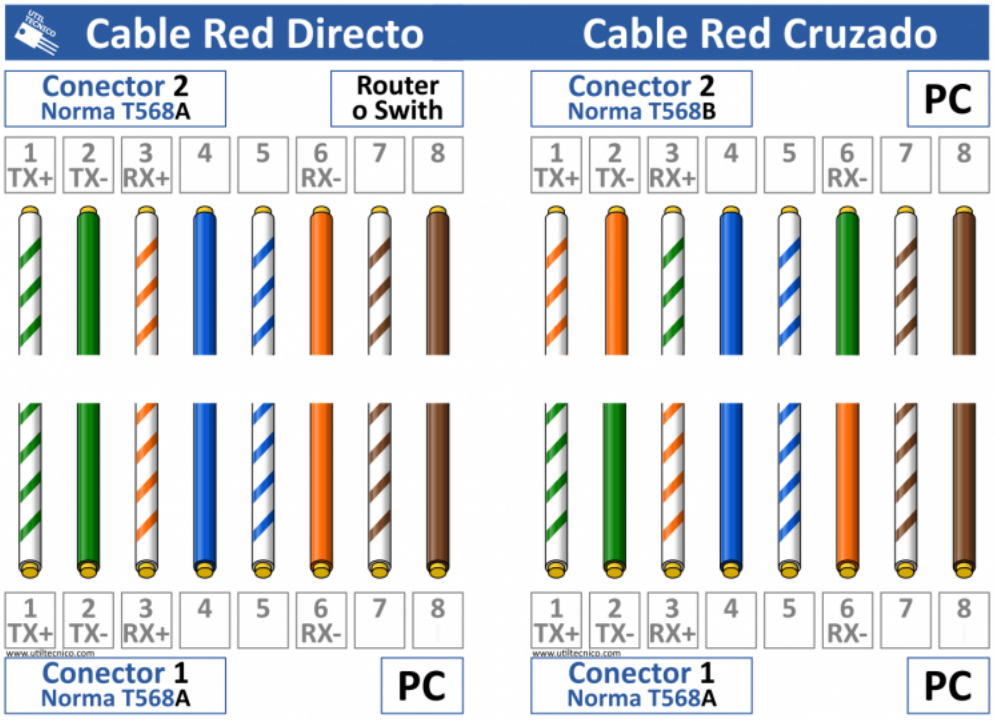

Figura 1.26: (a) Cable Cruzado y (b) Directo

Los cables de **conexión directos** son utilizados para interconectar equipos diferentes, como pueden ser una PC y un switch. Para este cable se debe de usar la misma norma en cada extremo ya sea A o B. Para una **conexión cruzada** se implementa la norma A y B, una en cada extremo. Esta configuración se utiliza para la conexión de equipos iguales como por ejemplo dos PC o la conexión entre switch. Cabe mencionar que sólo dos pares son los que tienen importancia en las conexiones, el par de transmisión TX+ TX- y el par de recepción RX+ RX-.

(ii)ANSI/TIA/EIA-569 Rutas y espacios de telecomunicaciones para edificios comerciales.

Este estándar tiene como objetivo definir los espacios o áreas del edificio, así como las canalizaciones para el cableado interno. Las áreas de trabajo deben ser administradas por al menos un cuarto de telecomunicaciones. Para los puntos de consolidación (CP) se instalarán en sitios permanentes del edificio como son paredes, columnas y piso falso; dependiendo de la construcción y estética final para el edificio. Cada uno de los CP deben ser diseñados para servir en una sola área de piso útil, con aproximadamente 34$[m^2]$y 82 $[m^2]$.

Algunas de las recomendaciones para el cuarto de telecomunicaciones son las siguientes:

- El área no será compartida con instalaciones eléctricas ajenas al sistema de telecomunicaciones.
- Ningún equipo o servicio no relacionado será instalado o pasar a través del cuarto de telecomunicaciones.
- Múltiples cuartos en un mismo piso tienen que ser interconectados por medio de un ducto de 3 pulgadas como mínimo o canalización equivalente.
- No deberá tener techo falso.

Algunas consideración para el cuarto de equipos son las siguientes:

- Instalación de equipos UPS[8] hasta máx. 100 [KVA].
- Estar separada de las demás áreas del edificio.
- El tamaño dependerá de los equipos que albergará.

[8]Del inglés Uninterruptible Power Supply, es un dispositivo que proporciona energía durante un tiempo por medio de un sistema de baterias que entran en funcionamiento cuando el suministro eléctrico se corta.

- Estar alejado de cualquier interferencia electromagnética.

Algunas consideraciones para las canalizaciones son:

- No se instalarán en el cubo de los ascensores.
- Las canalizaciones horizontales deben ser instaladas en espacios secos, para proteger los cables de los niveles de humedad inusuales en cable de uso interno.
- Los techos falsos pueden ser utilizados para cableado, o algún otro tipo de dispositivo de conexión. Para esta implementación se debe considerar que el techo falso no esté conformado por panel no-removibles, láminas o yeso. También contar con soportes a el cableado ya que no es permitido el tendido directo sobre los paneles de techo falso.

Canalizaciones medulares Estas canalizaciones intra-edificio consisten en perforaciones entre pisos de un edificio, se instalan de manera recta de manera que los cuartos de telecomunicaciones y de equipos estén colocados uno encima del otro, véase Figura 1.25.

Escalerillas y ductos para cables Estas canalizaciones consisten de estructuras prefabricadas donde se disponen los cables, comúnmente reciben el nombre de canasta o charola.

(iii) ANSI/TIA/EIA 606 Administración para la infraestructura de telecomunicaciones de edificios comerciales.

Este estándar proporciona un esquema para la administración total sobre la infraestructura, sin importar las aplicaciones o servicios que proporcione. El estándar establece cuatro clases de sistemas de administración, según el tamaño y características de la infraestructura de telecomunicaciones:

Clase I: Se conforma de un único cuarto de telecomunicaciones en un edificio.

Clase II: Se conforman de múltiples cuartos de telecomunicaciones en un edificio.

Clase III: Se conforman por múltiples edificios en un campus, con múltiples cuartos de telecomunicaciones.

Clase IV: Se conforma por múltiples campus, con múltiples edificios.

Para esto, se recomienda identificar cada uno de los elementos de la infraestructura de telecomunicaciones, como son, el espacio de telecomunicaciones, enlaces horizontales, cableado medular, barra principal de tierra para telecomunicaciones, cableado medular inter edificio, entre otros. Con la finalidad de proporcionar una guía para la administración de la infraestructura. Todos los datos recabados deberán ser actualizados y la manera de guardarlos dependerá en gran medida de la clase.

(iv) ANSI/TIA/EIA 607 Requerimientos de puesta a tierra y puenteado de telecomunicaciones para edificios comerciales.

Este estándar especifica cómo se deberán proteger los equipos e instalaciones de telecomunicaciones contra descargas eléctricas proponiendo que todos éstos estén aterrizados o conectados a un sistema de tierras físicas y así protegerlos de daños por descargas eléctricas. Para puesta en tierra se necesita de varillas sólidas de cobre aproximadamente de $\frac{1}{4}$ pulgadas de grosor y 4 pulgadas de altura, estas varillas tienen que ser instaladas a una distancia lejana de la entrada del edificio. Todos los cuartos de telecomunicaciones y el cuarto de equipos se conectan a las varillas por un backbone con aislamiento.

Las principales funciones que deben cumplir los sistemas de puesta a tierra son:

- Protección al personal y equipos de descargas eléctricas bajo fallas.
- Proporcionar un circuito de mínima impedancia para la propagación de corrientes de falla.
- Minimizar la inducción de ruido en los equipos de telecomunicaciones.

El estándar recomienda que cada equipo tenga su independiente y propia puesta a tierra, todas las canastillas del cableado vertical y horizontal deberán también estar aterrizados a tierra. Se descarta totalmente una conexión en serie de las puesta a tierra entre equipos y se aconseja una conexión en paralelo. El cuarto de equipos y de telecomunicaciones deberán tener una barra de tierra para telecomunicaciones (TGB). Esta barra es el punto central de conexión para las tierras de todos los equipos ubicados en estos cuartos. La TGB debe ser una barra de cobre, con perforaciones roscadas y ser de 6 [mm] de espesor, 50 [mm] de ancho y un largo adecuado para las perforaciones necesarias (dependerá de cuántos equipos hay en el cuarto de equipos o de telecomunicaciones).

1.6.2. Normalización y Certificación Electrónica (NYCE)

NYCE nace como un Organismo Nacional de Normalización en la industria electrónica, telecomunicaciones y tecnologías de información liderando en la evaluación en materia de las Normas Oficiales Mexicanas y Normas Mexicanas para diversas industrias. La misión principal de NYCE es desarrollar estándares y evaluar la conformidad para que los usuarios tengan confianza en el acceso al mercado.

La NYCE tiene las dos normas orientadas al cableado estructurado y cableado de telecomunicaciones:

- NMX-I-248-NYCE-2008 (Cableado Estructurado genérico, Cableado de telecomunicaciones para edificios comerciales, especificaciones y métodos de prueba). Esta Norma Mexicana especifica un sistema de cableado estructurado genérico para telecomunicaciones en edificios comerciales que puede implementarse con productos de uno o varios fabricantes. Especifica los requisitos de desempeño, distancias, configuraciones y topología del cableado estructurado genérico. Proporciona guías para la instalación, operación y verificación de cableados para tecnologías de la información. Esta norma es equivalente a la Norma Internacional ISO/IEC 11801 "Information technology – Generic cabling for customer premises", second edition (2002-09).

- NMX-I-14763-1-NYCE-2010 (Telecomunicaciones cableado-Cableado Estructurado, implementación y Operación de Cableado en Edificios Comerciales). Esta Norma Mexicana contiene requisitos y recomendaciones para la identificación de elementos de infraestructura de cableado en apoyo a la norma NMX-I-14763-2-2017 y normas equivalentes. Esta Norma Mexicana es aplicable a todos los productos de este tipo que se fabriquen, comercialicen y distribuyan en territorio nacional.Esta norma es idéntica (IDT) con la Norma Internacional ISO/IEC/TR 14763-2-1:2011, Information technology – Implementation and operation of customer premises cabling –Part 2-1: Planning and installation – Identifiers within administration systems.

Capítulo 2 Situación actual de la red en los Laboratorios de Geomática y Especialidades de Civiles

Capítulo 2

Situación *actual* de la red en los Laboratorios de Geomática y Especialidades de Civiles

2.1. Antecedentes de estructura lógica del laboratorio

El Laboratorio de Geomática y Especialidades de Civiles contaba con una red LAN para todo el equipo del site (servidor, switch) y el equipo de cómputo (docente, académico y administrativo), manteniendo una configuración de IP estática. La topología física de red con la que contaba el laboratorio es como se muestra en la siguiente Figura 2.1.

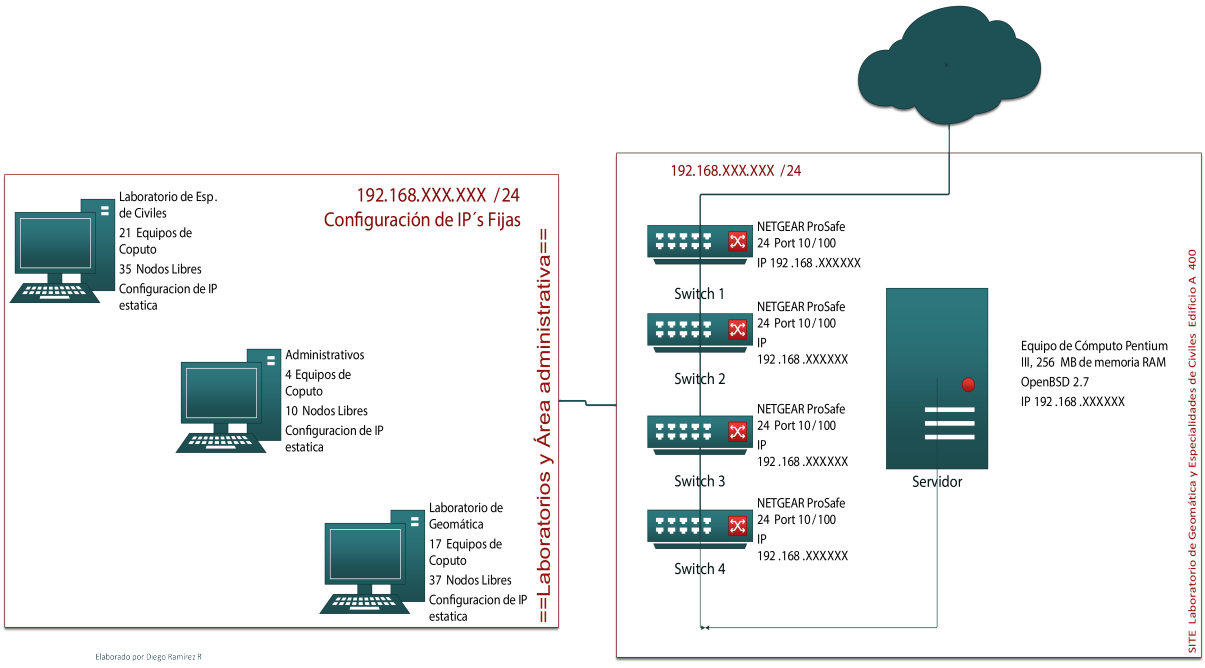

Figura 2.1: Topología inicial de red

Cada equipo conectado en la red del laboratorio se configuraban de manera física ingresando los siguientes datos:

- Direccion IP: 192.168.XXX.XXX
- Máscara de Subred:255.255.XXX.XXX
- Gateway: 192.168.XXX.XXX

- DNS: DNS UNAM

Desde sus inicios el laboratorio cuenta con responsables en el área de ingeniería civil que les ha interesado el área tecnológica y aunque se han realizado diferentes cambios a través del tiempo en el mismo, las estructuras y desarrollo de proyectos no contaba con esa visión que un ingeniero en computación pudiera otorgar.

Las personas que hacen uso del laboratorio tienen diferentes necesidades de software y hardware, y es necesario contar con los dispositivos adecuados y que sean totalmente ad-hoc a las necesidades de estudiantes y profesores.

El laboratorio tiene como prioridad dar un buen servicio a sus estudiantes y profesores que en este caso, podemos tener con un grado académico desde licenciatura hasta doctorado, lo cual enriquece mucho el lado académico del mismo, lo anterior hace relevancia ya que las necesidades propias y requerimietnos específicos de cada uno de los usuario que solicitan el servicio, es variado y a veces puede llegar a contraponerse por las mismas condiciones del software específico que se requiere para la impartición de sus cursos, clases, diplomados, entre otros.

2.2. Equipo con el que se contaba

El Laboratorio de Geomática y Especialidades de Civiles contaba con el siguiente equipo e infraestructura de red:

- Equipo de Cómputo Pentium III, 256 MB de memoria RAM, dos interfaces de red, OpenBSD 2.7 como sistema base(servidor).
- Cuatro switches NETGEAR ProSafe 24 Port 10/100, no administrables.
- Rack de dos postes, 45 unidades.
- Cableado horizontal y patch cord cat 5.
- Cuatro patch panel 24 rj45.

Con el cual ofrecía el servicio de red a los equipos dispuestos en cada una de las áreas de trabajo, véase de la Figura 2.2 a Figura 2.6.

Figura 2.2: Rack con equipo de red

Figura 2.3: Cableado horizontal

Figura 2.4: Detalle de cable UTP

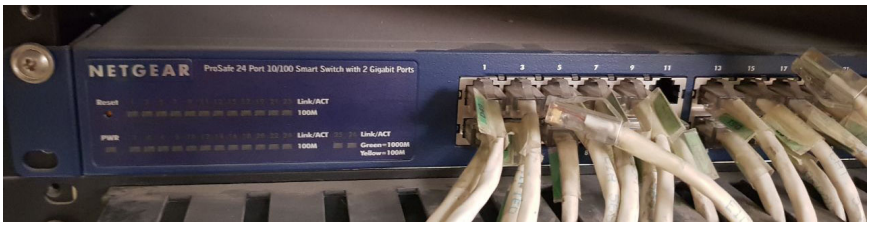

Figura 2.5: *Switch* NETGEAR

Figura 2.6: Equipo de Cómputo

Esta infraestructura no tenía la capacidad de ser escalable para algún proyecto a medio o largo plazo. Como consecuencia del sismo del 19 de septiembre del 2017 el laboratorio presentó daño estructural y también daño en su infraestructura de red, por lo que se aprovechó la oportunidad para mejorar los servicios prestados en el laboratorio, los cuales se describen a continuación.

Servicio que ofrece el laboratorio

El laboratorio solamente ofrece el servicio de internet por el momento, se tienen equipos con software especializado, pero todo se maneja de manera local y no hay un servidor que pueda hacer gestión de ningún tipo.

Aunque se ha pensado poder tener un servicio para alojar la página web del laboratorio, no se cuenta con dicha infraestructura. Además, también tener aplicativos que puedan apoyar y complementar todas las actividades académicas que se realizan en dichos laboratorios.

2.2.1. Sistema de gestión de calidad

Es un sistema de gestión para dirigir y controlar una organización con respecto a la calidad, se deben de cumplir los requisitos de la norma ISO 9001:2018, la cual adopta un enfoque basado en procesos. Con el propósito de "establecer un marco de referencia para asegurar que cada vez que un proceso es desarrollado, la misma información, métodos, herramientas y controles son usados y aplicados de forma consistente"[1].

Actualmente la Facultad de Ingeniería tiene 25 laboratorios certificados y seis de ellos pertenecientes a la División de Ingenierías Civil y Geomática. Estos laboratorios deben cumplir los siguientes objetivos de calidad:

- Asegurar que el equipo, instalaciones y materiales de los laboratorios sean suficientes y se encuentren en buenas condiciones.
- Asegurar que los alumnos reciban el apoyo docente que facilite el desarrollo de las prácticas.
- Contribuir a la formación científica de los futuros ingenieros.
- Asegurar la eficacia y la mejora continua del servicio.

[1]Dale, B., Van der Wiele, T., Van Iwaarden, J. (2007). Managing Quality, 5th Edition, Blackwell Publishing, UK

Se necesitaría un cambio completo de infraestructura para poder pensar en incluir al Laboratorio de Geomática y Especialidades de Civiles en el sistema de gestión de la calidad de la Facultad de Ingeniería.

El servicio que se ofrece en los laboratorios no cumple con los requisitos mínimos para la certificación.

2.2.2. Diagnóstico lógico

La red lógica que se tenía en el laboratorio contaba con un esquema tipo estrella que creció sin ningún tipo de orden. Aunque básicamente todo estaría conectado al bastidor, la red lógica del laboratorio, podría sufrir de fallas que no serían fácilmente detectables. la administración de esta red, no contaba tampoco con subnet o segmentación, todas las computadoras contaban con su propia IP y aunque sí hay una barrera de seguridad, es mínima y enfocada a ataques externos.

Si bien, tampoco se cuenta con equipo necesario para poder hacer una buena administración, los equipos son cuasiautónomos y la conectividad era limitada, la asignación de nuevos equipos se volvía un problema porque no se cuenta con un administrador que tuviera un pleno control de la red.

2.2.3. Seguridad en el laboratorio qué tipo de seguridad ofrece

El servidor alberga el cortafuegos de filtro de paquetes (PF) para su uso. Todos estos programas están incluidos en la instalación base. OpenBSD sigue un vertiginoso ciclo de lanzamientos de seis meses, sin embargo, no se contaba con un plan o programa de acción que se llevará a cabo para mantener los datos a salvo.

Teniendo en cuenta que mantener un OpenBSD actualizado sería uno de los primeros puntos a cubrir, sin embargo, estas actualizaciones podrían tardar incluso años en realizarse.

Otro punto importante es que el acceso al servidor solamente se llevaba a cabo por medio de usuario y contraseña. La idea y recomendación serían las llaves SSH que son un par de llaves criptográficas que pueden ser usadas para autenticarse en un servidor SSH; es un método alternativo al uso de contraseñas. La creación del par compuesto por llave pública y privada es llevada a cabo como un paso anterior a la autenticación. La llave privada la conserva el usuario de manera secreta y segura, mientras que la llave pública puede ser compartida con otros usuarios sin restricción.

2.2.4. Necesidades reales

Como se describió en secciones anteriores, el poder contar con un laboratorio que permanezca a la vanguardia no solo requiere de un compromiso por parte de la parte de alta dirección, sino también con el apoyo presupuestal. En el caso de la Universidad, el poder tener un laboratorio que siempre esté en la punta tecnológica resulta muy caro, tanto en recursos humanos como en materiales, puesto que requiere de creación de plazas y adquisición de equipo.

Para este proyecto, se tuvo la oportunidad de tener la mirada puesta en el laboratorio debido a la gran catástrofe que resultó el sismo 19 de Septiembre del 2017, lo cual, permitió tener un apoyo económico por parte de la alta dirección y con ello lograr proponer un proyecto que pueda satisfacer las necesidades que por más de 15 años no se han atendido.

El laboratorio no solamente apoya con la impartición de clases a nivel licenciatura y posgrado sino también apoya a la realización de proyectos de investigación solicitados por la Facultad de Ingenería, la iniciativa privada y el sector público. Con esta acción se consigue la participación de los alumnos al final de sus estudios, que en algunos casos pueden emplear dichos proyectos como tema de tesis y titularse como Ingenieros Civiles, Geomáticos y actualmente Ambientales.

Esto justificó en su totalidad el proyecto que a continuación se describe, diseñando, desarrollando e implementando nuevas tecnologías y soluciones para poder alcanzar un nuevo nivel tecnológico más avanzado y así, los estudiantes y profesores puedan concentrarse en un objetivo académico claro y no ocuparse solamente de las limitaciones que se tienen en los equipos de cómputo personales.

Capítulo 3 Configuración del Servidor

Capítulo 3

Configuración del Servidor

3.1. Servicios Necesarios

La infraestructura de red cuenta con una renovación en su cableado horizontal (cat 6A) e instalación de piso falso, así como la instalación de canastillas para el tendido de los cables red y electricidad. Se cuenta con un espacio destinado para el cuadra rack de 45 unidades, dos minisplits, un UPS, tres switch HP 5130, seis patch panel 24 rj45 y un servidor DELL PowerEdge R440. Los switches se conectáron en cascada mediante cable UTP cat 6A. El cambio de infraestructura fue necesario, esto se pudo lograr gracias al área de oportunidad que se dio en la Facultad, a continuación se muestran las imágenes que detallan toda la renovación de cableado y equipo que contempla el proyecto justo antes de la instalación y configuración del nuevo servidor véase de la Figura 3.1 a la Figura 3.7. Cabe mencionar que la remodelación estuvo a cargo de un proveedor externo y se siguieron estándares locales e internacionales, los cuales se encuentran descritos en el capítulo 1 sección 1.6.1 y sección 1.6.2.

Figura 3.1: Colocación de piso falso

Figura 3.2: Detalle de cable UTP

Figura 3.3: Tendido de cableado de red y electricidad

Figura 3.4: Cableado horizontal

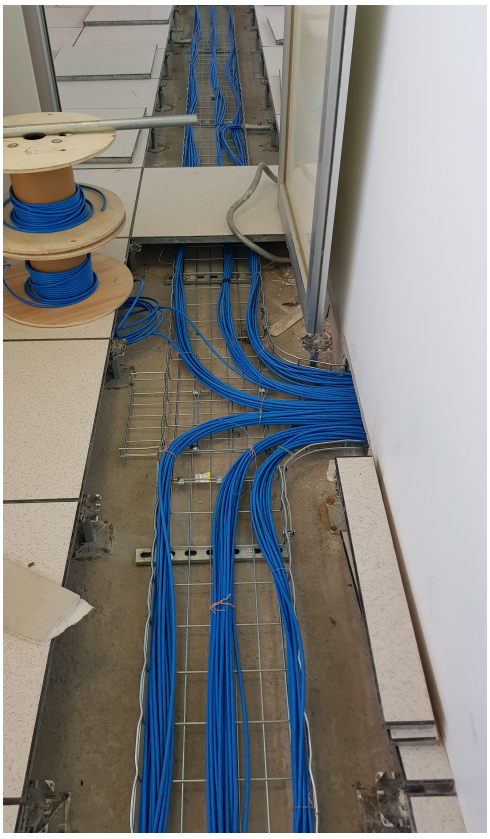

Figura 3.5: Cableado horizontal dirección SITE

Figura 3.6: Aire acondicionado

Figura 3.7: Cuadra rack con todo el equipo de red

Después de un análisis en conjunto de las autoridades de la División y el área de cómputo de la misma, se llegaron a los acuerdos y requerimientos finales que se en listan a continuación.

Servicios que tendrá el site del LGyEC a corto plazo:

- VLAN para cada área de trabajo y el equipo de red.
- DCHP con rangos de 100 IP's en cada VLAN.
- NAT de página WEB. Firewall prohibitivo.
- Servidor pagina WEB LGyEC.
- Monitoreo de red en todas las VLAN.
- Administración remota mediante SSH y VPN.

Servicios que se pretenden tener en el site del LGyEC a largo plazo:

- Puesta en marcha de IDS/IPS.
- Bloqueo de sitios maliciosos, publicidad y amenazas en cada VLAN.
- Filtrado MAC de cada equipo.
- Apilamiento de los switch.

3.2. Instalación del Sistema Operativo

De acuerdo al análisis y alcance de este proyecto, se requiere de un servidor que pueda alojar a varios servidores virtuales, ya que, se necesitan debido a la diversidad de servicios que se estarán ofertando en el Laboratorio de Geomática y Especialidades de Civiles, tanto en corto como en mediano y largo plazo, también se considera la potencia y características de hardware del equipo adquirido. Algunos de los aplicativos que se estuvieron considerando, se llevarán a cabo en proyectos posteriores, sin embargo, por el momento este trabajo se centrará en algunos particulares que se requieren para el servicio inmediato de dichos laboratorios (citados en el apartado 3.1). Se eligió implementar un Hypervisor de tipo Bere Metal por lo que el sistema base del servidor será ESXi 6.7.0.

3.2.1. Instalación del Servidor

En este punto ya se decidió instalar el hypervisor ESXi, gracias a las ventajas que ya se vieron en el capítulo 1. Como primer paso se verificaron los requisitos mínimos de hardware que necesita el servidor.

Los cuales son:

- Servidor compatible.
- Contar con un CPU mínimo de dos núcleos.
- 4 GB de RAM. Recomendable 8 GB para entornos en producción.
- Una o más controladoras Gigabit o Ethernet más rápidas.
- Un disco conectado a través de controladoras SAS compatibles o controladoras SATA integradas compatibles.

Para obtener una copia del hypervisor, se siguieron los siguientes pasos:

- Primero se tuvo que crear una cuenta de My VMware en https://my.vmware.com/web/vmware/.
- Una vez creada la cuenta se descargo el isntalador de ESXi desde https://my.vmware.com/en/web/vmware/evalcenter?p=fre esxi7.
- Se confirma el valor de md5sum del archivo descargado.

Se procedió a instalar ESXi de manera interactiva, la cual se puede efectuar con una unidad flash USB de arranque mediante los pasos siguientes:

- Montar el archivo ISO del instalador en un dispositivo USB.
- Insertar la unidad flash USB y reiniciar el equipo.
- Configurar la prioridad de arranque para el dispositivo USB.
- Aparecerá un recuadro donde se proporciona una liga para visualizar la compatibilidad de ESXi con los sistemas, véase Figura 3.8. Así como los términos de licencia, véase Figura 3.9.

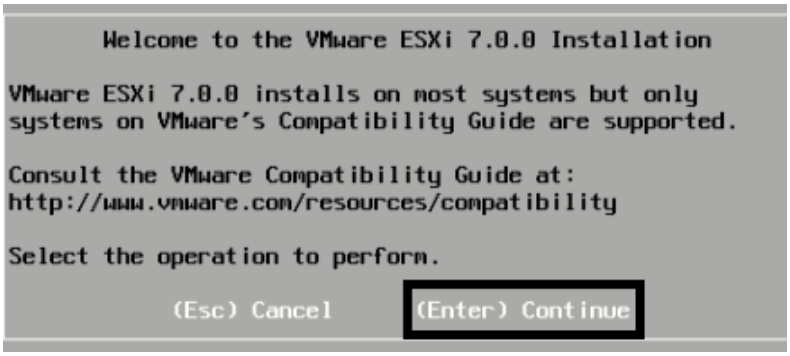

Figura 3.8: Compatibilidad con ESXi

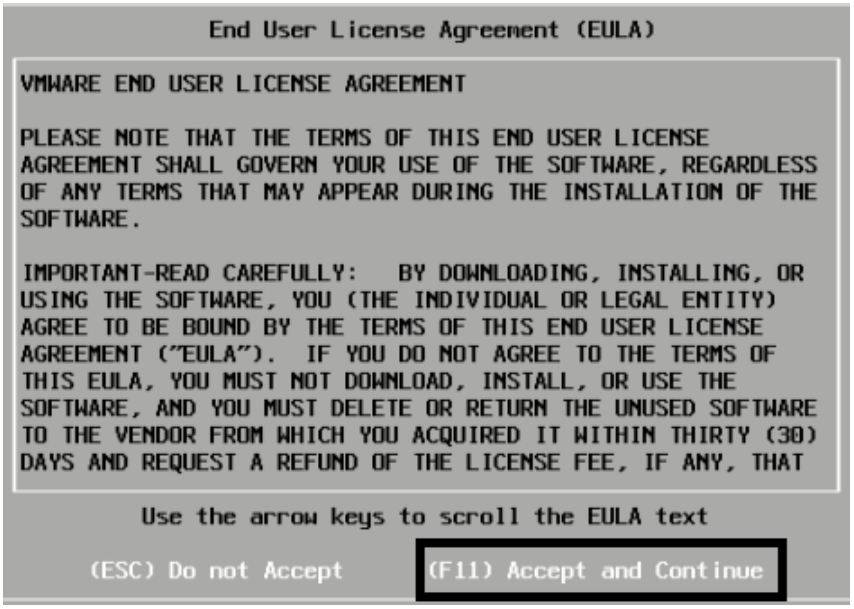

Figura 3.9: Términos de licencia

- Se seleccionó el disco duro donde se instalará el hypervisor, en este caso como es una instalación limpia se elegió todo el disco duro del servidor, véase Figura 3.10.

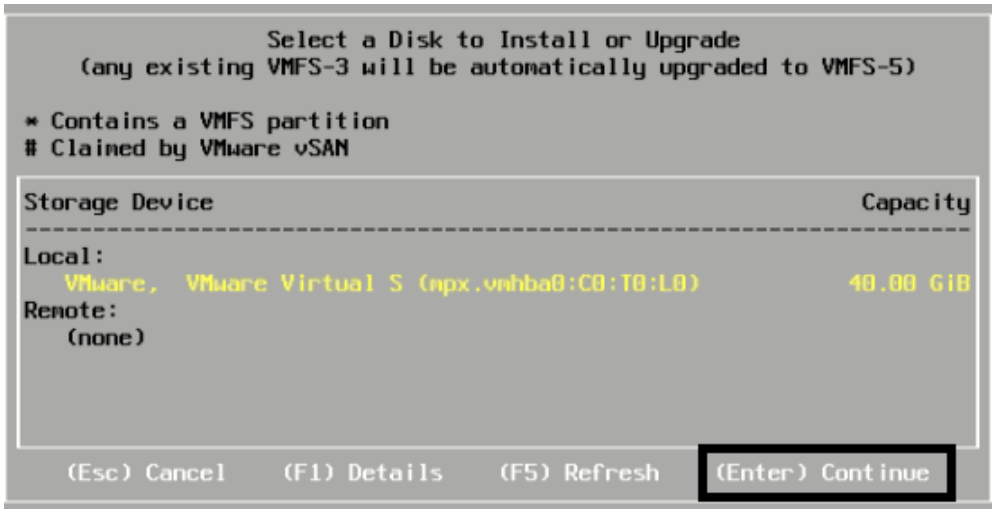

Figura 3.10: Elección de disco duro para la instalacion

- A continuación se seleccionó la distribución del teclado. En este caso se eligió Español, véase Figura 3.11.

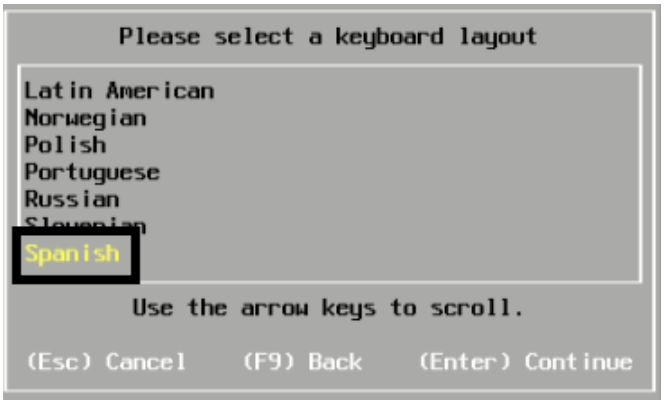

Figura 3.11: Distribución del teclado

- Se introduce una contraseña para el usuario root, la que nos permitirá entrar posteriormente a la interfaz web, véase Figura 3.12.

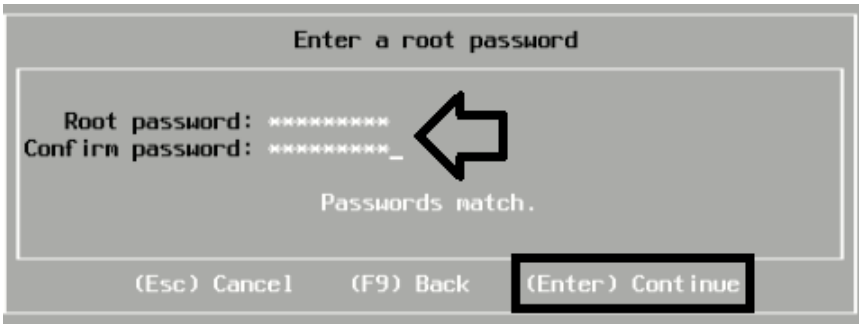

Figura 3.12: Contraseña de *root*

- Se aceptarán las configuraciones de la instalación, y una vez que finalice la instalación aceptaremos el reinicio del servidor, véase Figura 3.13 y Figura 3.14.

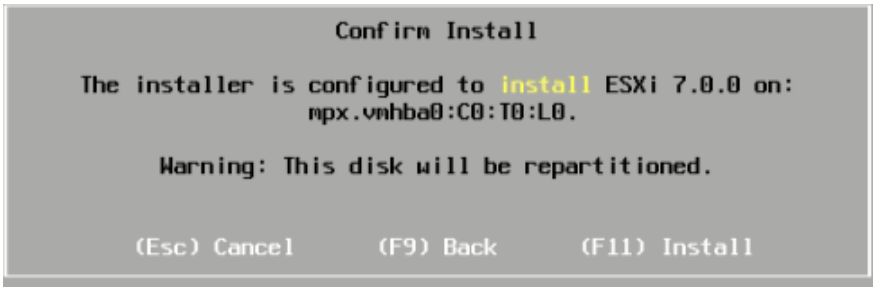

Figura 3.13: Configuración de instalación

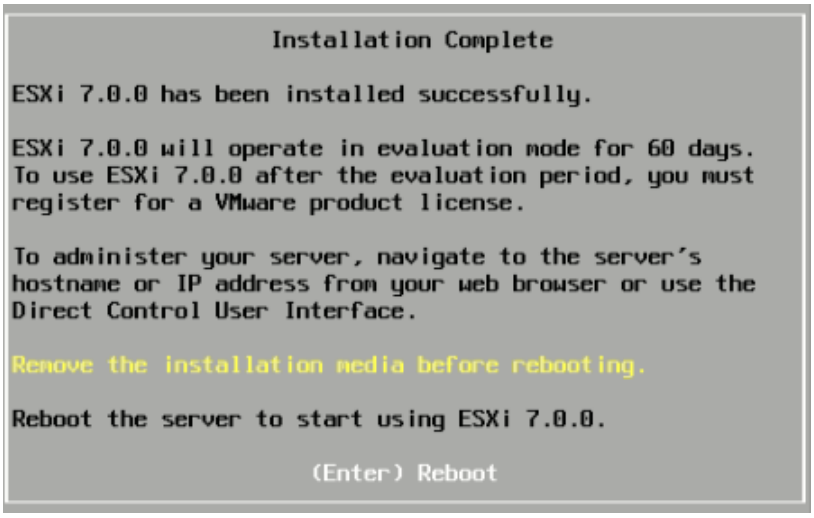

Figura 3.14: Reinicio del servidor

- Configurar la prioridad de arranque para el disco duro, donde se instaló el hypervisor.

Después del reinicio del servidor, se iniciará la fase de autoconfiguración. Donde los dispositivos de red (configuración de IP por DHCP) y de almacenamiento (Dispositivos en blanco se formatean con el sistema de archivos VMFS) se configurarán de manera predeterminada. Se podrá visualizar la versión de ESXi, detalles del procesador, memoria ram y la dirección IP del Servidor. Recordando que se podría visualizar la página de login desde un equipo que se encuentre en el mismo segmento de red, véase Figura 3.15.

Figura 3.15: Detalles del servidor

3.2.2. Configuración del Servidor ESXi

Configuración de IP y adaptador de red de Administración.

Para que el la IP y el adaptador de red se ajusten a las especificaciones de administración, se asignó de manera manual mediante la consola directa, véase Figura 3.17.

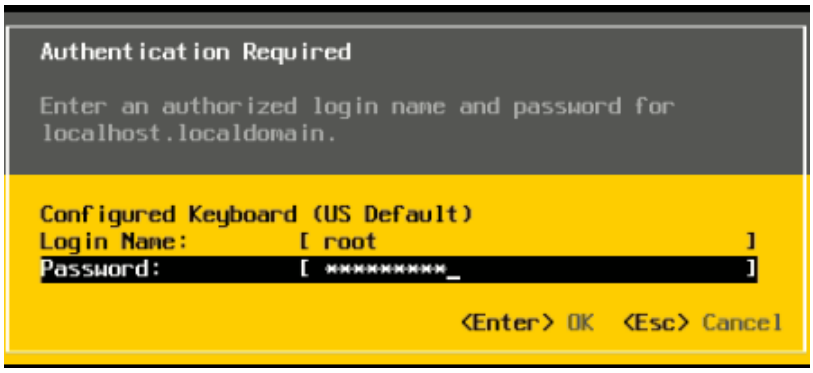

Figura 3.16: Ingreso a personalizacion del sistema

Figura 3.17: Configuración de red

En las configuraciones de red se seleccionó el adaptador de red, de forma automática ESXi nombra a la primera interfaz como wmnic0 y así sucesivamente. Por convención se eligió la primer interfaz Ethernet para la LAN. Véase Figura 3.18.

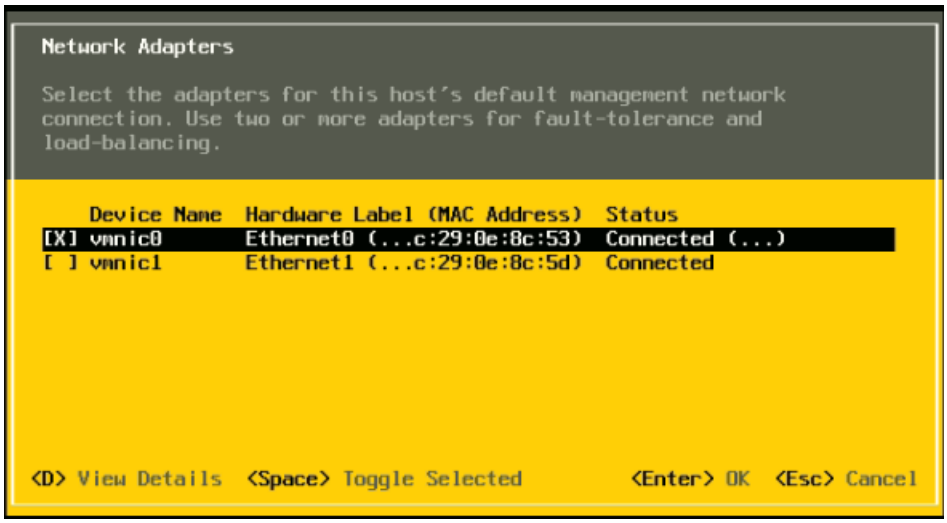

Figura 3.18: Selección de interfaz de red para LAN

Ya seleccionada la interfaz de red, se configuró la dirección IP en el apartado IPv4 de manera estática con los datos de; IP, máscara de subred y puerta de enlace correspondientes a la red LAN, véase Figura 3.19.

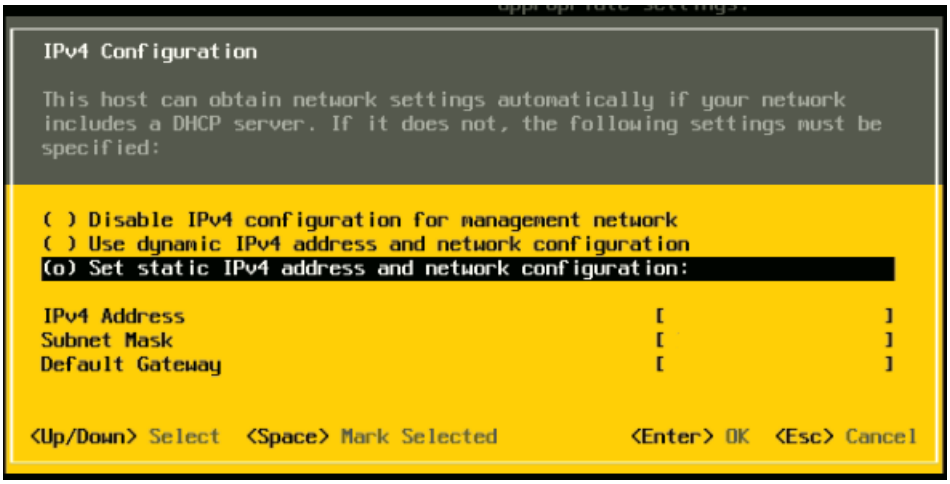

Figura 3.19: Datos de red

En el apartado configuración de DNS se ingresaron los dos DNS de la UNAM y se dejó el nombre de host automático (*localhost*), véase Figura 3.20.

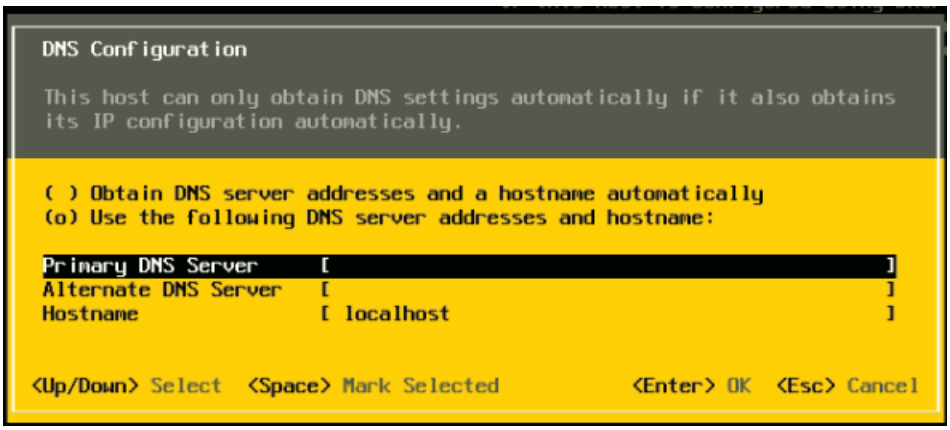

Figura 3.20: Dirección de los DNS

Configuración de Almacenamiento.

Para contener las máquinas virtuales y los archivos necesarios para su configuración, se creó un almacenamiento de 1,81 TB. Con la ayuda de vShere Web Client se realizaron los siguientes pasos.

Se seleccionó **crear nuevo almacén de datos de VMFS**, véase Figura 3.21 y Figura 3.22.

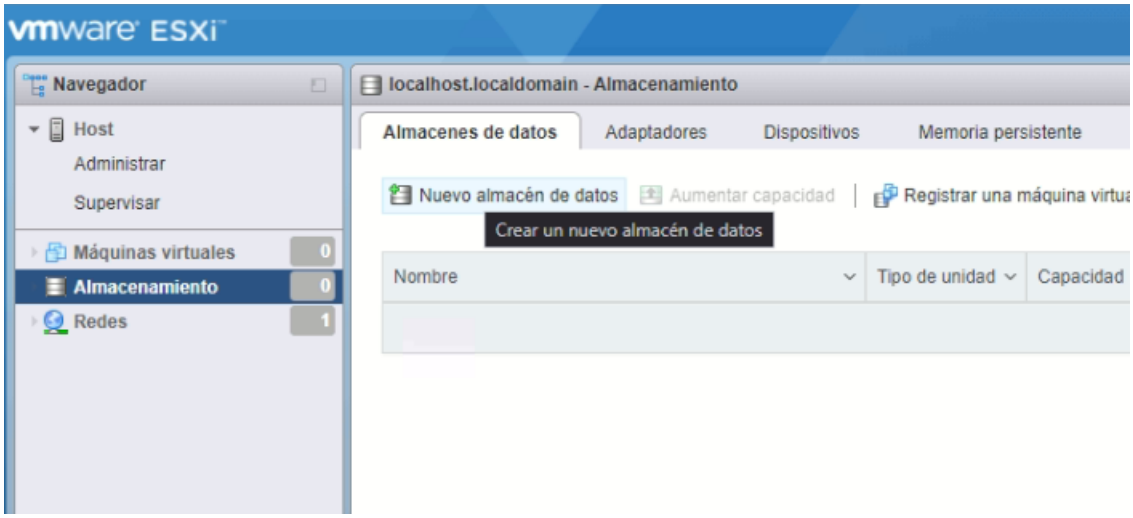

Figura 3.21: Creación de almacenamiento

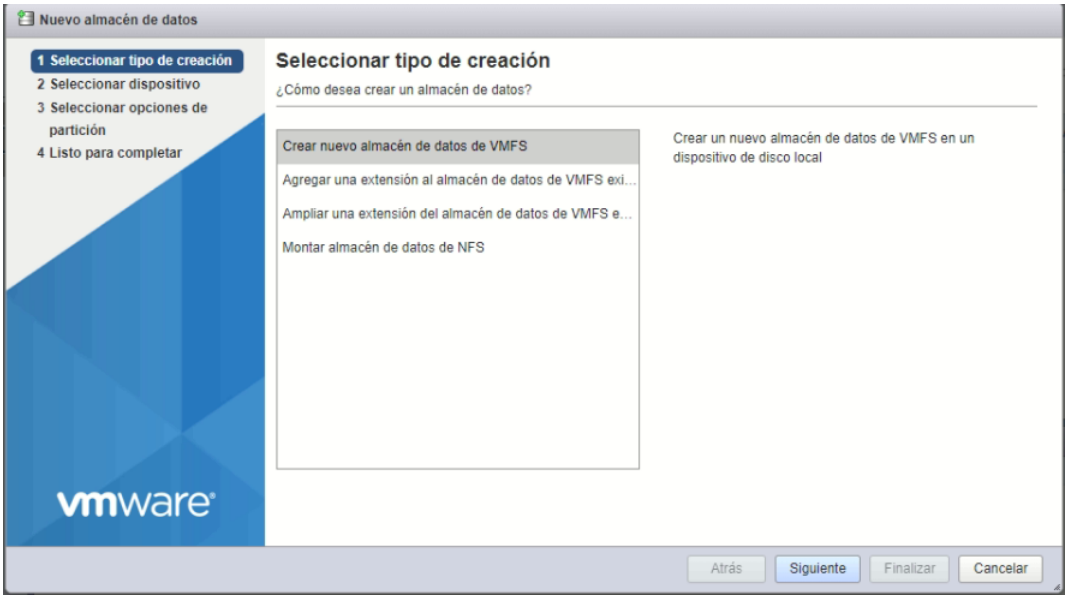

Figura 3.22: Tipo de creación

Se le dio el nombre de **datastore1** y se le asignó el espacio antes mencionado. Al finalizar la creación se confirmó la configuración especificada, véase de la Figura 3.23 a la Figura 3.27.

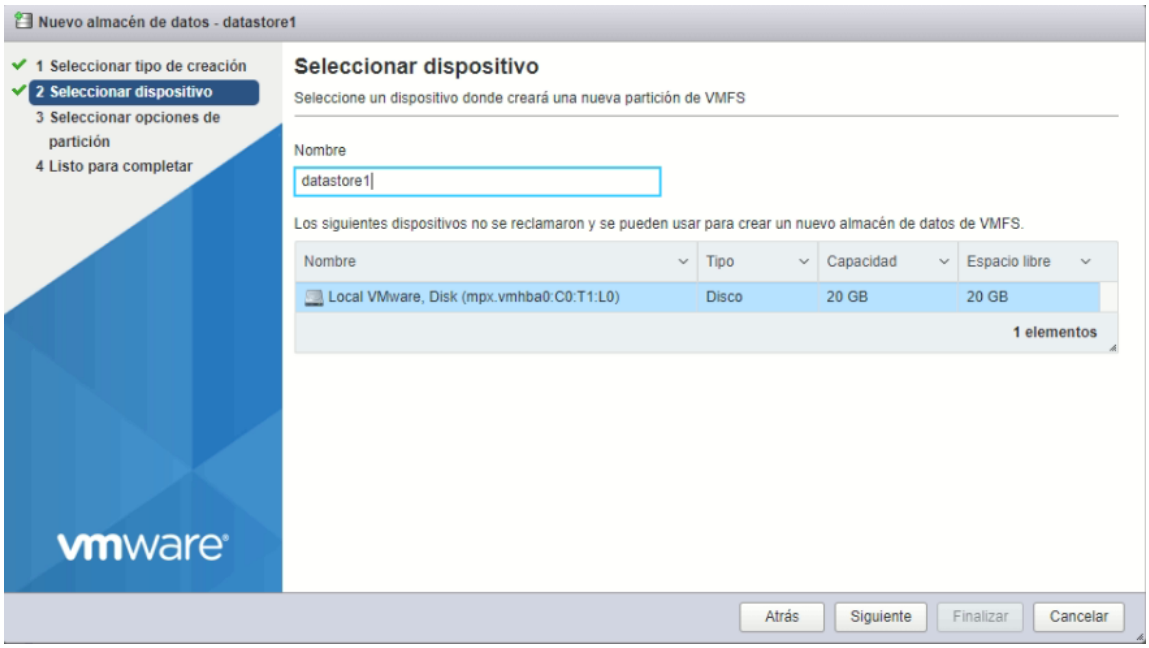

Figura 3.23: Selección de dispositivo y asignación de nombre

Figura 3.24: Espacio a utilizar y tipo de partición

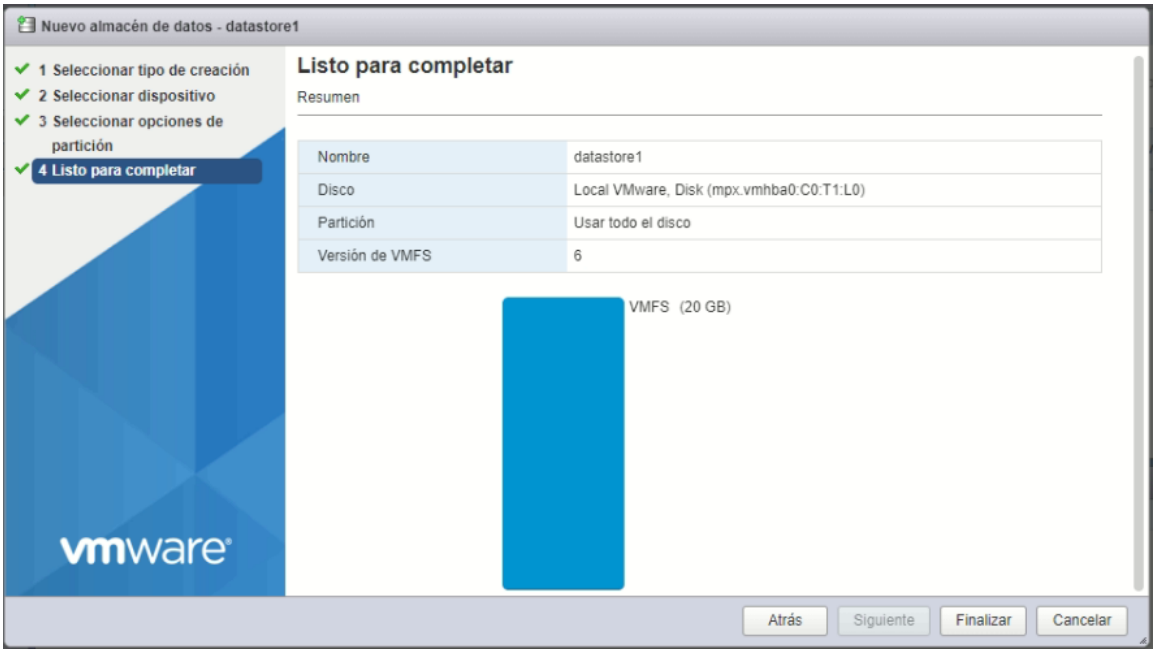

Figura 3.25: Información de la partición

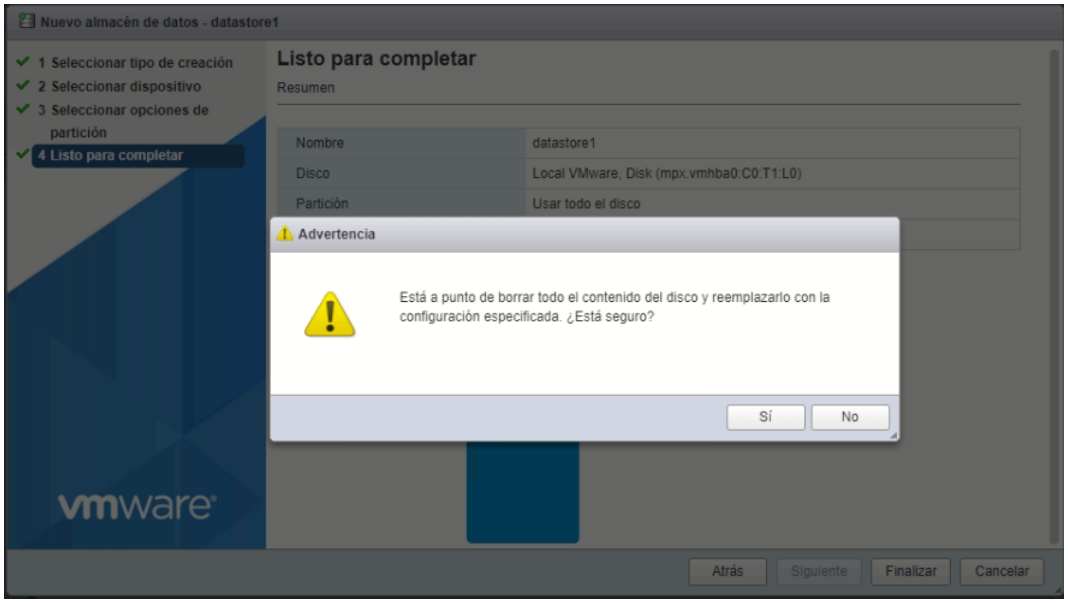

Figura 3.26: Confirmacion en la creación de la partición

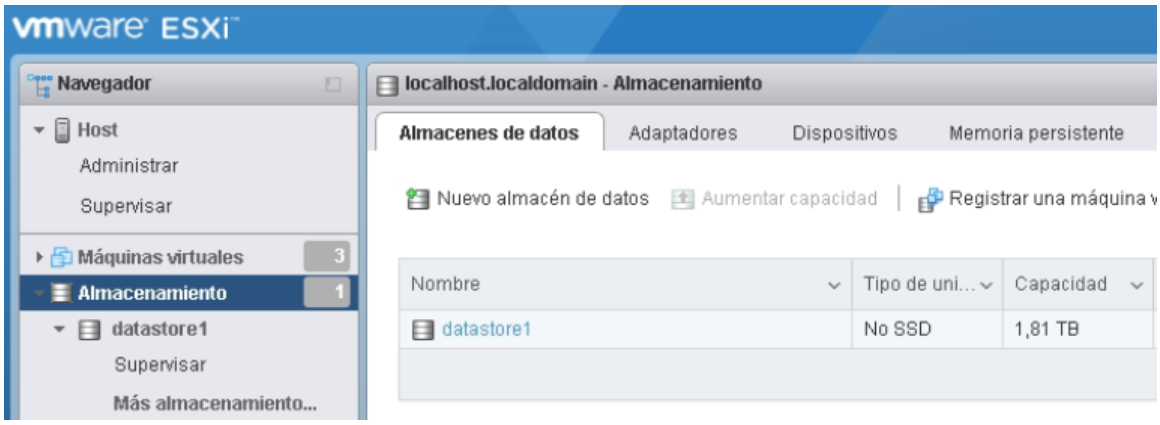

Figura 3.27: Almacenamiento creado

Una vez realizadas las configuraciones del servidor ESXi, se planificó la creación de los servidores virtuales.

3.2.3. Creación de Servidores Virtuales

pfSense(*Firewall*)

Para la instalación de pfSense se descargó la imagen ISO de la página https://www.pfsense.org/download/ y se seleccionaron las opciones. Por seguridad se efectuó la comprobación SHA256 del archivo descargado. Véase Figura 3.28.

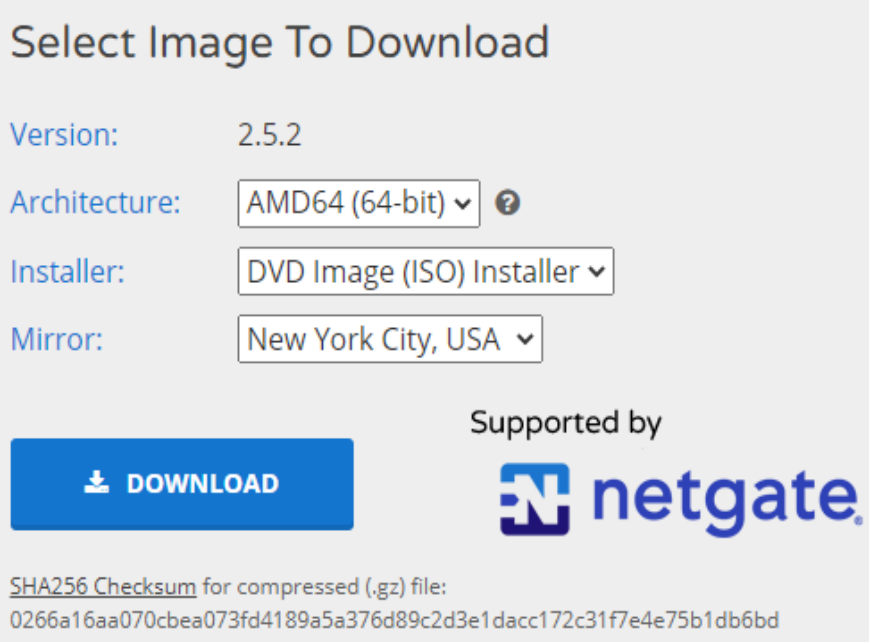

Figura 3.28: Especificaciones de imagen ISO de pfSense

Se cargó la imagen ISO de pfSense mediante el vShere Web Client esto en la sección de Almacenamiento y en la partición de **datastore1**. Véase Figura 3.2.3 y Figura 3.30.

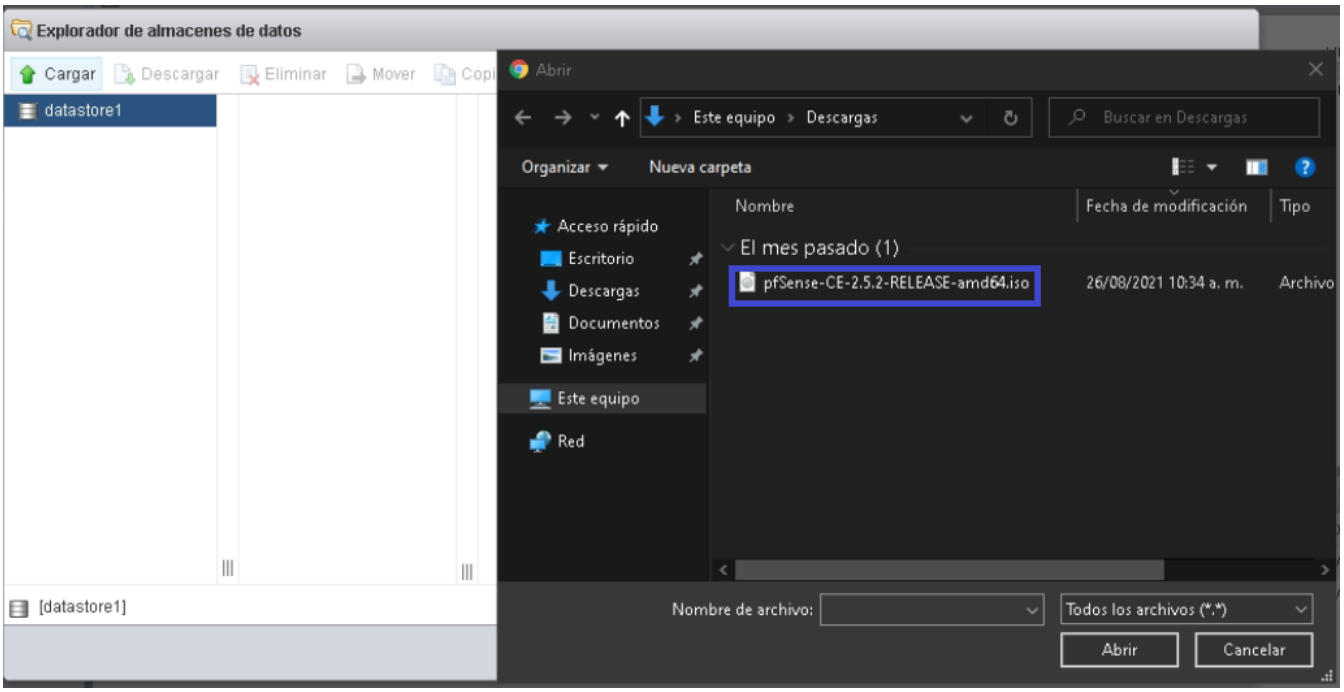

Figura 3.29: Carga de imagen ISO en datastore1

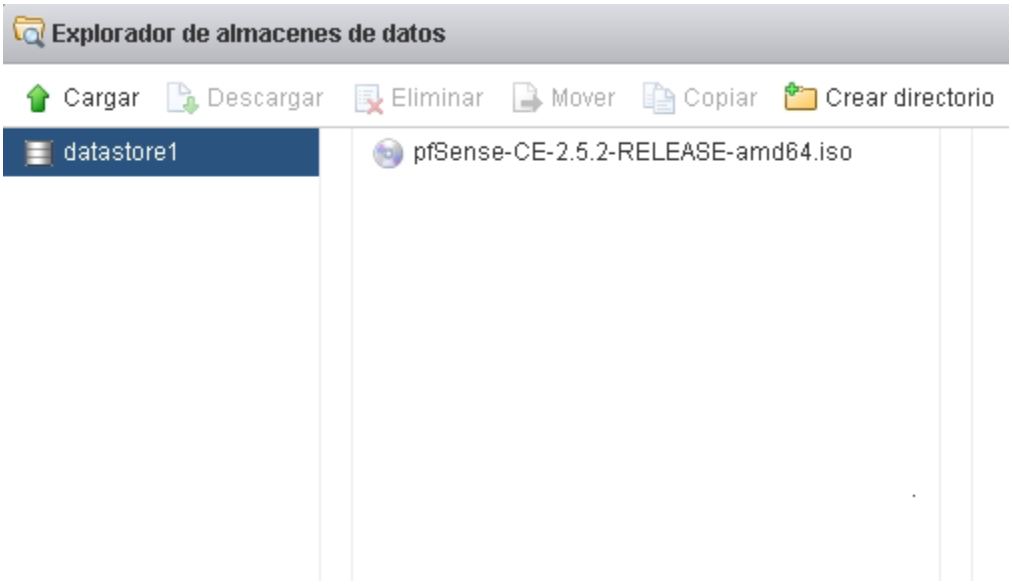

Figura 3.30: ISO en datastore1

La máquina virtual de pfSense contará con las siguientes características:

- Nombre: Firewall
- CPU: 4 vCPU.
- RAM: 4 GB.
- Hard Disk: 100 GB.
- Network adapter: dos interfaces (WAN y LAN).

Cómo se necesitaron dos adaptadores de red se crearon dos switches virtuales y dos grupos de puertos para la WAN y LAN. Al crear los switches se nombraron según la red a utilizar y cómo vinculo superior se seleccionó la interfaz de red física específica para cada una, véase Figura 3.31 y Figura 3.32.

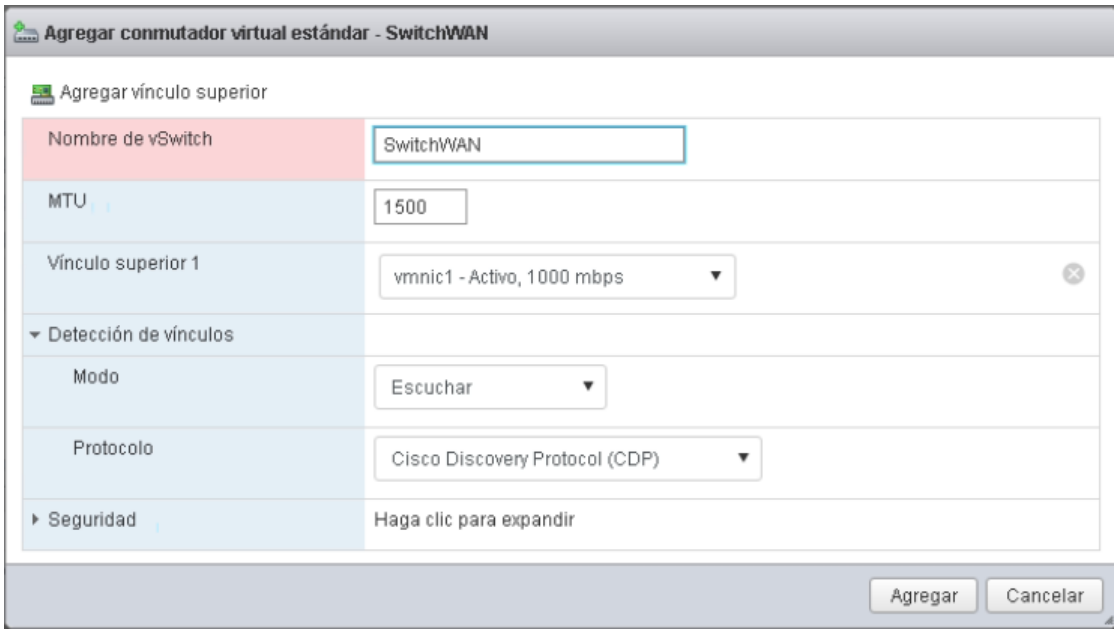

Figura 3.31: Configuración de *switch* para la WAN

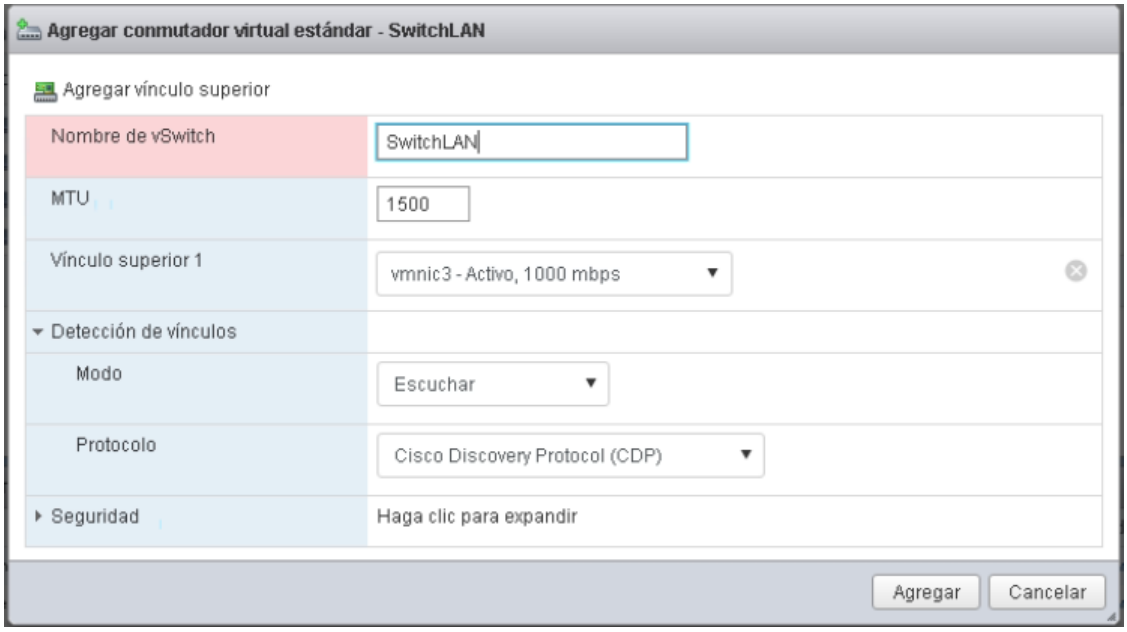

Figura 3.32: Configuración de *switch* para la LAN

Al configurar cada uno de los grupos de puertos se asoció el *switch* virtual que le corresponde a cada red y se hereda la configuración de seguridad del mismo, , véase Figura 3.33 y Figura 3.34.

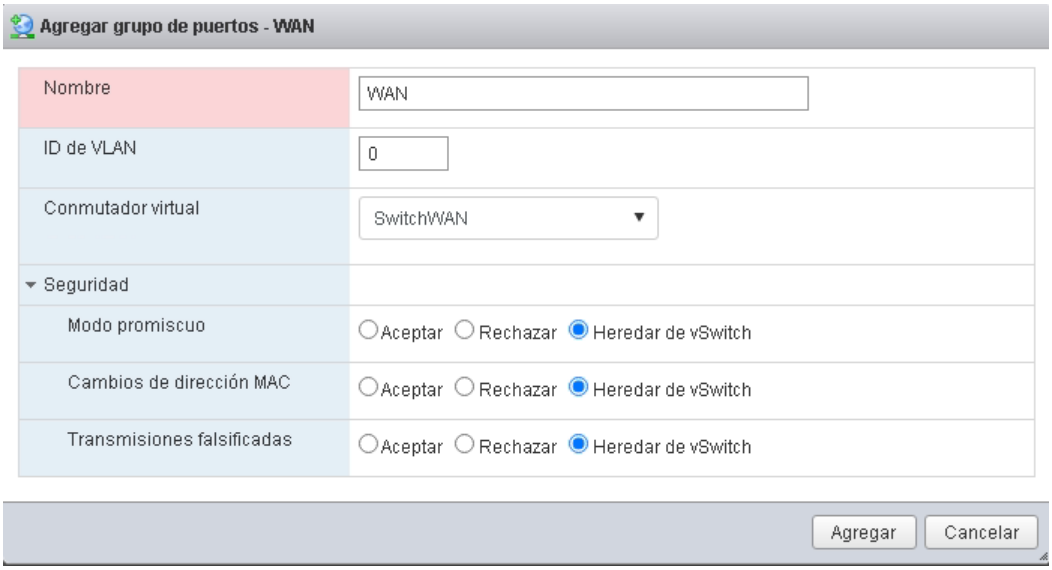

Figura 3.33: Configuración de grupo de puertos para la WAN

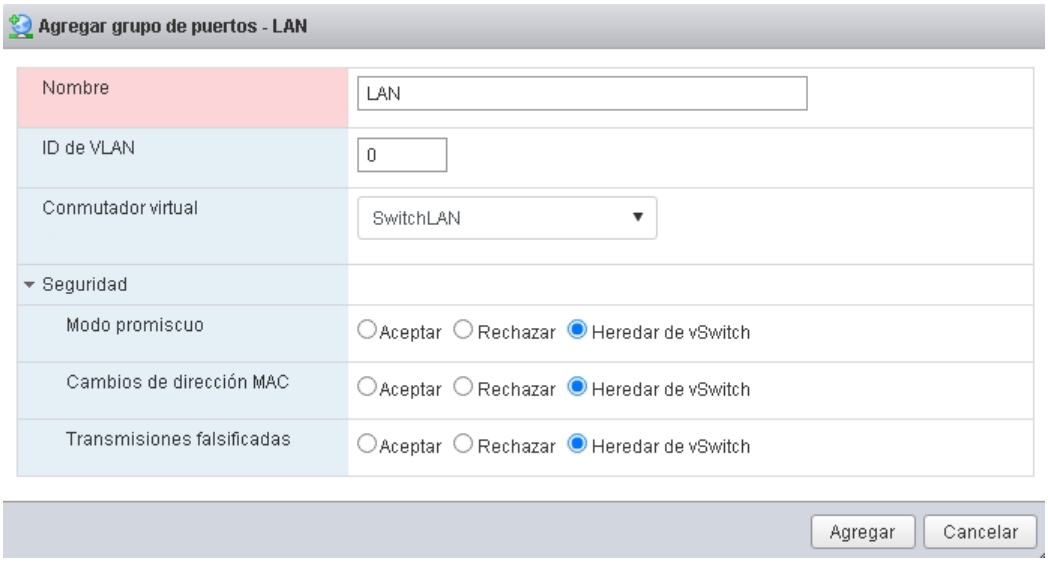

Figura 3.34: Configuración de grupo de puertos para la LAN

Para crear la máquina virtual en ESXi, se seleccionó **Crear / Registrar máquinas virtuales** en el apartado **Máquinas virtuales**, véase Figura 3.35.

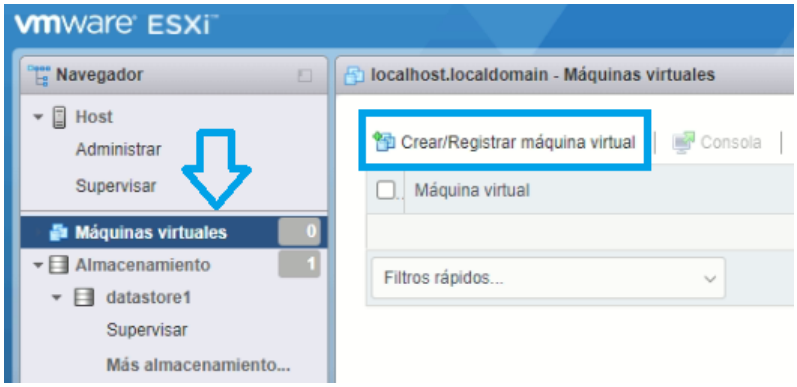

Figura 3.35: Sección Máquinas virtuales

Se eligió como **Otro** a la Familia del sistema operativo invitado y FreeBSD 12 o superior como la versión, se eligió **datastore1** para contener los archivos de configuración de la máquina, véase Figura 3.36 y Figura 3.37.

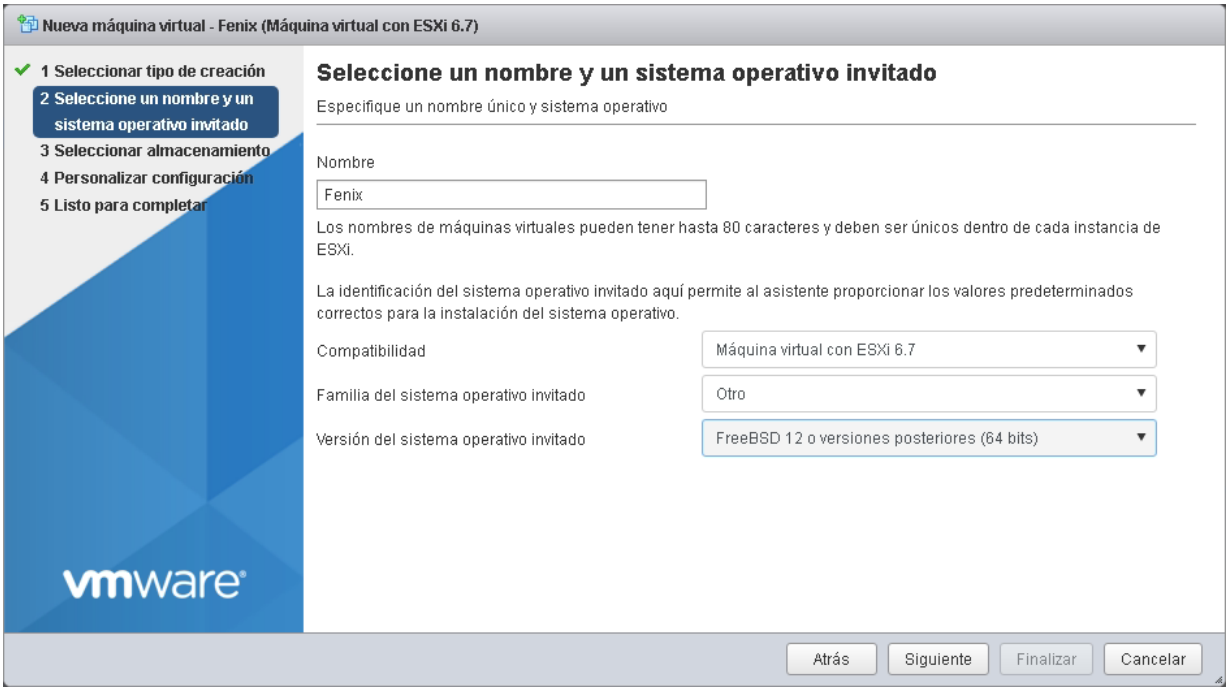

Figura 3.36: Especificaciones para la máquina virtual

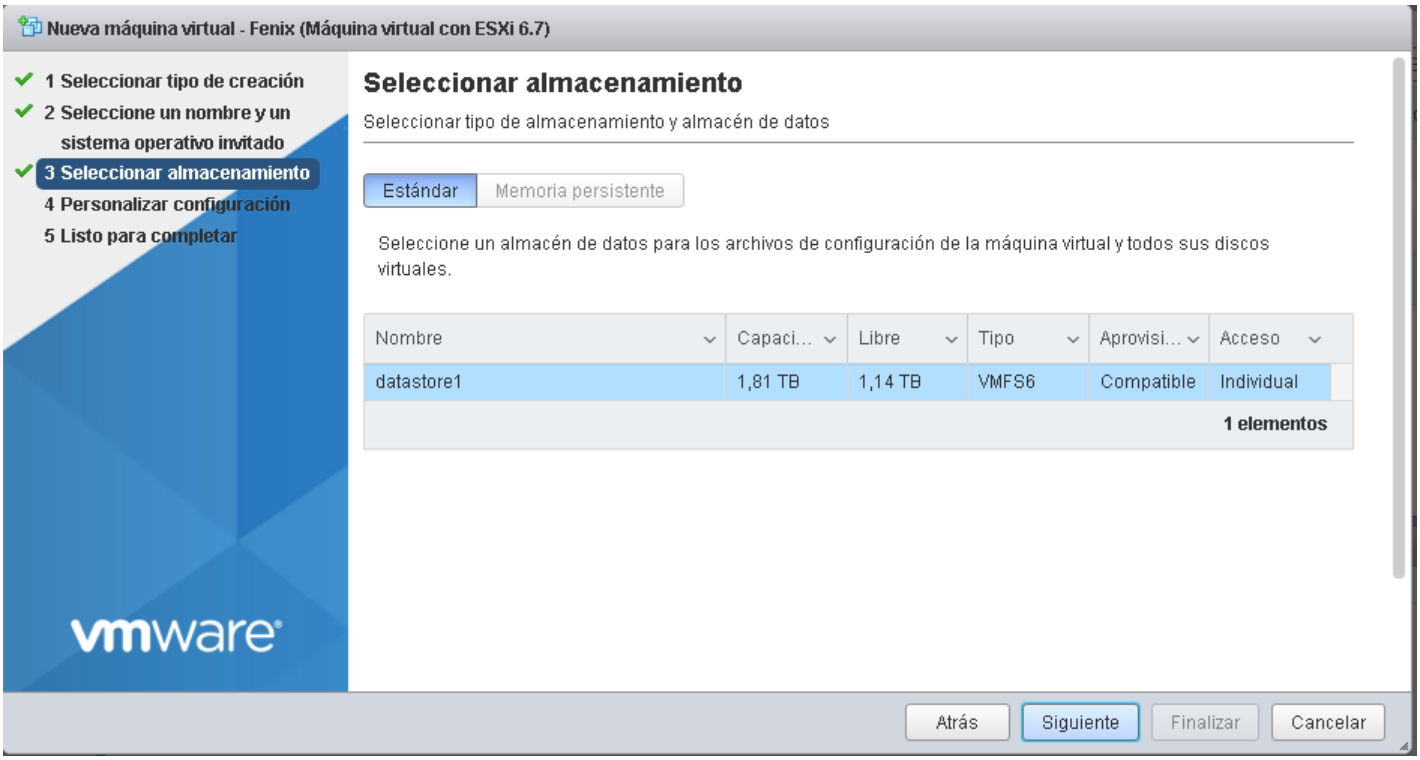

Figura 3.37: Almacenamiento para la máquina virtual

Al agregar los adaptadores de red extra también se agregó el archivo ISO desde el almacenamiento. De igual manera se asignaron los grupos de puertos a cada una de las interfaces de red, se asignaron conforme a la Figura 3.38.

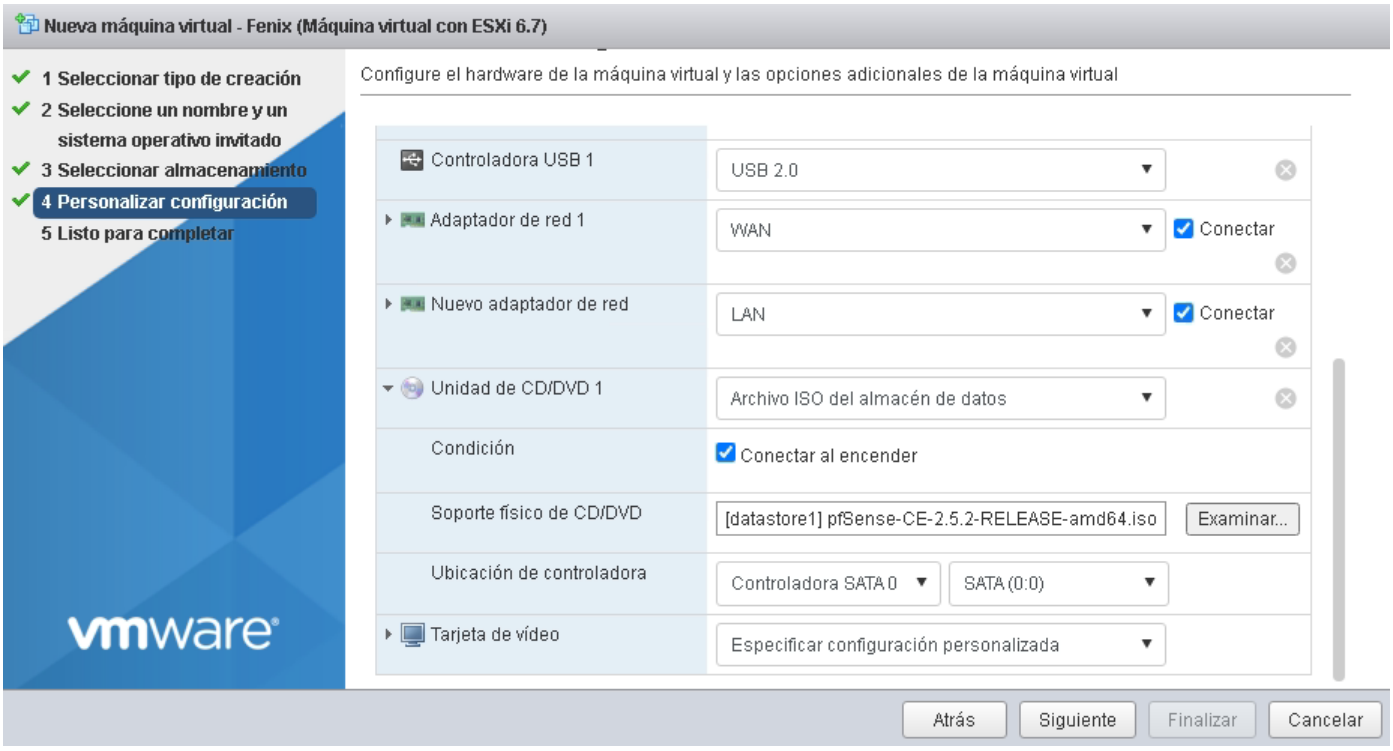

Figura 3.38: Configuración de interfaces de red e imágen ISO de pfSense

Al finalizar la configuración de la máquina virtual se encendió para continuar con la instalación de pfSense. Al cargar la imagen ISO se comenzó la instalación y se seleccionó la partición guiada, véase Figura 3.39 y Figura 3.40. Al reiniciar la máquina virtual se descartó la configuración de VLANs, véase Figura 3.41, pero se asignaron las configuraciones (véase Figura 3.42y Figura 3.43) para la WAN y LAN acorde a la Tabla 3.1.

Tabla 3.1: Configuración de pfSense para las interfaces de red.

Interfaces	Interfaz Fisica	Puerto Servidor	Etiqueta pfSense	Asignación IPv4	Address	Subnet Mask
WAN	vmnic1	GB1	vmx0	Static	xxx.xxx.xxx.xxx	255.xxx.xxx.xxx
LAN	vmnic3	GB3	vmx01	Static	192.168.xxx.xxx	255.xxx.xxx.xxx

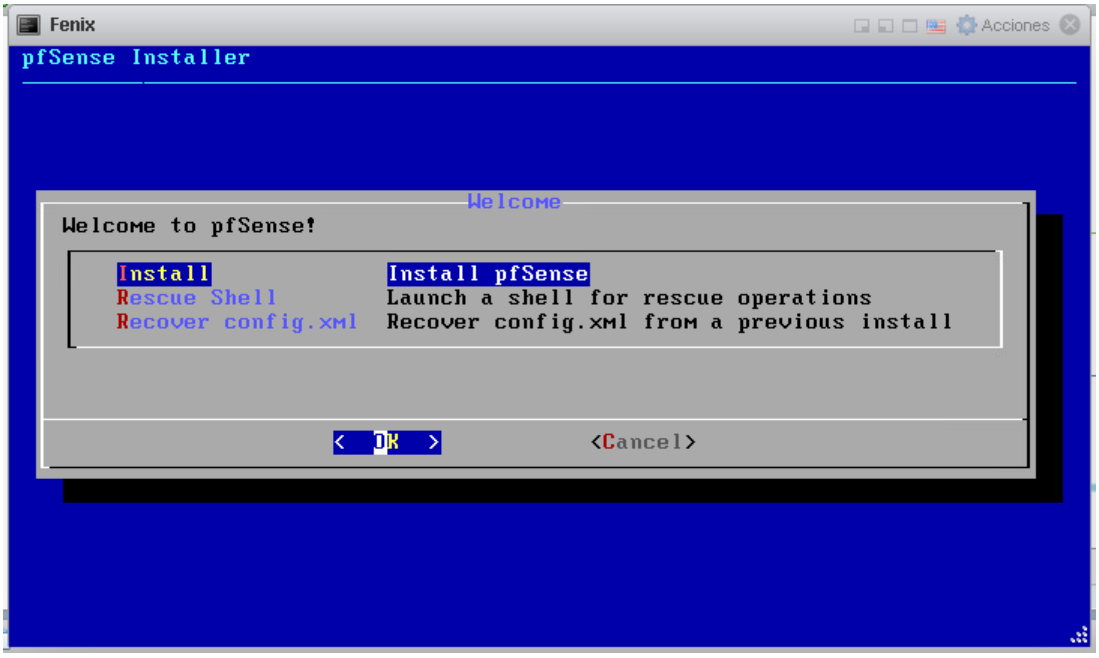

Figura 3.39: Instalación de pfSense

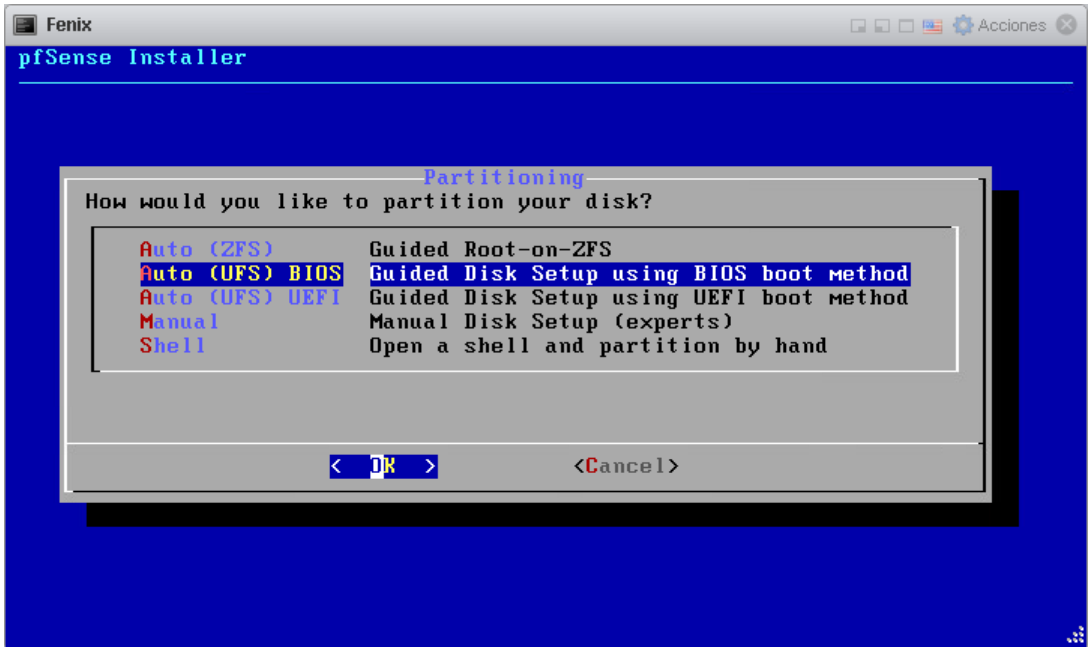

Figura 3.40: Partición guiada de pfSense

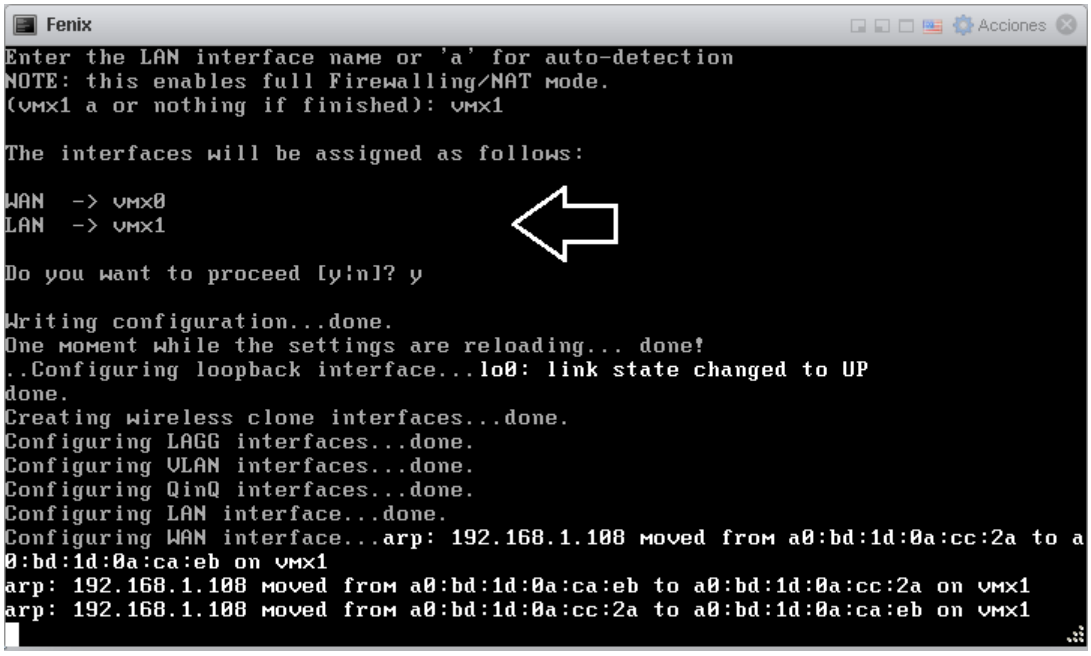

Figura 3.42: Interfaces de red configuradas

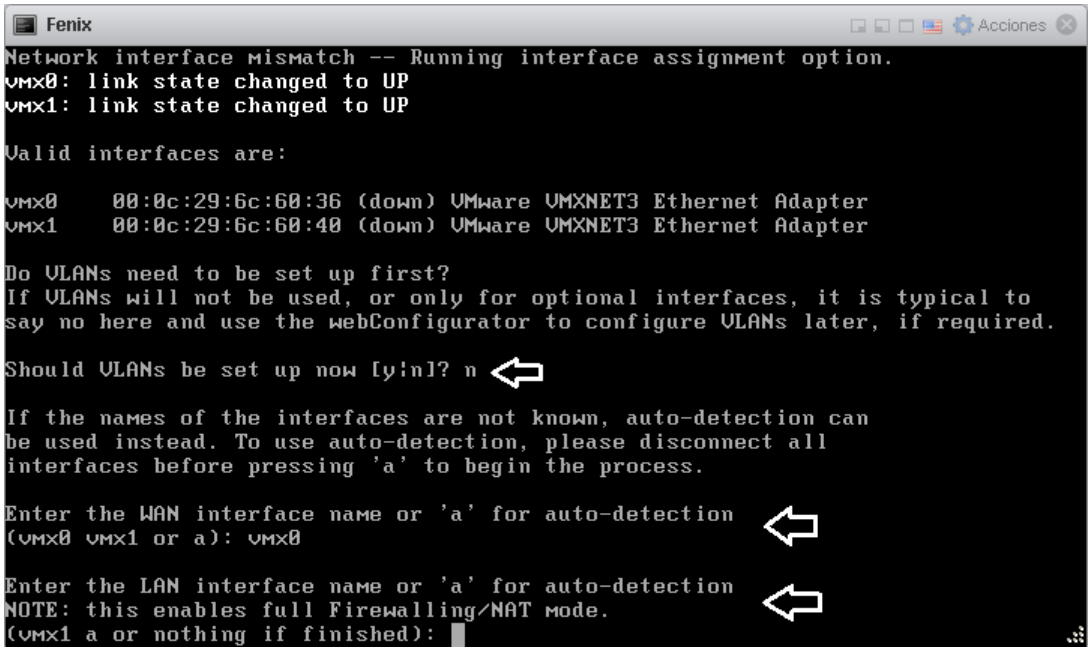

Figura 3.41: Configuraciones de interfaz de red para WAN y LAN

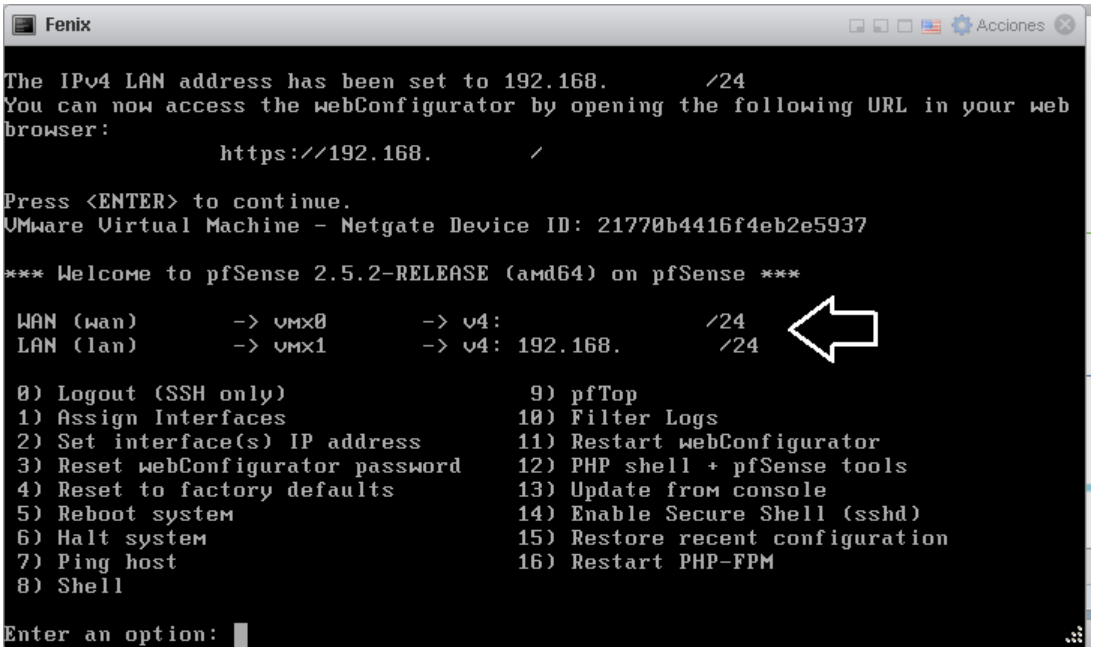

Figura 3.43: Consola pfSense

Como último paso se comprobó el acceso a la interfaz web de pfSense conectándonos desde algún equipo ya en esa LAN, véase Figura 3.44.

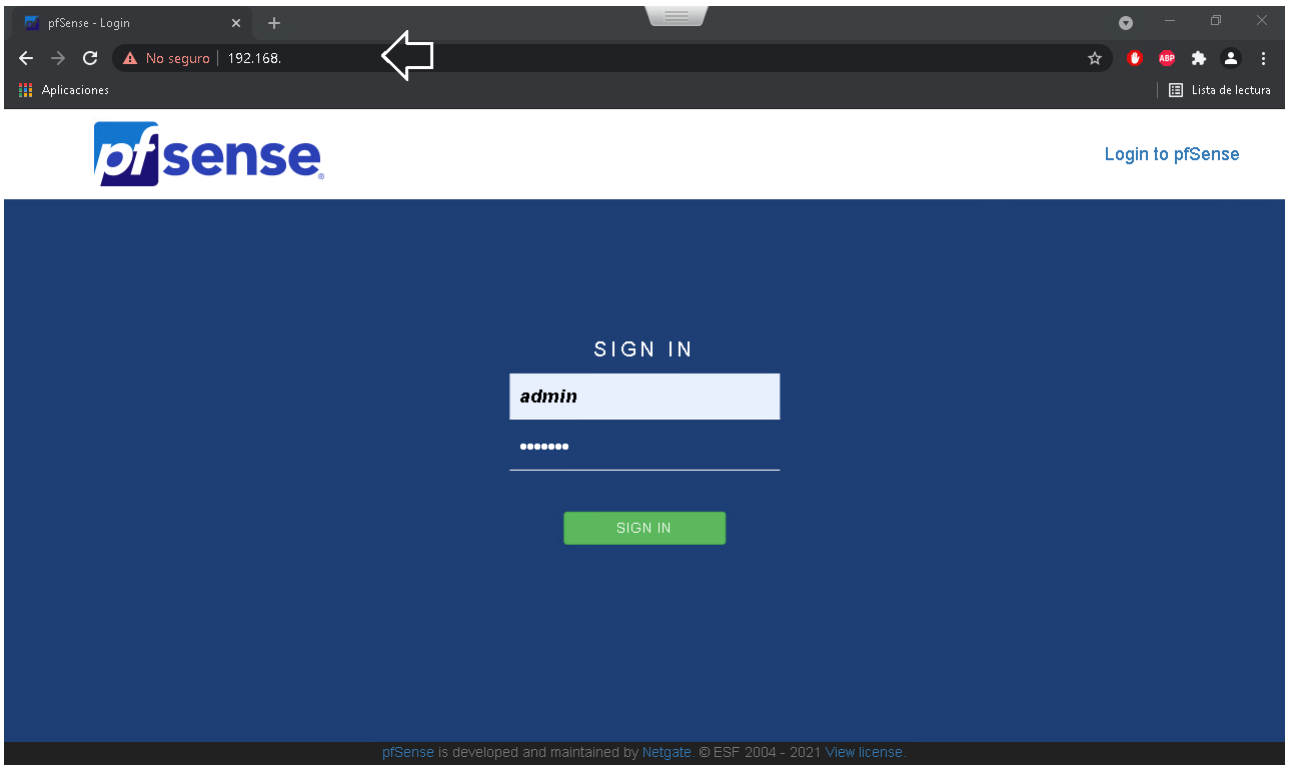

Figura 3.44: Página de login de pfSense

Configuración básica del Firewall, NAT y DHCP

Para el ingreso por primera vez se utilizaron las credenciales default y posteriormente se cambiaron a petición del administrador de la red. La interfaz web despliega automáticamente la configuración guiada y el aviso de cambio

de contraseña para el administrador, véase Figura 3.45.

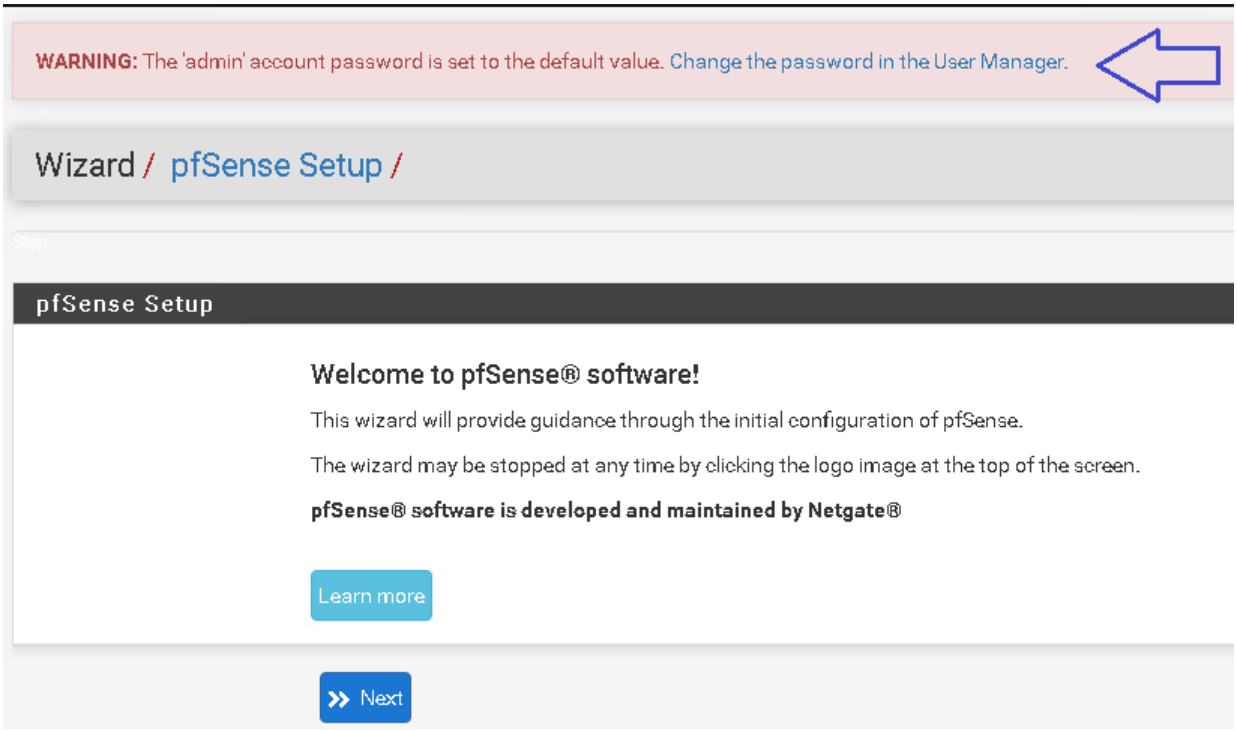

Figura 3.45: Vista de primer inicio de pfSense

Se ingresan los DNS de la UNAM, así como el servidor de la zona horaria, véase Figura 3.46 y Figura 3.47.

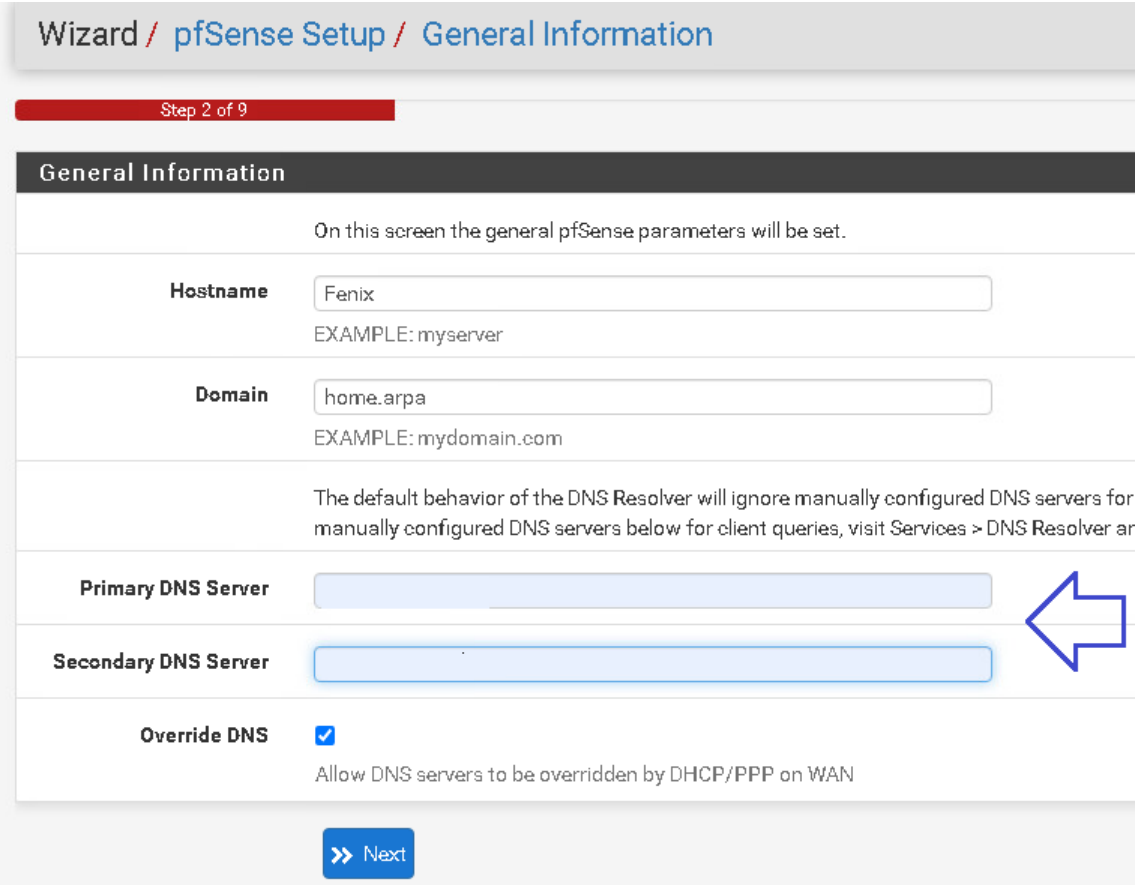

Figura 3.46: Información general de pfSense

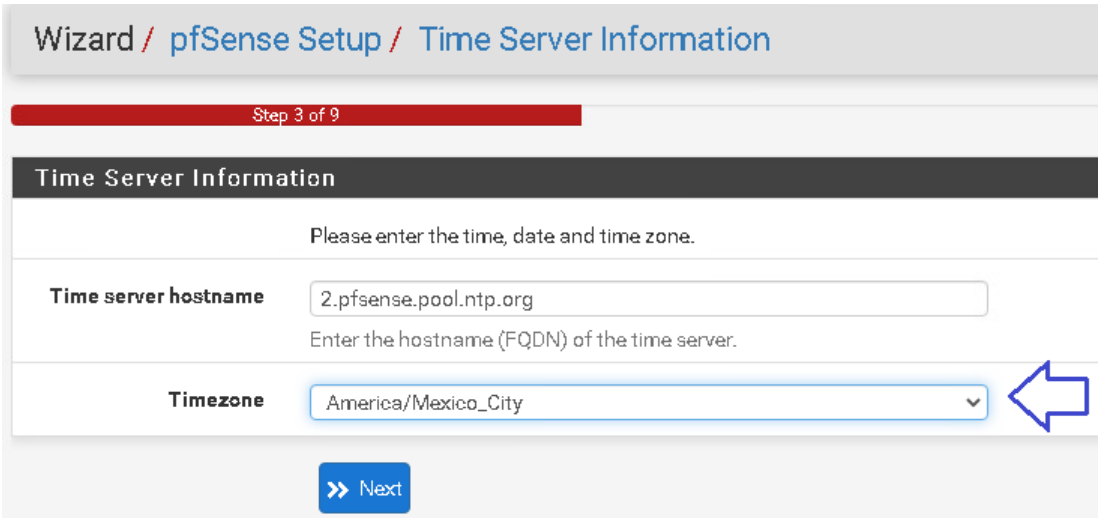

Figura 3.47: Zona horaria pfSense

Para la configuración de la interfaz WAN, se corroboró la IP estática proporcionada así como su *gateway*, véase Figura 3.48. También se habilitaron los bloqueos a las redes privadas[1] y redes bogon[2], véase Figura 3.49.

[1]Son bloques de direcciones IP que han sido reservados por la IANA para identificar redes privadas:10.0.0.0 – 10.255.255.255 , 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255.

[2]Las direcciones IP de Bogon son el conjunto de direcciones IP no asignadas a ninguna entidad por la Autoridad de Números Asignados de Internet (IANA) y RIR (Registro Regional de Internet).

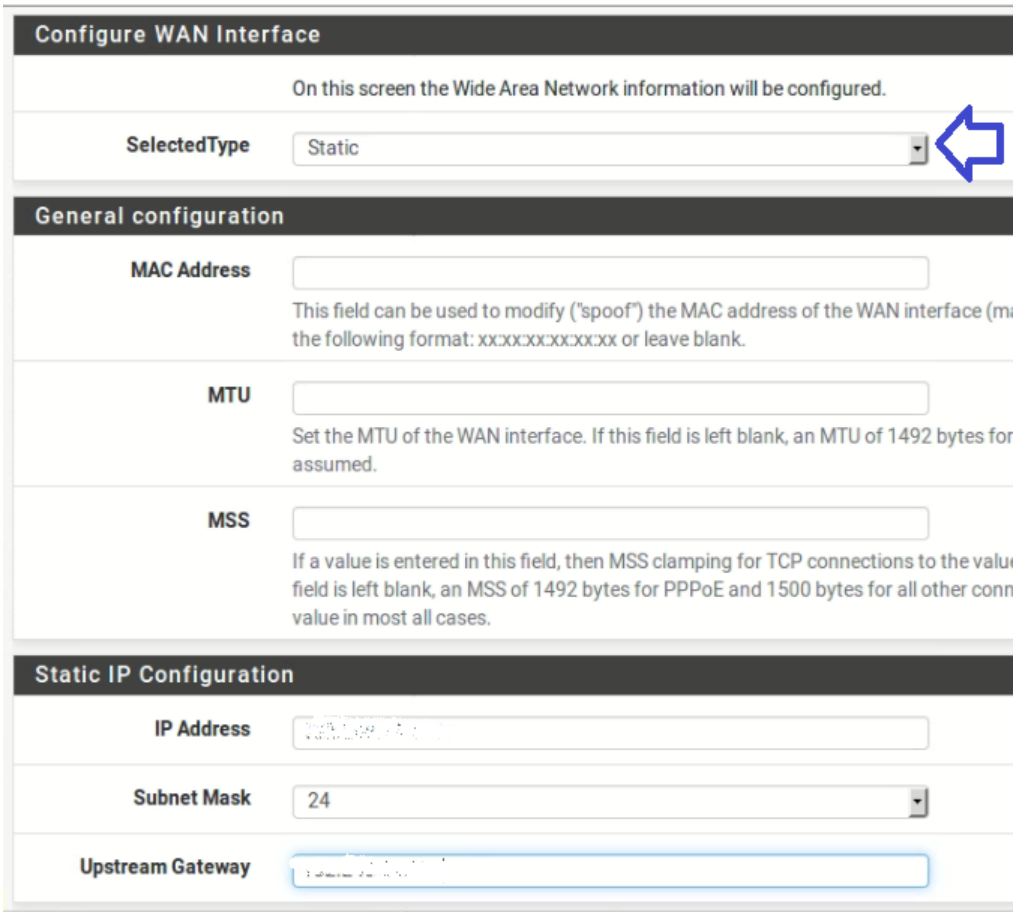

Figura 3.48: Configuración de interfaz WAN

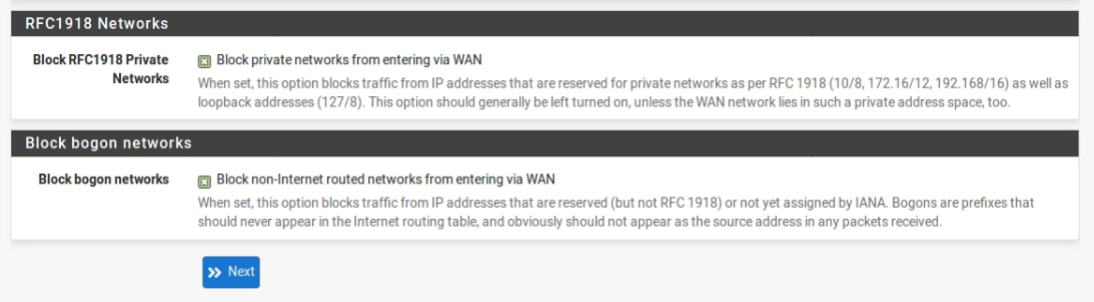

Figura 3.49: Bloqueo de redes privadas y bogon

Para la configuración de la interfaz LAN se asignó la dirección 192.168.xxx.xxx y su máscara de subred, véase Figura 3.50. Hay que recordar que esta dirección es la dirección del *Firewall*.

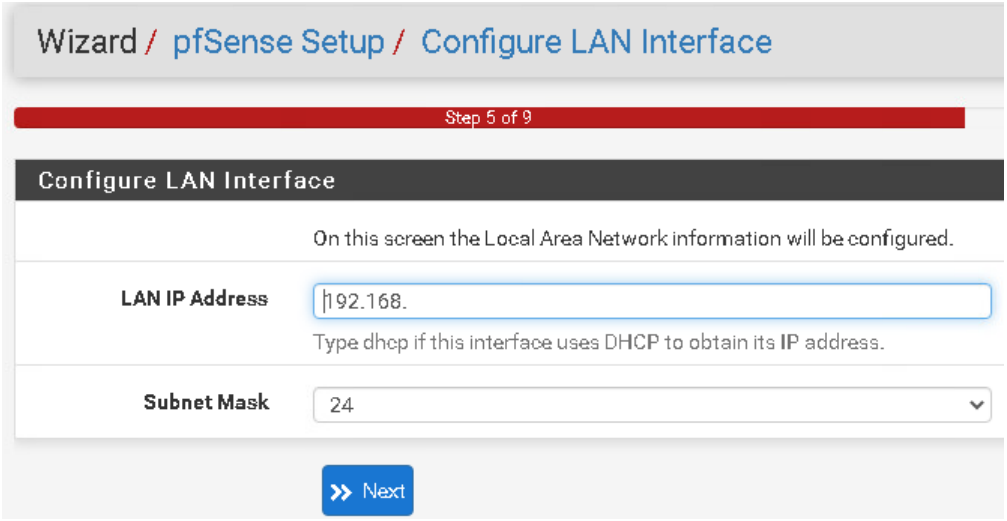

Figura 3.50: Configuración de interfaz LAN

Por último se cambió la contraseña del administrador, véase Figura 3.51.

Figura 3.51: Actualización de contraseña para pfSense

Al finalizar el asistente, se configuró de manera básica el *Firewall*. Como paso siguiente se configuró el DHCP estático de la LAN en la sección **Services** / **DHCP Server** / **LAN**, en el cual, se configuraron los rangos de IP's y los DNS de la UNAM, véase Figura 3.52 y Figura 3.53.

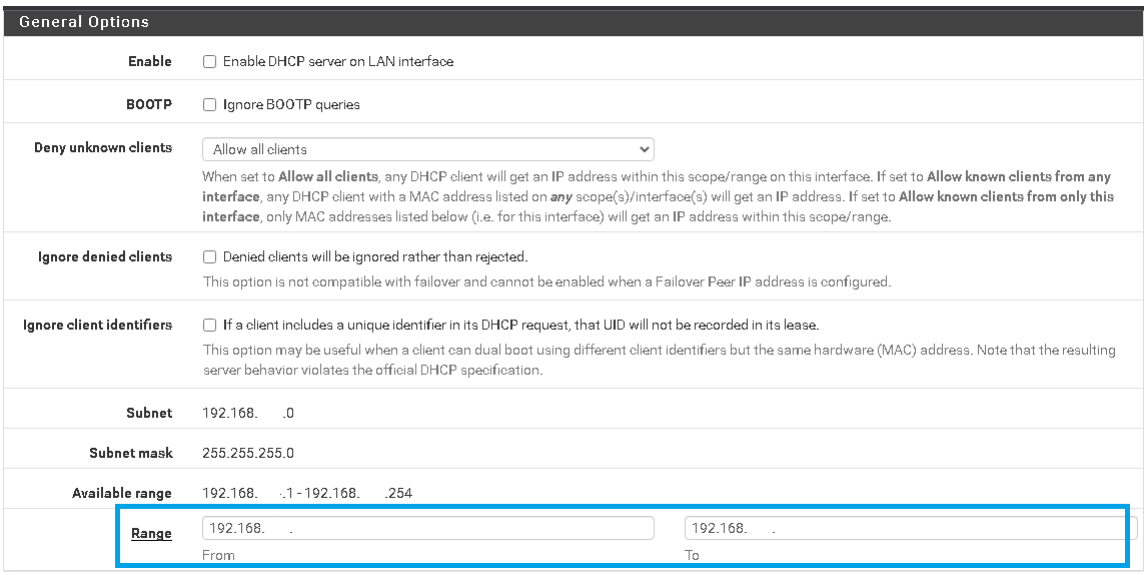

Figura 3.52: Configuración DHCP LAN

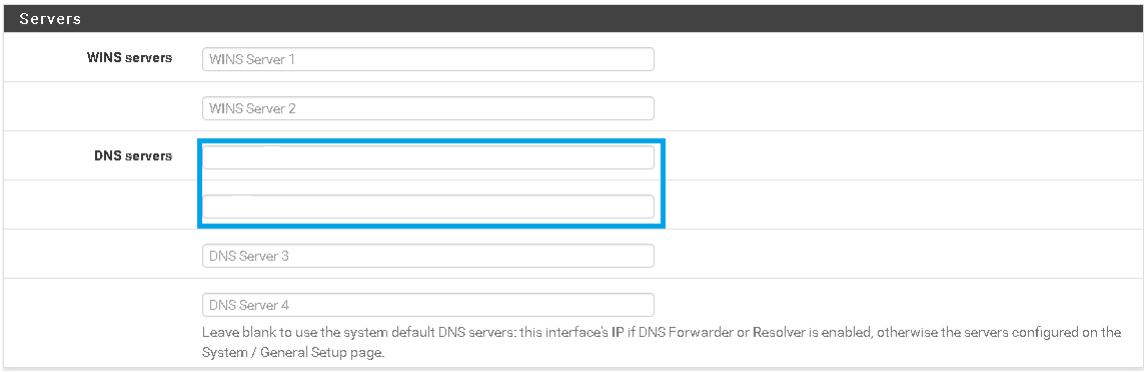

Figura 3.53: DNS de la UNAM

Se crearon dos usuarios nuevos y se agregaron al grupo de administradores, con la finalidad de usarlos para conexiones remotas SSH.

Servidor WEB En el caso del servidor que contendrá la página web del laboratorio, se eligió ubuntu server LTS se descargó la imagen ISO de la página https://ubuntu.com/download/server y se cargo al **datastore1** de ESXi, para poder crear la máquina virtual.

La máquina virtual para el servidor WEB contará con las siguientes características:

- Nombre: Server LGYEC
- CPU: dos vCPU
- RAM: 3 GB
- Hard Disk: tres unidades 512 GB, 40 GB y 40 GB
- Network adapter: 1 interfaz (LAN)

El servidor WEB contará con las siguientes configuraciones:

- Asignación IPv4: Static
- Address: 192.168.xxx.xxx

- Subnet mask: 255.xxx.yyy.zzz
- DNS UNAM Asignación
- IPv6: none
- Nombre: Laboratorio de Geomática y Especialidades de Civiles
- Nombre de la máquina: lgyecs
- Usuario:xxx
- Contraseña:XXX

Para la creación de la máquina virtual se siguieron los mismos pasos que la sección 3.2.3. Una vez creada la máquina virtual se procedió a configurar un LAMP[3].

Finalizada la configuración del servidor web se crearon las reglas en el NAT del pfSense a partir de la sección ***Firewall / NAT / Por Forward*** . Para crear cada regla se necesito: interfaz, protocolo, dirección fuente, puerto fuente, dirección destino, puerto destino, NAT IP (dirección del servidor), NAT puerto (puerto del servidor interno). Se crearon las reglas para los servicios HTTP y SSH del servidor web de los Laboratorios de Geomática y Especialidades de Civiles, véase Figura 3.54.

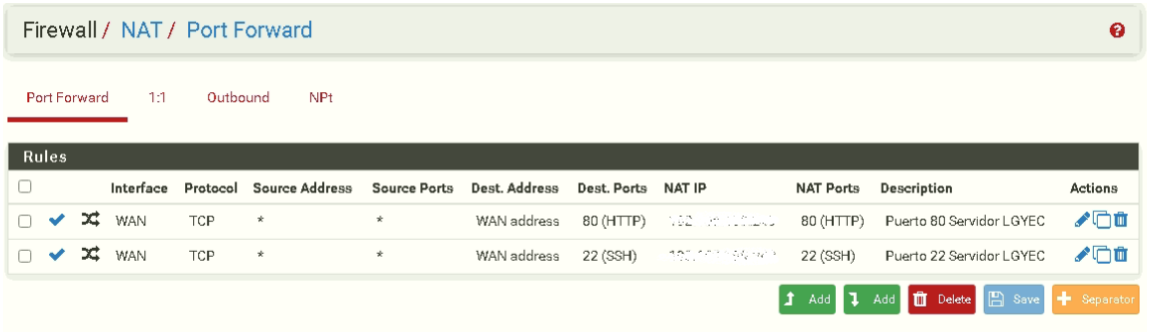

Figura 3.54: Reglas NAT

Al crear estas reglas en el NAT se crearon automáticamente las reglas en el *Firewall*, véase Figura 3.55. Como punto adicional se crearon tres usuarios en el servidor proporcionándoles permisos de administrador, para poder conectarse remotamente mediante SSH.

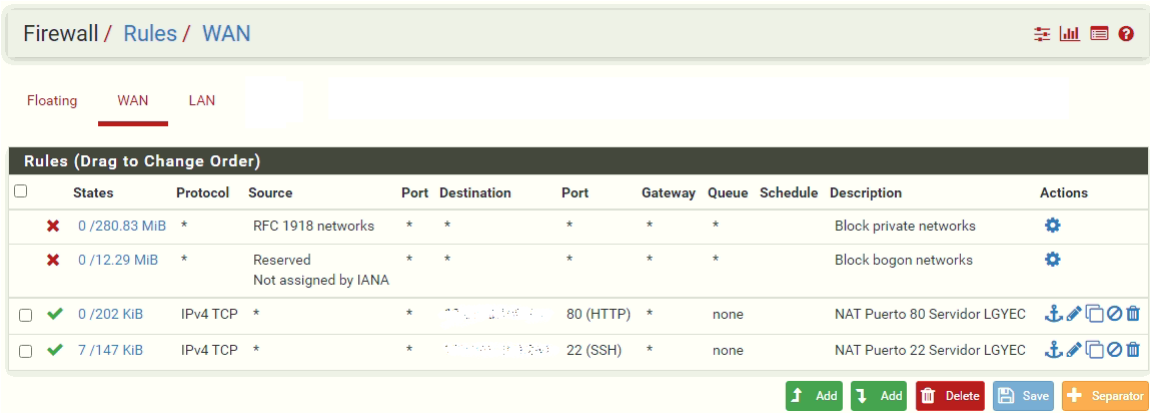

Figura 3.55: Reglas en *Firewall*

[3]Acrónimo que describe un sistema de infraestructura de red que cuenta con las siguientes herramientas:Linux, Apache, MySQL y PHP.

3.2.4. Seguridad del Servidor

SSH mediante clave pública y privada, para el servidor web y pfSense (*Firewall*)

Para la administración de cada una de las máquinas virtuales de manera remota se implementó el protocolo SSH[4] con criptografía asimétrica, con la finalidad de que la comunicación se encuentre cifrada mediante claves y no con una frase que se pueda determinar. Con esta implementación sólo el personal y equipo autorizado tendrá acceso a las máquinas vituales. En el caso del servidor web se utilizará el puerto PP y para el pfSense se utilizará el puerto PPPP. Las llaves se generaron en el equipo del administrador mediante el comando ***ssh-keygen -t rsa.***

Al generar las llaves, estas se guardaron en la ruta por default, se agregó una contraseña para poder aumentar la seguridad de la llave privada, véase Figura 3.56 y Figura 3.57.

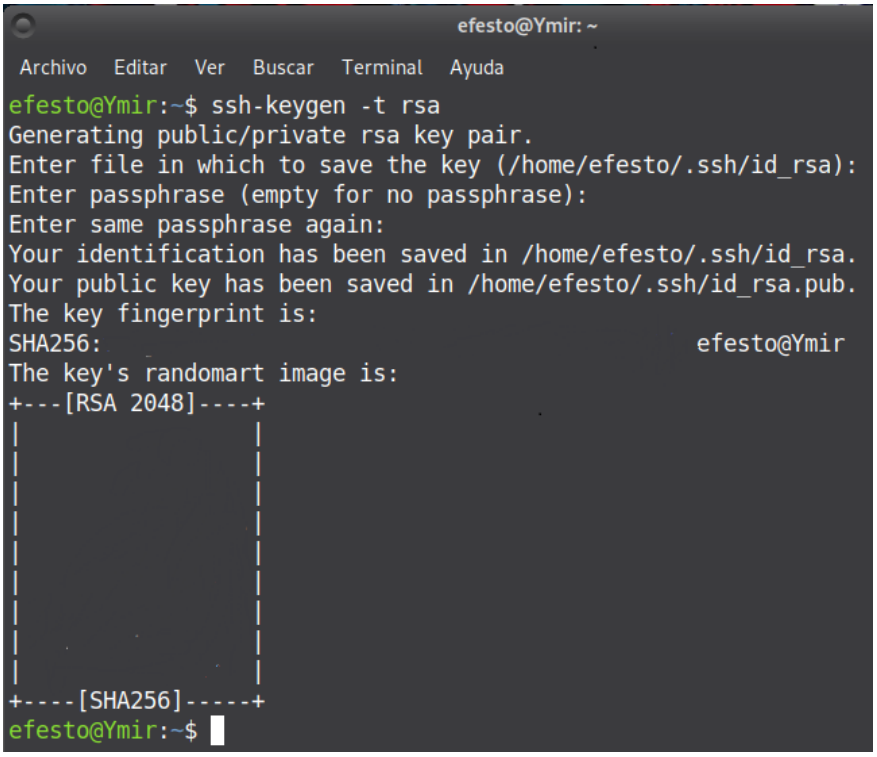

Figura 3.56: Generación de llaves pública-privada

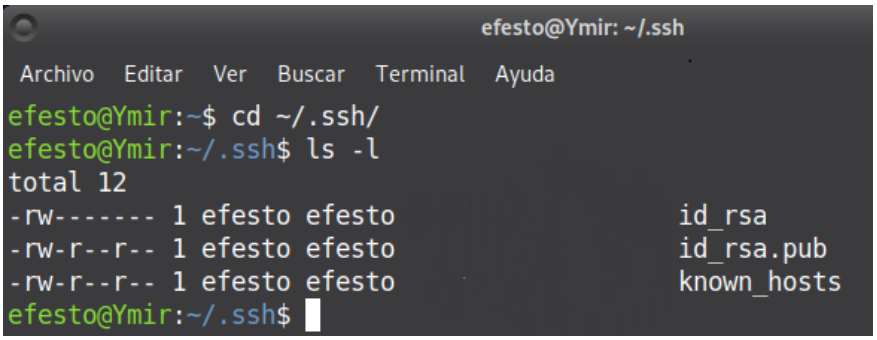

Figura 3.57: Directorio de las llaves pública-privada

Una vez generadas las dos llaves, se copió la llave pública al servidor web mediante el comando **ssh-copy-id usuario@direccion_servidor**, se ingresó la contraseña del usuario para confirmar su identidad, véase Figura 3.58. La llave pública del cliente se copió en el archivo **authorized_keys**.

[4]Protocolo que proporciona una comunicación segura entre dos sistemas, implementando la arquitectura cliente-servidor. A diferencia de otros protocolos de comunicaciones, SSH cifra la conexión.

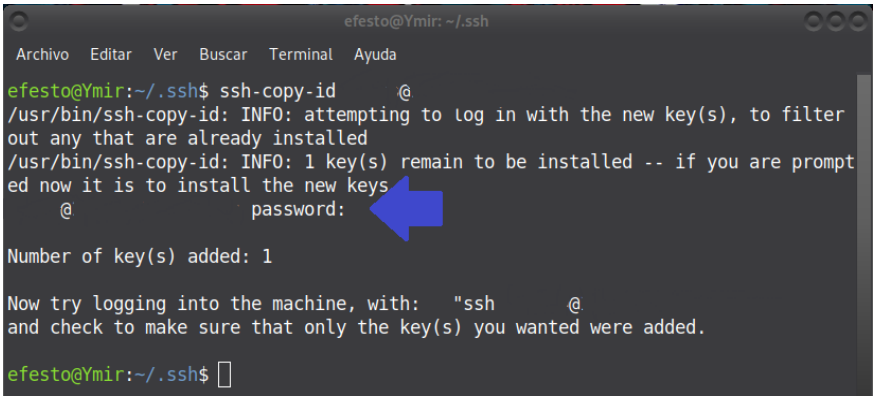

Figura 3.58: Copia de clave pública al servidor web

Se comprobó la conexión mediante el comando **ssh usuario@direccion_servidor**, paso siguiente, se confirmó la contraseña con la que se crearon las llaves, ya que, esta la solicita el sistema para poder leer la llave privada. Posteriormente se cerró la conexión automáticamente, véase Figura 3.59.

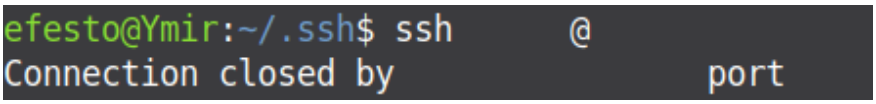

Figura 3.59: Conexión al servidor web

Se probó nuevamente la conexión con el comando **ssh usuario@direccion_servidor** y en esta ocasión la conexión no solicitó ninguna confirmación de contraseña, inmediatamente mostró el usuario en específico, véase Figura 3.60.

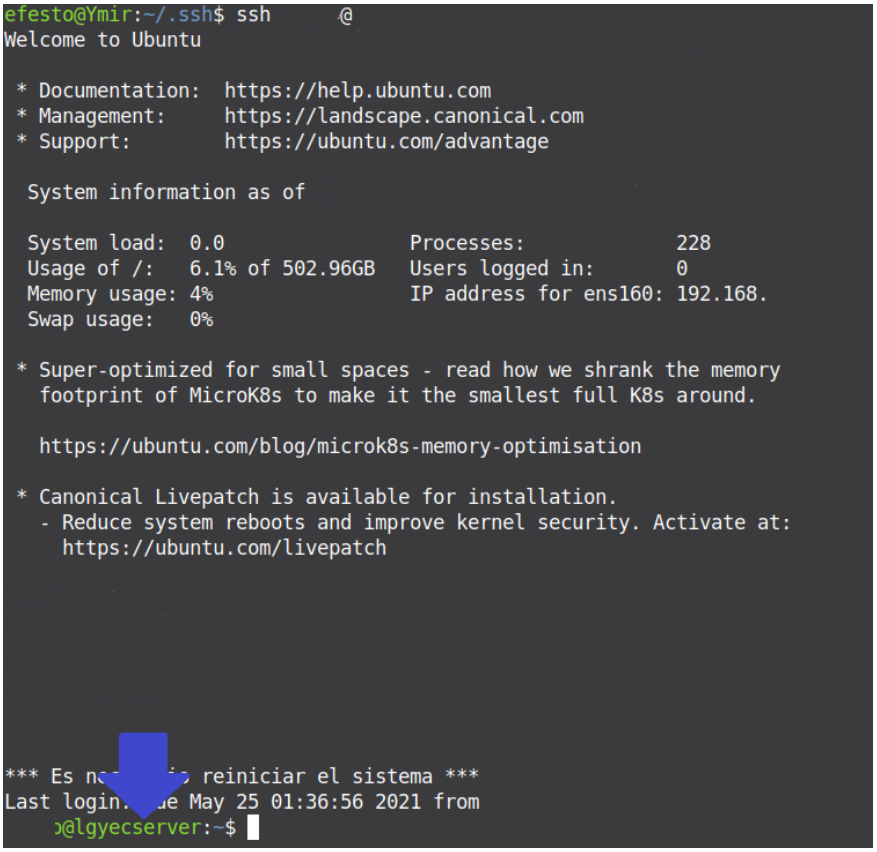

Figura 3.60: Conexión con el servidor web sin confirmar contraseña

Se modificó el archivo de **sshd_config** y se negó el acceso mediante contraseña para la conexiones, con el argumento **PasswordAuthentication no**.

En el caso de pfSense se habilitó *Secure Shell* en el apartado ***System / Advanced / Admin Access***, forzando el uso de llave pública y cambiando el puerto común de conexión SSH, véase Figura 3.61. Se utilizó la misma llave pública, la cual se agregó en el apartado de ***Keys / Authorized SSH Keys*** en los campos del usuario administrador, véase Figura 3.62.

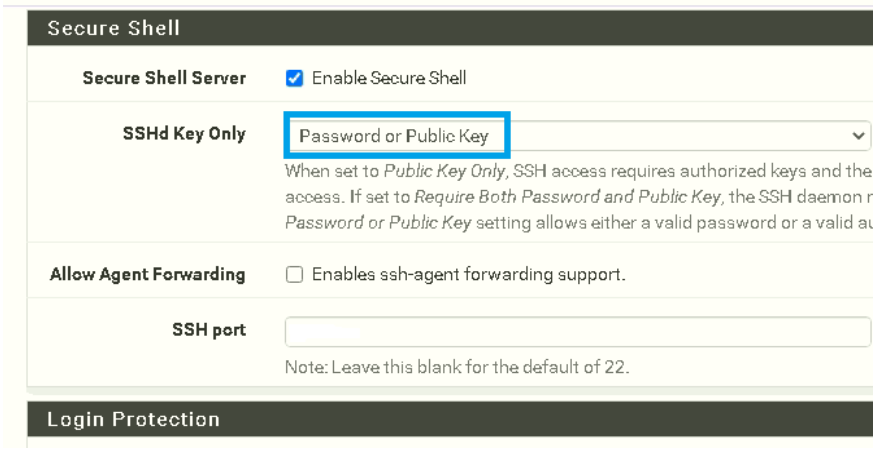

Figura 3.61: Especificaciones de SSH en pfSense

Figura 3.62: Llave pública en pfSense

Para finalizar las configuraciones en pfSense, se creó una nueva regla de acceso en el *Firewall* especificando el puerto usado y la descripción de la regla. Se probó la conexión mediante el comando **ssh -l usuario -p puertoUsado direccion_servidor**, posteriormente, se confirmó la contraseña con la que se crearon las llaves ya que esta la solicita el sistema para poder leer la llave privada, véase Figura 3.63 y Figura 3.64. Posteriormente se cerró la conexión automáticamente.

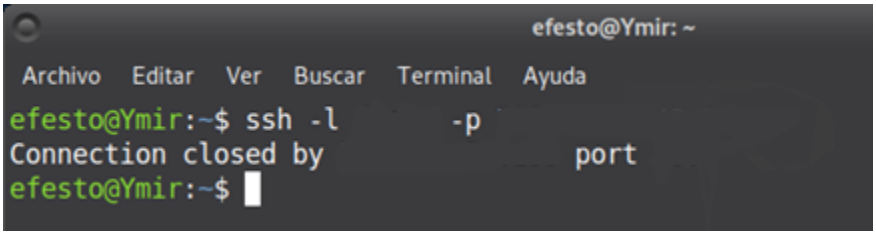

Figura 3.63: Conexión SSH a pfSense

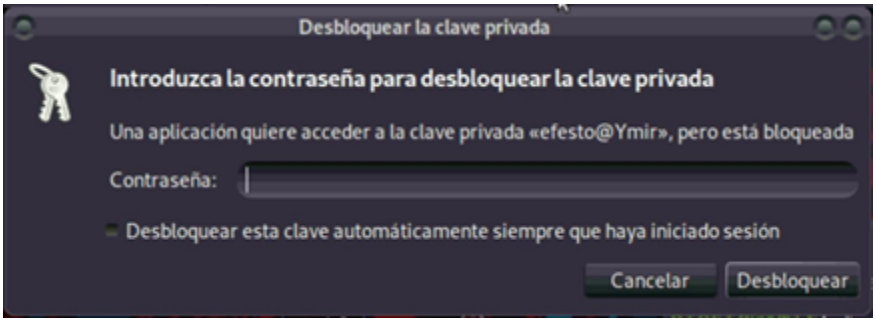

Figura 3.64: Desbloqueo de llave pública en cliente

Se probó nuevamente la conexión con el comando **ssh -l usuario -p puertoUsado direccion_servidor** y en esta ocasión la conexión no solicitó ninguna confirmación de contraseña, inmediatamente mostró el usuario en específico, véase Figura 3.65.

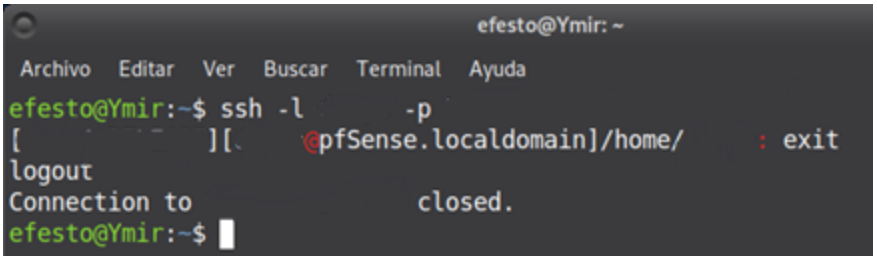

Figura 3.65: Conexión con pfSense sin confirmar contraseña

3.2.5. Creación de las VLAN

Grupos de Trabajo

Aprovechando las ventajas de las VLAN explicadas en el capítulo 1 sección 1.3.1, se crearon cinco redes virtuales que corresponden a cada área de trabajo:

- Laboratorio de Geomática
- Laboratorio de Especialidades de Civiles
- Conexiones Inalámbricas
- Personal Administrativo
- Administración de red

Se asignaron los PVID, nombre de VLAN y gateway para cada VLAN (véase Tabla 3.2), así como identificar los patch cords e interfaces de red físicas en el ESXI de la WAN y LAN (véase Tabla 3.3).

Tabla 3.2: Datos de VLAN

PVID	VLAN	Gateway
10	Personal Administrativo	192.168.XX.XX/24
20	Conexiones Inalámbricas	192.168.XX.XX/24
30	Lab.Geomática	192.168.XX.XX/24
40	Lab. Esp. de Civiles	192.168.XX.XX/24
1000	Equipo de Red	192.168.XX.XX/24

Tabla 3.3: Datos de las interfaces físicas

Red	Dirección Física Interface Física	Dirección Física Interface Virtual	Etiqueta	Puerto en switch 3
LAN y VLAN´s	D0:94:66:xx:yy:zz	00:0C:29:xx:yy:zz	GB-01	pp
WAN	D0:94:66:xx:yy:zz	00:0C:29:xx:yy:zz	GB-02	pp

3.2.5.1. Configuración de las VLAN

En la implementación y puesta en marcha de las VLAN, se mapearon todos los nodos del Laboratorio de Geomática y Especialidades de Civiles, para determinar su estado y la ubicación en switch. Esta información se puede revisar en el manual técnico para el administrador.

En la sección ***Interfaces / VLANs*** de pfSense se crearon las VLAN con sus respectivos datos, ingresando como interfaz principal la red LAN,véase de la Figura 3.66a la Figura 3.68.

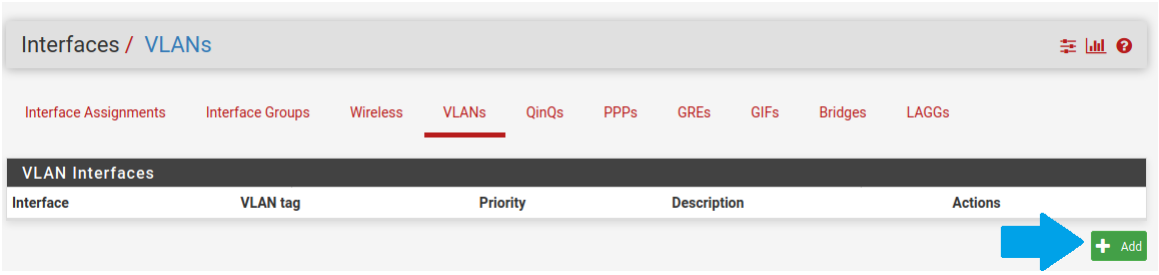

Figura 3.66: Agregar VLANs

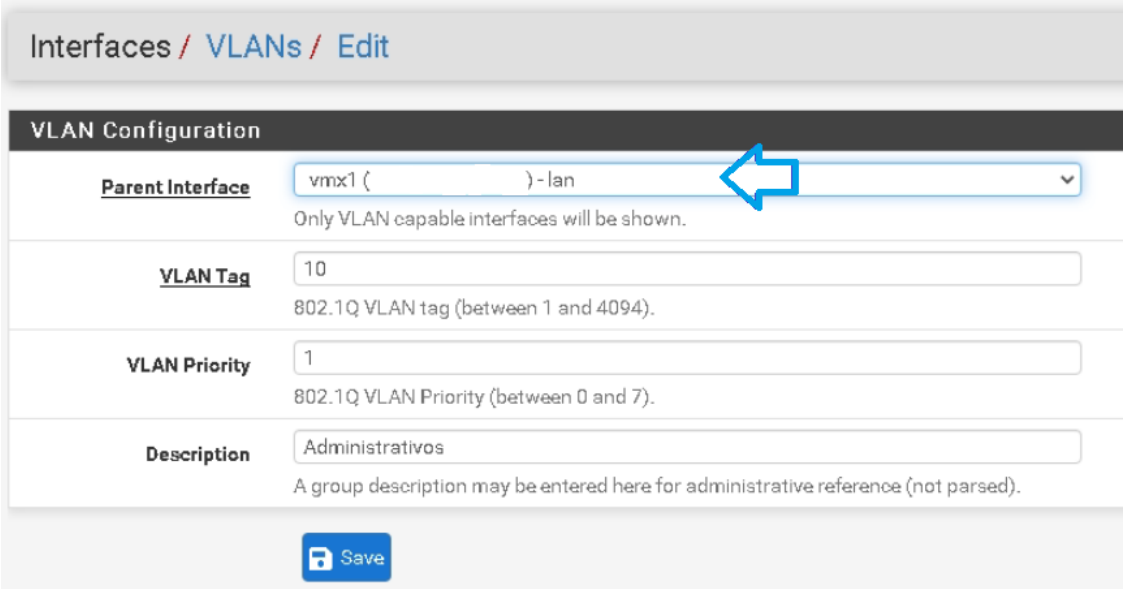

Figura 3.67: Detalles de VLAN

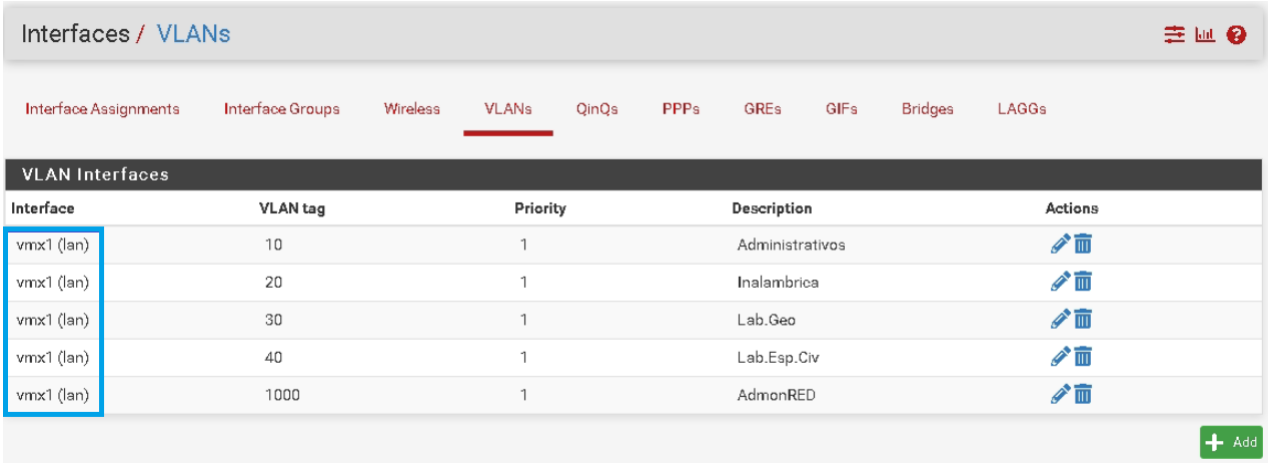

Figura 3.68: Listado de VLANs

En la sección ***Interfaces / Interface Assignments*** se asignaron cada una de las VLANs ya creadas, véase Figura 3.69.

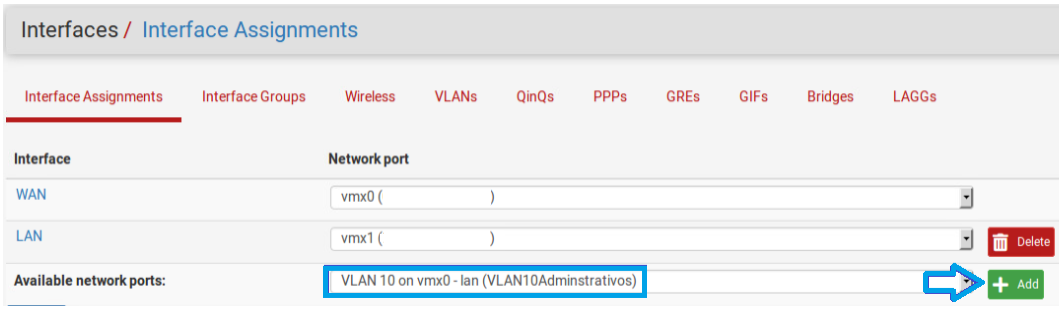

Figura 3.69: Asignación de VLANs

Se habilitaron las interfaces de cada VLAN y se asignó su IP de manera estática, recordando que esta IP será el gateway para cada VLAN, véase Figura 3.70 y Figura 3.71.

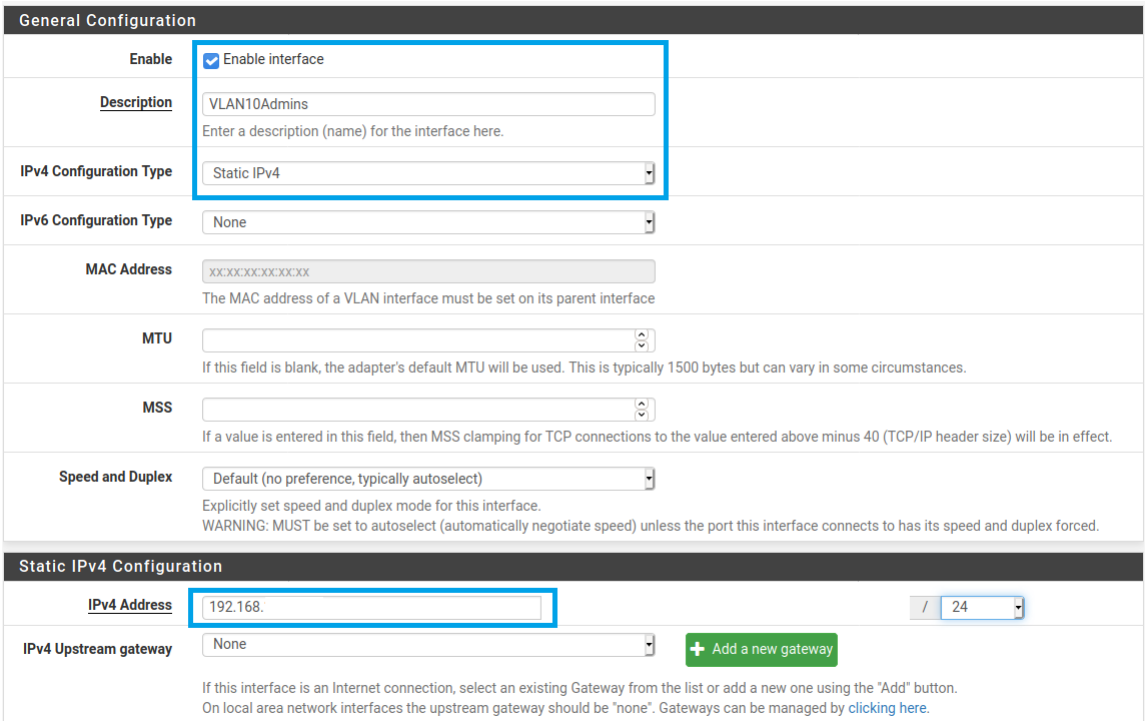

Figura 3.70: Configuración de VLAN

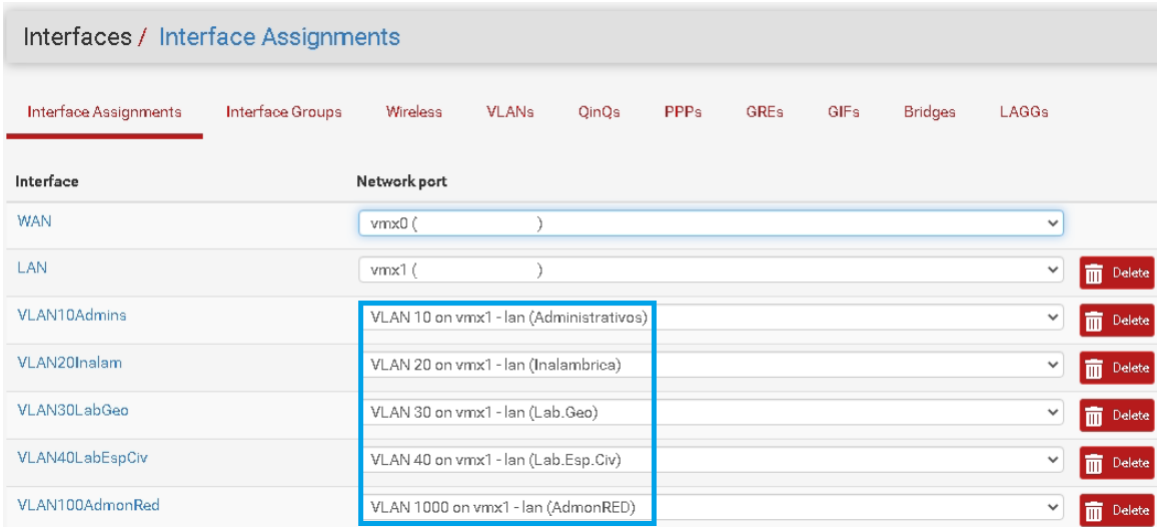

Figura 3.71: Listado de interfaces asignadas

Se habilitó el servicio DHCP en la sección ***Services / DHCP Server***, con un rango de ciento veinte IPs utilizables para los equipos y nodos libres de cada VLAN sin olvidar los DNS de la UNAM, véase Figura 3.72.

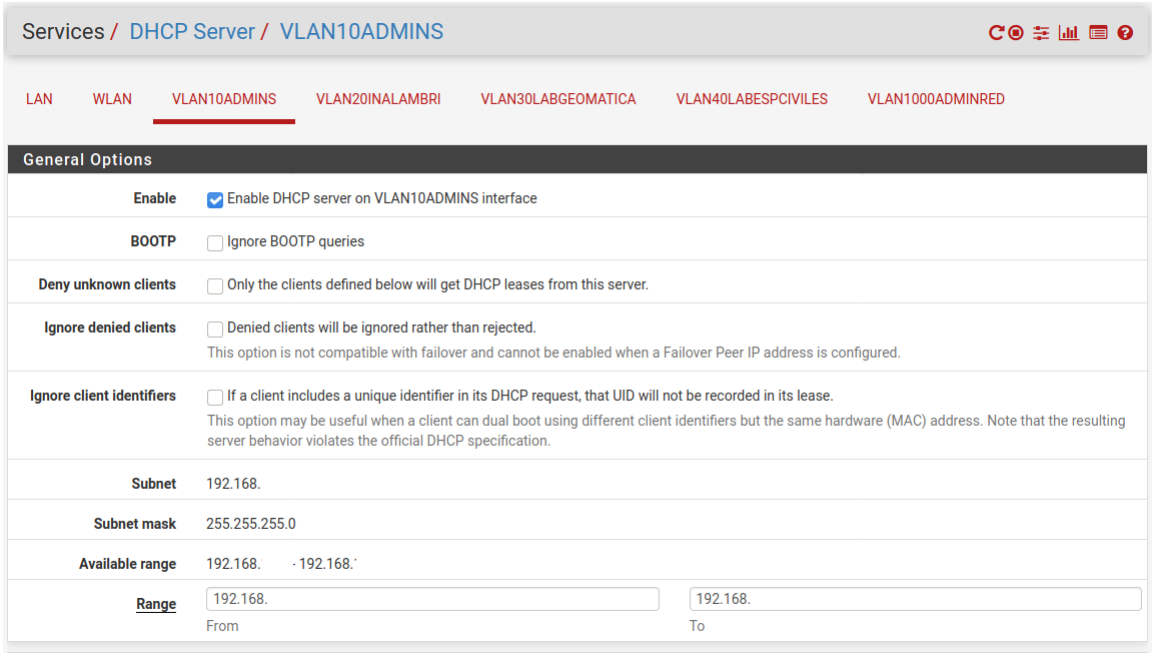

Figura 3.72: Configuración de DHCP para cada VLAN

En la sección ***Firewall / Rules***, se crearon las reglas básicas de paso para cada una de las VLAN, véase Figura 3.73.

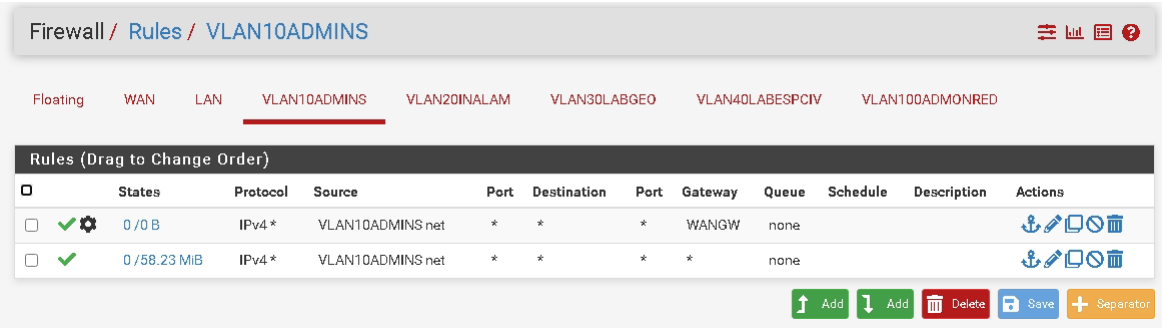

Figura 3.73: Reglas de paso

Dentro del host ESXi se crearon cinco grupos de puertos, uno por cada VLAN. En cada uno de ellos se especificó el Nombre y ID de la VLAN, también se seleccionó el SwitchLAN(switch virtual asociado a la interfaz de la LAN) como el conmutador virtual, véase Figura 3.74.

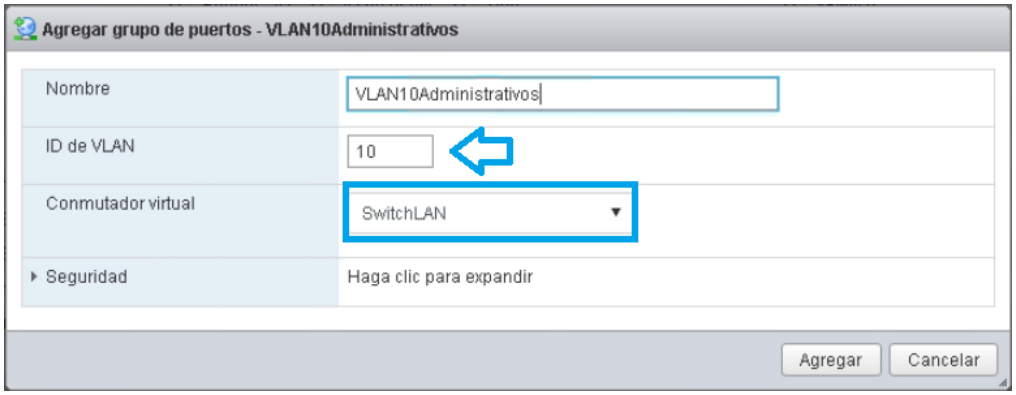

Figura 3.74: Creación de grupo de puertos para cada VLAN

Estos grupos de puertos servirán en el momento que se necesite alguna máquina virtual en una VLAN en específico.

Para que el grupo de puertos de la LAN pueda transmitir tráfico de cualquier VLAN, el ID se modificó a 4095, véase Figura 3.75.

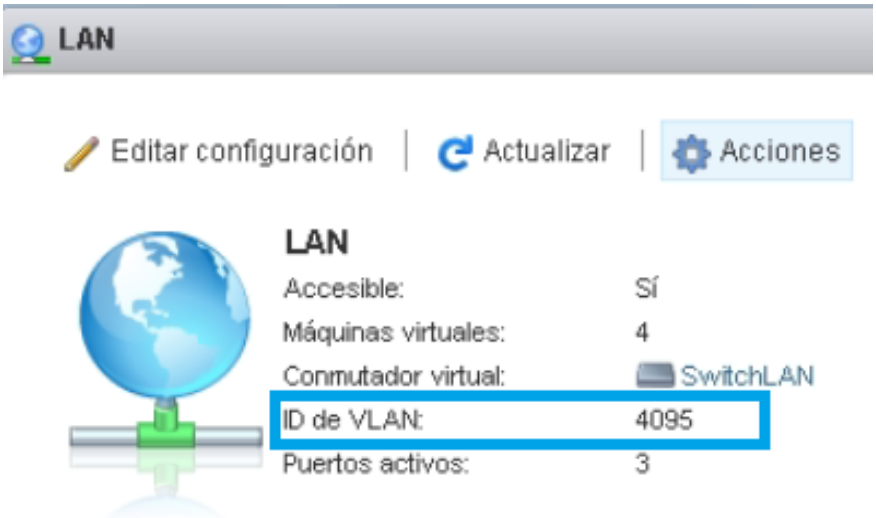

Figura 3.75: Grupo de puertos LAN

En el caso de los switch se crearon las VLAN con su respectivo PVID en la sección ***Network*** / ***Links***, se desplegó la VLAN 1 la cual corresponde a la LAN, véase de la Figura 3.76a la Figura 3.78.

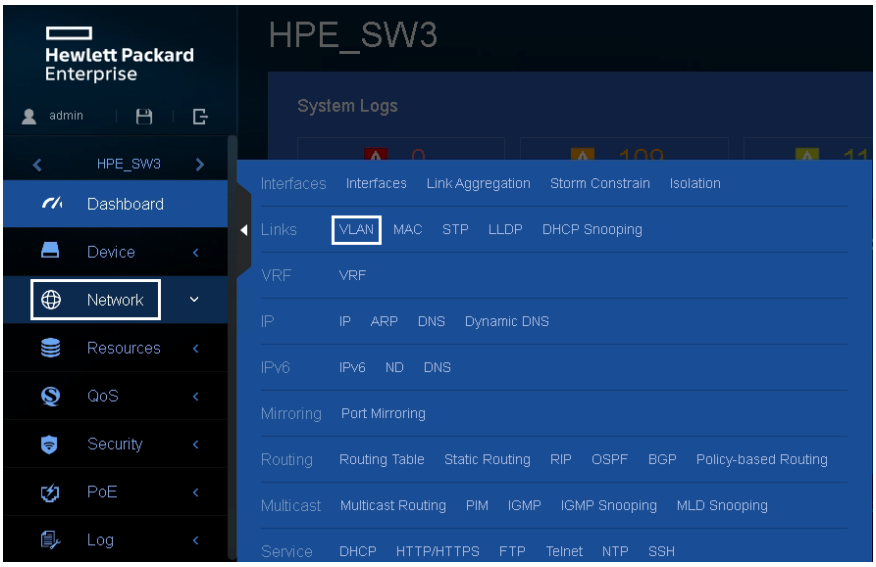

Figura 3.76: Sección para crear VLAN

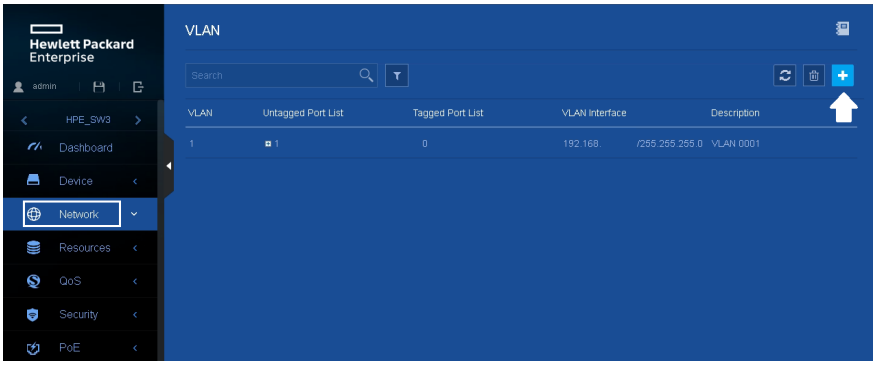

Figura 3.77: Agregar VLAN

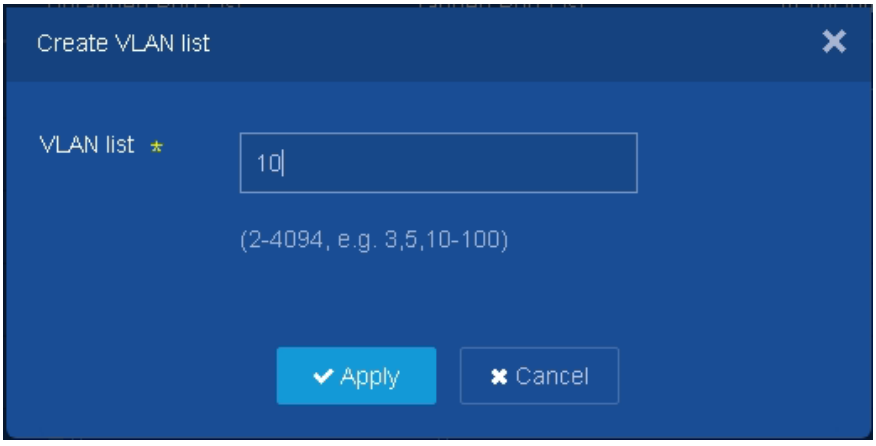

Figura 3.78: Asignación y creación de VLAN

Con la información de cada nodo, mediante el *port switching* se asignó *untagged* a cada puerto en su respectiva

VLAN. Estas configuraciones se realizaron en la interfaz de cada uno de los *switch*, véase Figura 3.79 y Figura 3.80.

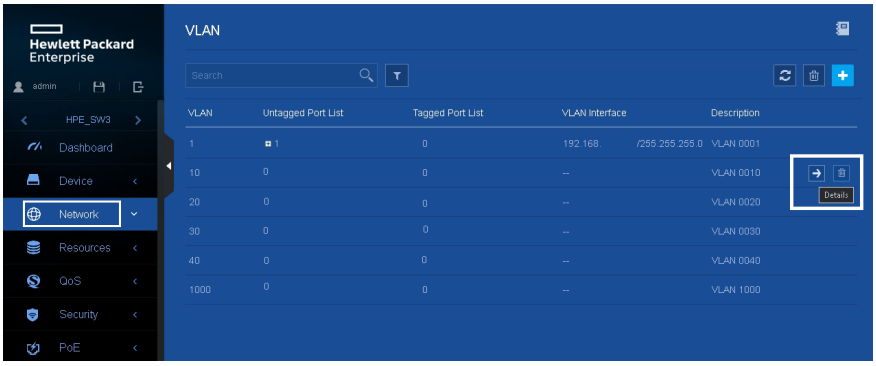

Figura 3.79: Editar configuración de VLAN

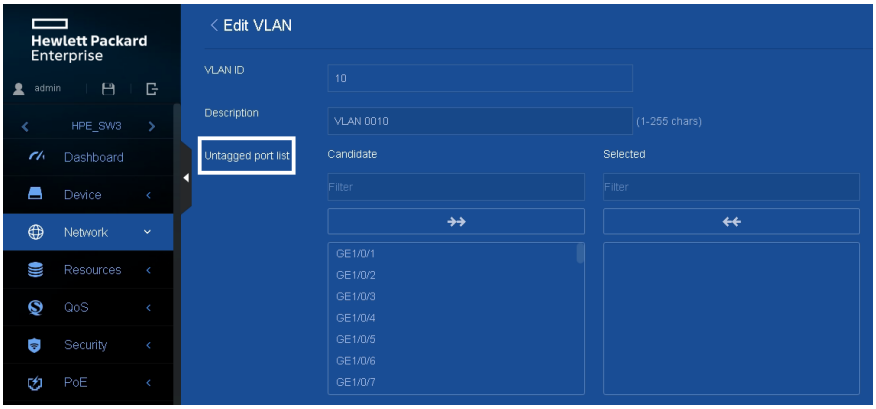

Figura 3.80: Asignación de puertos de manera *untagged*

En el caso de los puertos troncales, se asignaron de manera *hybrid*, *untagged* VLAN 1 y *tagged* el resto de las VLAN. De igual manera estas configuraciones se efectuaron en el resto de switches, véase Figura 3.81.

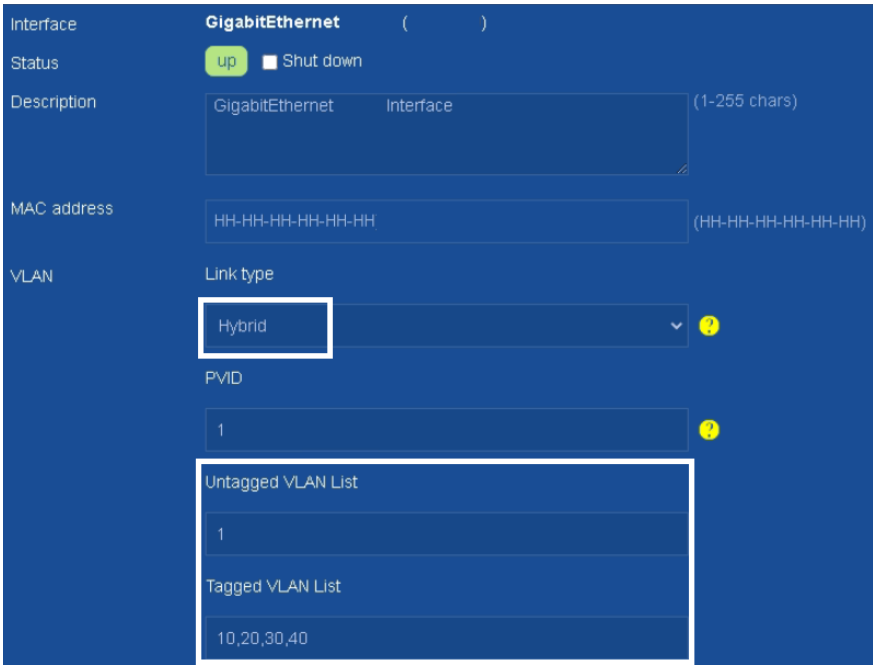

Figura 3.81: Configuración de puertos troncales

Para la fibra óptica se configuró un puerto en específico del *switch* 3 como *untagged* a la VLAN 1 (VLAN *default*) así como la WAN y el puerto del Administrador, también con puertos específicos, véase Figura 3.82.

Figura 3.82: Configuración de puertos

Por último, se asignó un puerto en especifico del *switch* 3 a la VLAN 20 como *tagged*, esto último para que el AP funcionará bajo esa VLAN, todos los cambios en los *switch* se guardaron en el archivo de configuración que utilizará en cada inicio, provocando que los cambios sean permanentes, véase Figura 3.83.

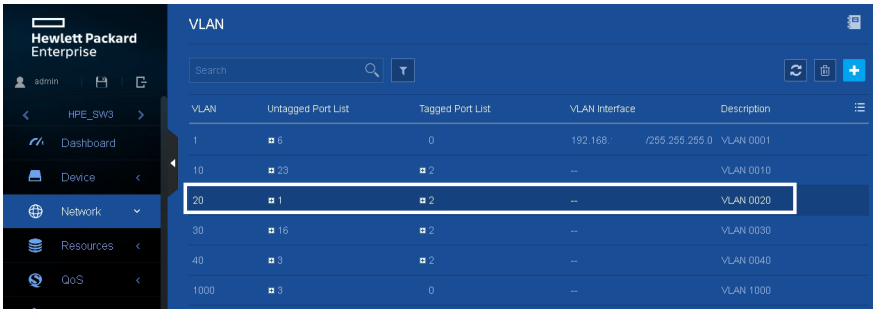

Figura 3.83: Configuración de puerto para AP

Con los datos obtenidos de los equipos de red y equipos de cómputo localizados en el Laboratorio de Geomática y Especialidades de Civiles, se creó un diagrama de red lógico final como se muestra en la Figura 3.84.

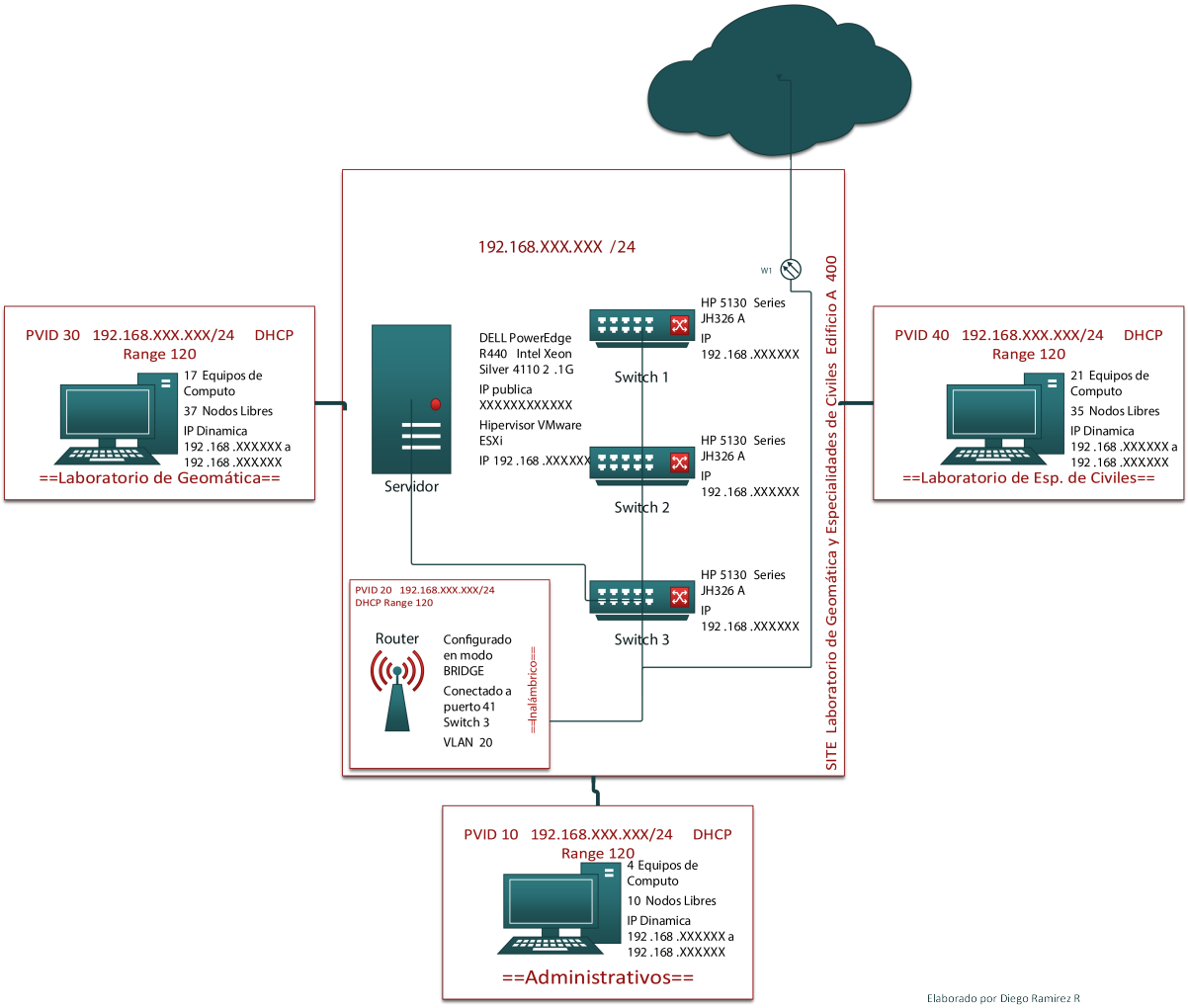

Figura 3.84: Topología Final de Red.

3.2.6. Cambio de equipo de red y servidores a VLAN 1000

Se procedió a cambiar las direcciones IP de los switches, ESXi, Servidor Web y Equipo Administrador, modificando solamente el tercer octeto. En el caso de las máquinas virtuales también se modificó el grupo de puertos de LAN a VLAN1000 esto para que puedan tener el servicio de internet, véase Figura 3.85. En este caso, la decisión de cambiar el segmento de red, así como todas las máquinas virtuales a la VLAN1000, se debió a

que se requirió separar y mantener independiente todo el tráfico del equipo de red para poder lograr una mejor administración del mismo, haciendo uso de las ventajas de tener VLAN.

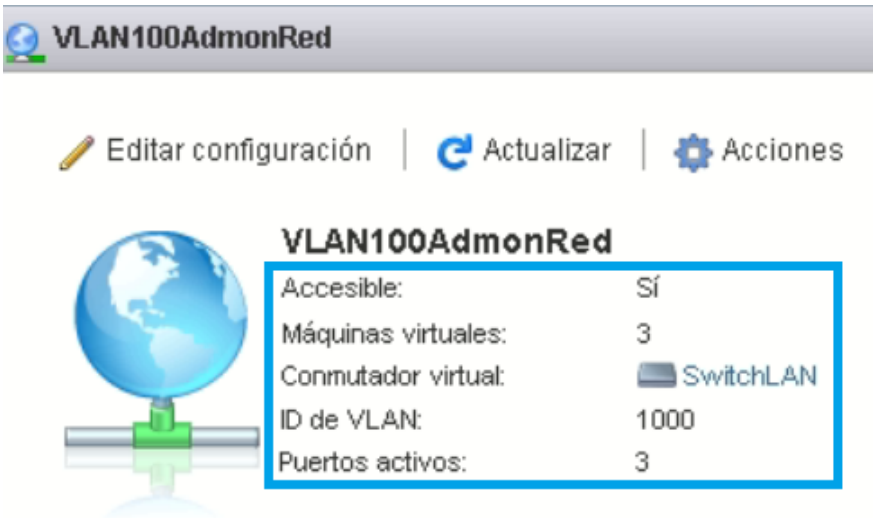

Figura 3.85: Grupo de puertos VLAN100

3.2.7. Creación de VPN

Con la finalidad de administrar de manera remota el equipo de red y los servicios prestados, se creará una VPN(véase el capítulo 1 sección 1.3.1) a la VLAN 1000 con ayuda del pfSense.

3.2.7.1. Configuración

Como paso inicial se instaló en la sección ***System / Package Manager / Available Packages***, el paquete **openvpn-client-export**, el cual servirá para poder exportar los clientes o en este caso los clientes administradores, véase Figura 3.86 y Figura 3.88.

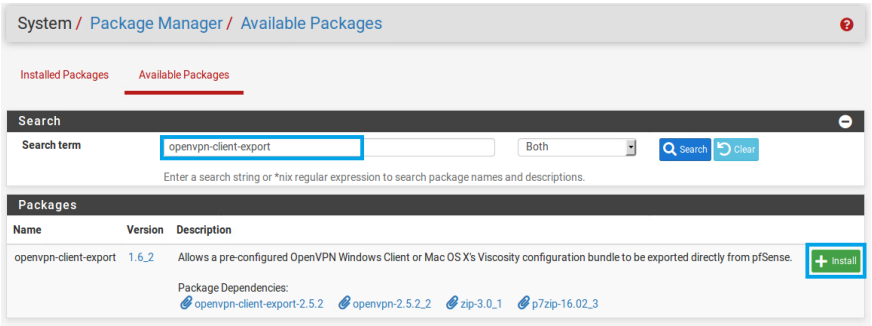

Figura 3.86: Instalación de paquete para exportar clientes VPN

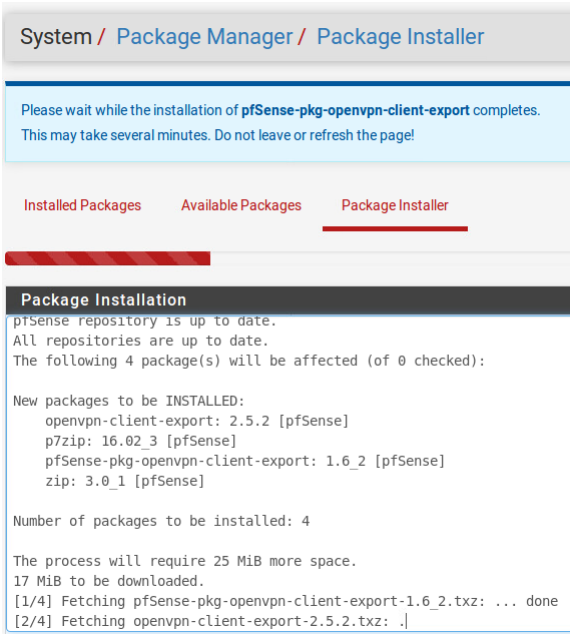

Figura 3.87: Proceso de instalación de paquete

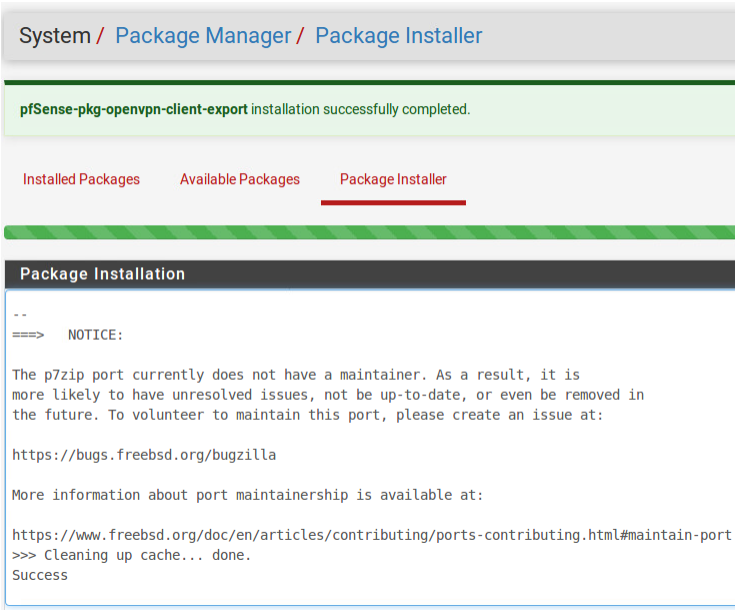

Figura 3.88: Instalación finalizada

Posteriormente se eligió la sección ***VPN*** donde se seleccionó OpenVPN. Para la configuración de la VPN se utilizó el asistente de configuración, véase Figura 3.89.

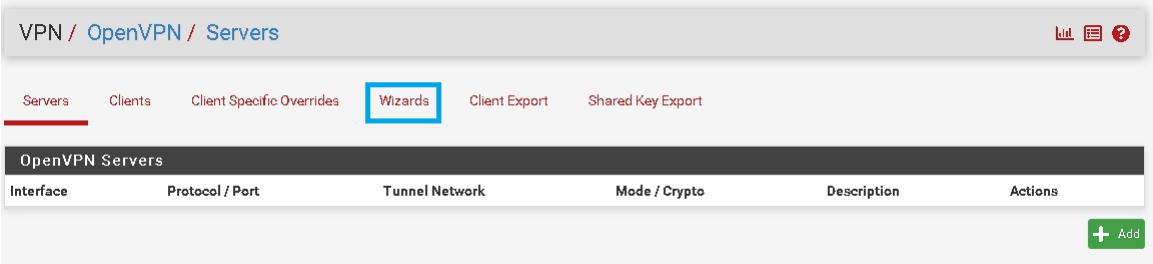

Figura 3.89: Asistente de configuración de OpenVPN

Lo primero es determinar la forma de autenticación de los usuarios, en este caso, se eligió *Local User Access*, véase Figura 3.90.

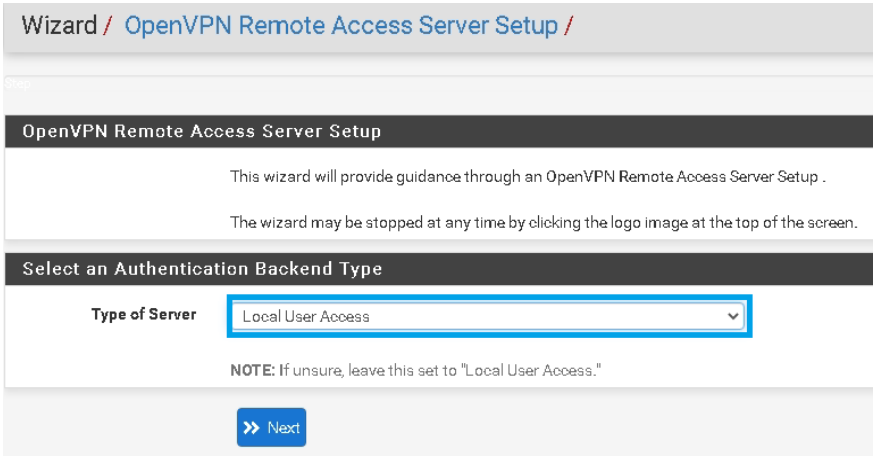

Figura 3.90: Tipo de Servidor a implementar

Paso siguiente se creó la autoridad certificadora la cual, se encargará de emitir los certificados. Los datos relevantes de la unidad certificadora son: la longitud de las llaves de cifrado no menor a 2048 bits y el tiempo en que sea válida la autoridad certificadora, este dato quedó a criterio del super administrador de red, véase Figura 3.91.

Los demás datos son informativos como:

- Código de País
- Estado o Provincia
- Ciudad
- Organización

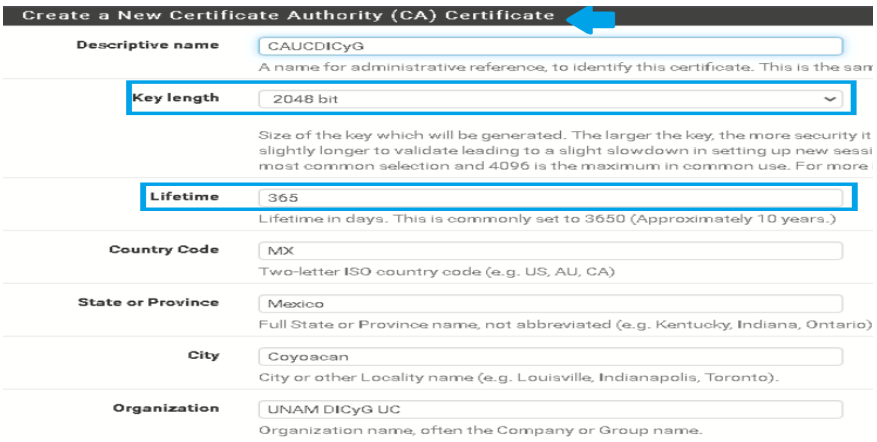

Figura 3.91: Creación de CA

Posteriormente, se creó el certificado del servidor OpenVPN, con la finalidad de demostrar "**que es quien dice ser**". Los datos relevantes en este servidor serán la longitud de las llaves de cifrado que no debe ser menor a 2048 bits, véase Figura 3.92.

Los demás datos son informativos como:

- Nombre del Servidor
- Código de País
- Estado o Provincia
- Ciudad
- Organización

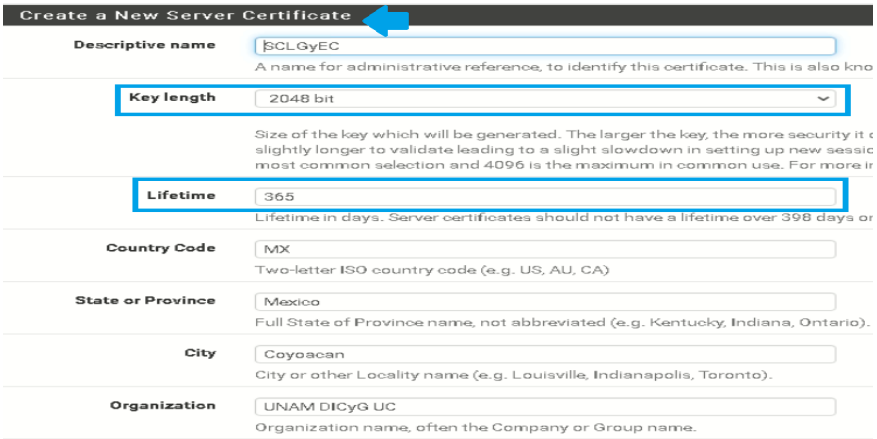

Figura 3.92: Servidor de certificados

En la configuración general del servidor OpenVPN, se seleccionó la interfaz WAN que será el medio por el cual, el servidor escuchará el tráfico de las concesiones VPN. El protocolo que se utilizó será el orientado a la conexión TCP, que garantiza que se establece la conexión entre los dos puntos, lo que nos permite rastrear algún problema si es que lo hubiera. OpenVPN utiliza el puerto 1194 para escuchar el tráfico, pero se tiene la posibilidad de cambiarlo; esto ayuda si se quiere enmascarar el puerto y agregar un nivel más de seguridad a la VPN. Por último se agregó un nombre descriptivo al servidor, véase Figura 3.93.

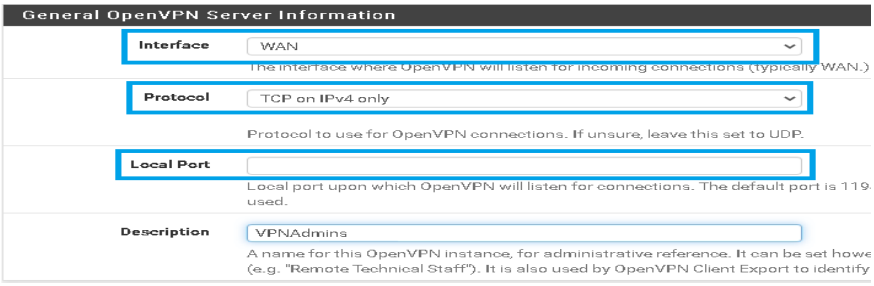

Figura 3.93: Configuraciones generales del Servidor

Para las configuraciones criptográficas, se utilizó TLS para la autenticación (véase Figura 3.94), que es generada por el propio servidor; además, usará el algoritmo de Diffie-Hellman[5], al cual se le proporcionará una longitud mínima de 2048 bits para la llave. También se empleó el algoritmo de cifrado AES-256[6] con un bloque de 128 bits y como algoritmo de digestión se implementó un SHA256[7](véase Figura 3.95).

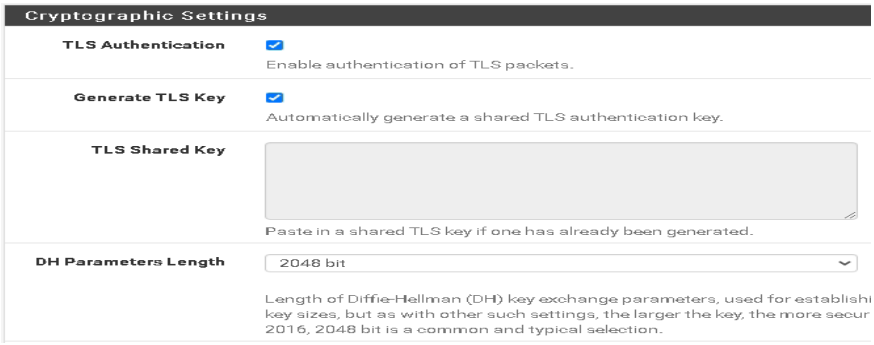

Figura 3.94: Configuraciones criptográficas

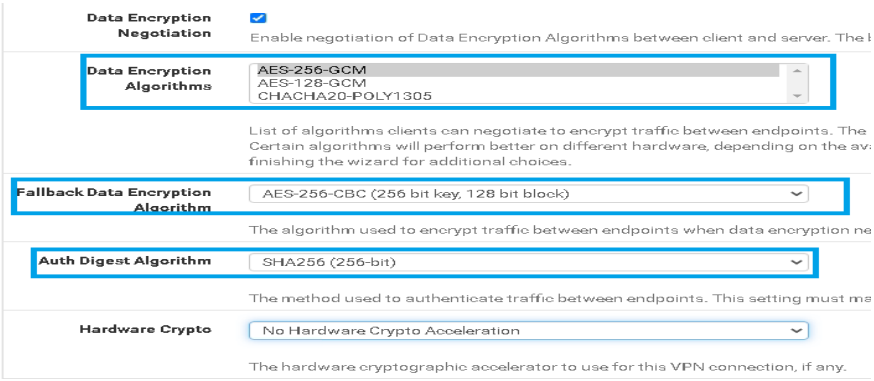

Figura 3.95: Configuración de algoritmos criptográficos

Para las configuraciones del Túnel VPN, se especificó la red que tendrá. Se habilitó el redireccionamiento del gateway, para que todo el tráfico del cliente pase por el túnel, así como la red local de destino, que en este caso será la red de administración. Por el momento solo se configuraron dos clientes concurrentes en el servidor OpenVPN y se prohibirán las conexiones duplicadas, esto para garantizar una sola conexión de algún cliente, véase Figura 3.96.

[5]Algoritmo implementado para el intercambio seguro de claves.Genera una clave secreta entre dos equipos, a través de un canal inseguro.Crea una clave simétrica que cifrara la comunicación entre ambos equipos.

[6]Se basa en sustituciones, permutaciones y transformaciones lineales, cada una de estas ejecutada en bloques de datos de 128 bits. Este proceso se repite varias rondas. El nombre de AES dependerá del tamaño de la llave, el cual puede ser 128, 192 o 256 bits.

[7]También conocido como función hash, es una huella digital única de longitud fija. Tiene entrada de longitud arbitraria y salida de longitud fija (128 a 160 bits). Sin importar la longitud de entrada la longitud de salida será siempre la misma.

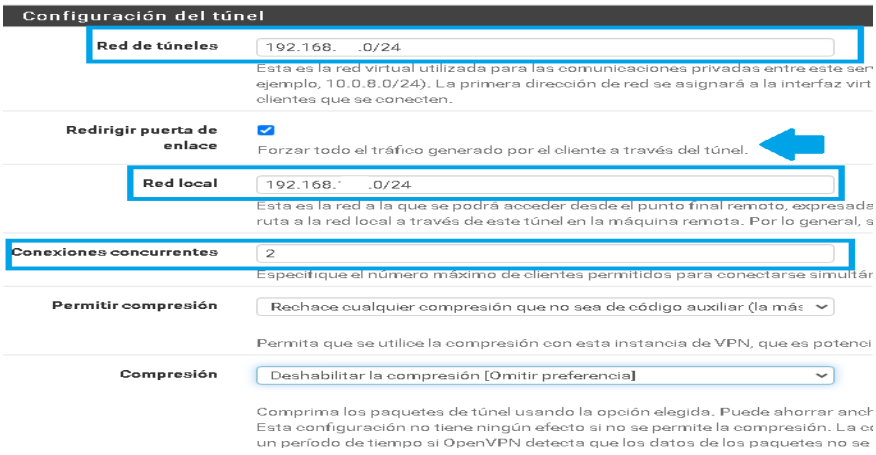

Figura 3.96: Configuraciones del túnel

Para las configuraciones de los clientes OpenVPN, se habilitó la asignación de IP dinámicas y los DNS de la UNAM, véase Figura 3.97. Por último, se generaron las reglas automáticamente en el Firewall, para permitir el tráfico a través de la VPN y el tráfico con el servidor OpenVPN, véase Figura 3.98.

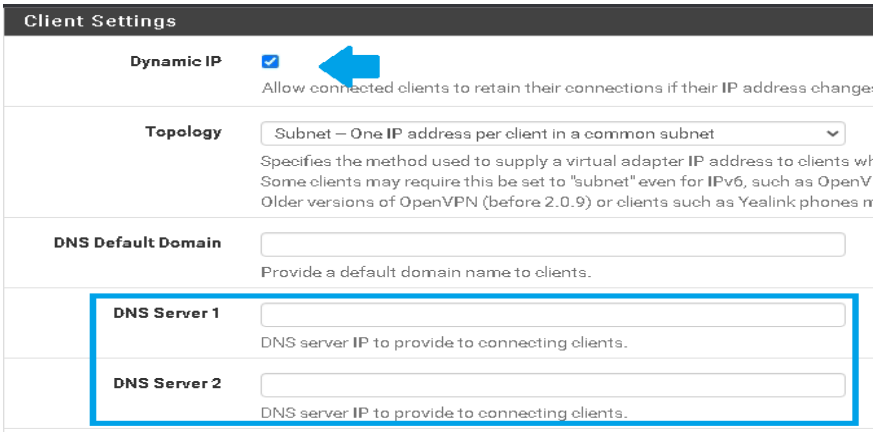

Figura 3.97: Configuraciones de clientes

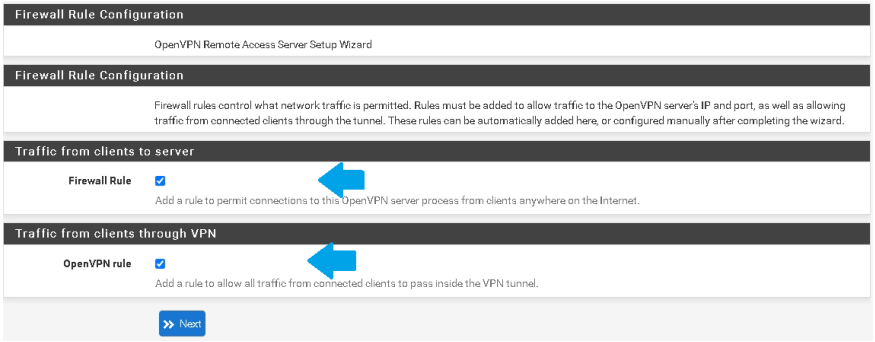

Figura 3.98: Creación de reglas en *Firewall*

Se aprovecharon los dos usuarios creados previamente. En la opción ***User Certificates*** se agregó el certificado para cada usuario, donde se eligió la autoridad certificadora, la longitud de la llave que es 2048, el tiempo de vida que tendrán estos certificados y una breve descripción, véase de la Figura 3.99 a la Figura 3.101.

Figura 3.99: Creación de certificado para usuario local

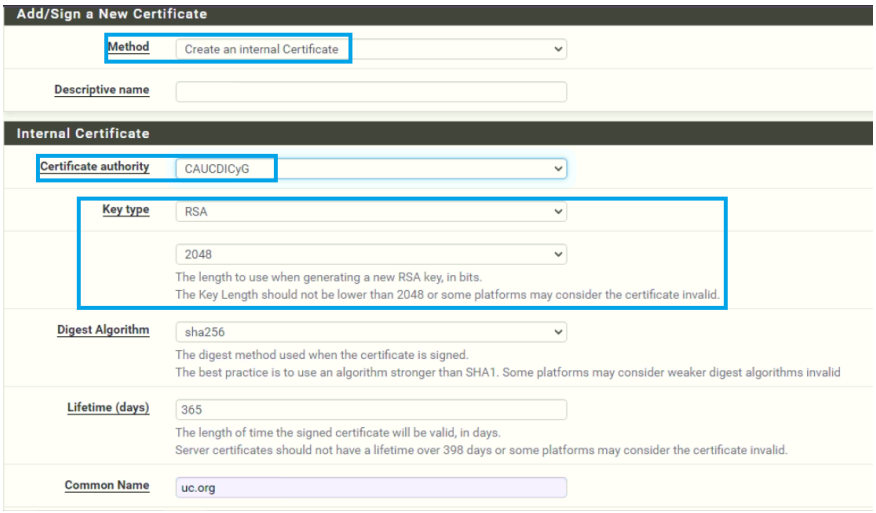

Figura 3.100: Configuración del certificado para usuario local

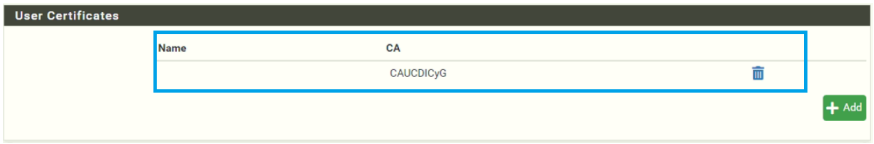

Figura 3.101: Certificado para usuario local

Ya creados los certificados, se exportaron los clientes OpenVPN, en la sección ***OpenVPN / Client Export Utility***. En la opción OpenVPN *Clients*, se exporto el archivo de instalación dependiendo del sistema operativo del cliente, véase Figura 3.102.

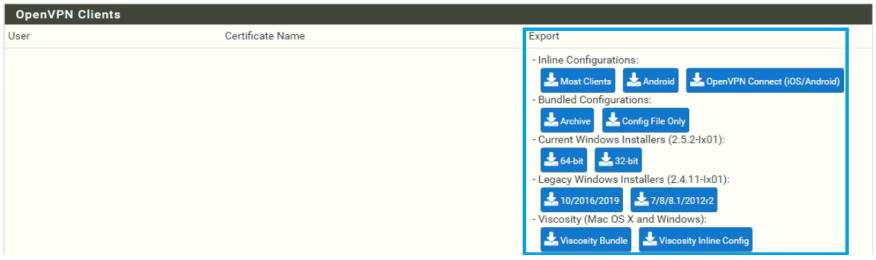

Figura 3.102: Cliente OpenVPN

Capítulo 4 Implementación de herramientas especializadas

Capítulo 4

Implementación de herramientas especializadas

4.1. Herramientas de monitoreo

El monitoreo de red proporciona la información necesaria para que el administrador pueda determinar si alguna red o servicio funciona correctamente e implementar medidas de seguridad y corrección. En el mercado, existen muchas y diversas herramientas que ayudan al monitoreo y control de una red de datos, sin embargo, en la Unidad de Cómputo tienen herramientas que usan de manera estándar, algunas de ellas son NTOPNG y tcpdump.

4.1.1. NTOPNG

Es una herramienta que permite monitorear en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red, puede ayudar a identificar malas configuraciones de algún equipo o servicio. Actualmente existe ntopng que está basado en libpcap[1] / PF_RING[2].

Es capaz de ejecutarse virtualmente en diferentes plataformas como Unix, MacOS y Windows. Proporciona una interfaz web para la exploración de información de tráfico histórica y en tiempo real.

Algunas características:

- Ordena el tráfico de red, de acuerdo con muchos criterios, incluidos la dirección IP, el puerto, los protocolos de aplicación de capa 7 (L7), el rendimiento, los sistemas autónomos (AS).
- Muestra el tráfico de red en tiempo real y los hosts activos.
- Análisis de tráfico IP y orden según la fuente / destino.
- Informar el uso del protocolo IP ordenado por tipo de protocolo.
- Produce estadísticas de tráfico de red HTML5 / AJAX.
- Soporte completo para IPv4 e IPv6.
- Gestión de identidad, incluida la correlación de los usuarios de VPN con el tráfico.

Esta herramienta se instaló en pfSense, en el apartado ***System / Package Manager / Available Packages*** ingresando ntop en la búsqueda, véase Figura 4.1.

[1] Biblioteca C / C ++ portátil para la captura de tráfico de red.

[2] Es un módulo del kernel de Linux y una estructura de espacio de usuario que le permite procesar paquetes a altas velocidades mientras le proporciona una API consistente para aplicaciones de procesamiento de paquetes.

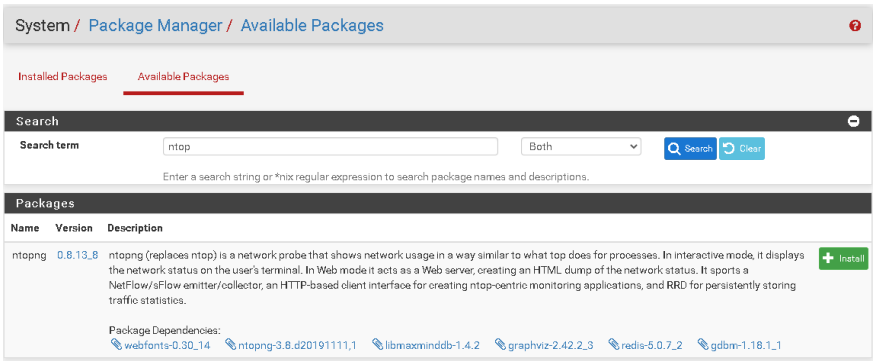

Figura 4.1: Paquete *ntopng*

Se confirmó la instalación de los paquetes necesarios para ntopng, el número de paquetes a instalar y el espacio requerido, véase Figura 4.2 y Figura 4.3.

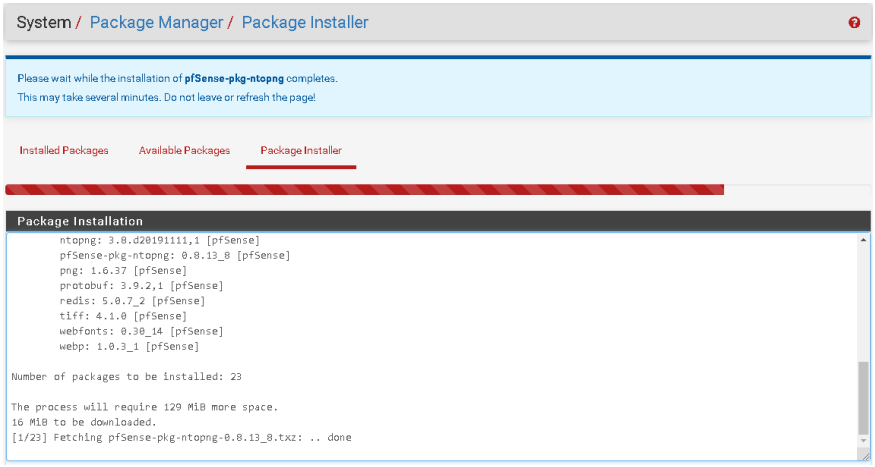

Figura 4.2: Instalación de paquetes necesarios para *ntopng*

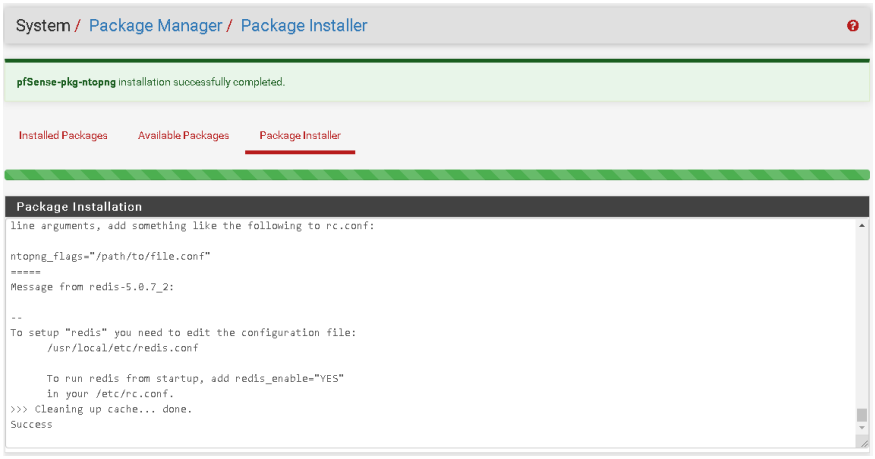

Figura 4.3: Instalación exitosa de ntopng

Para su configuración se ingresó al apartado ***Diagnostics / ntopng Settings***, en las opciones generales se habilitó ntopng, se eligieron todas las interfaces de red y se ingresó una contraseña, véase Figura 4.4.

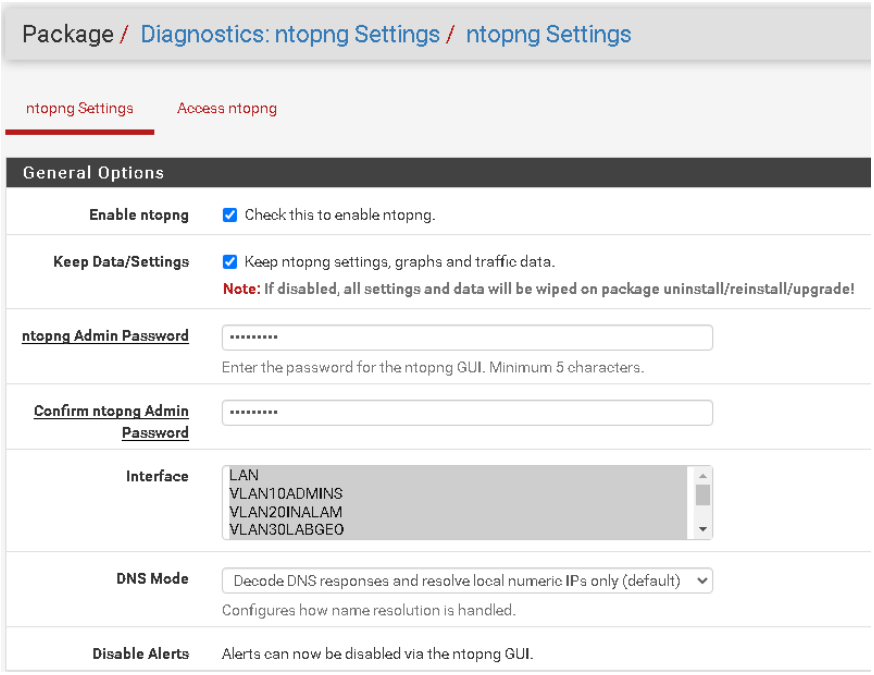

Figura 4.4: Configuraciones generales *ntopng*

Al guardar las configuraciones de ntopng, se corroboró que el servicio esté activo en el apartado ***Status*** / ***Services***, véase Figura 4.5.

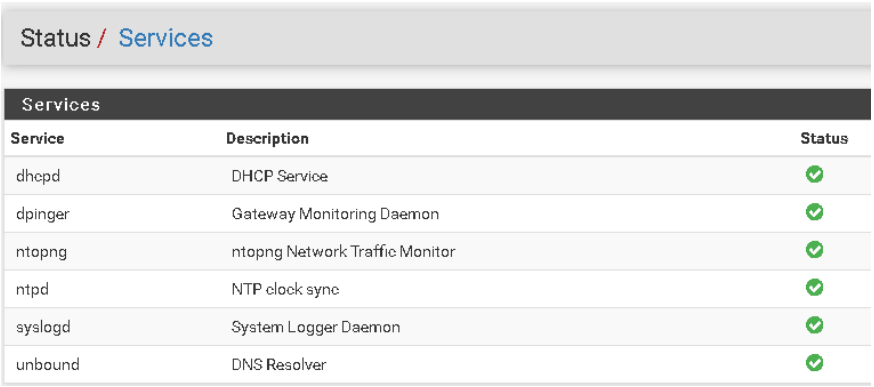

Figura 4.5: Estatus de *ntopng*

Para ingresar a la interfaz de ntopng, se ingresó en el apartado ***Diagnostics*** / ***ntopng***. También se puede acceder con la dirección IP local de pfSense y el puerto 3000, véase Figura 4.6.

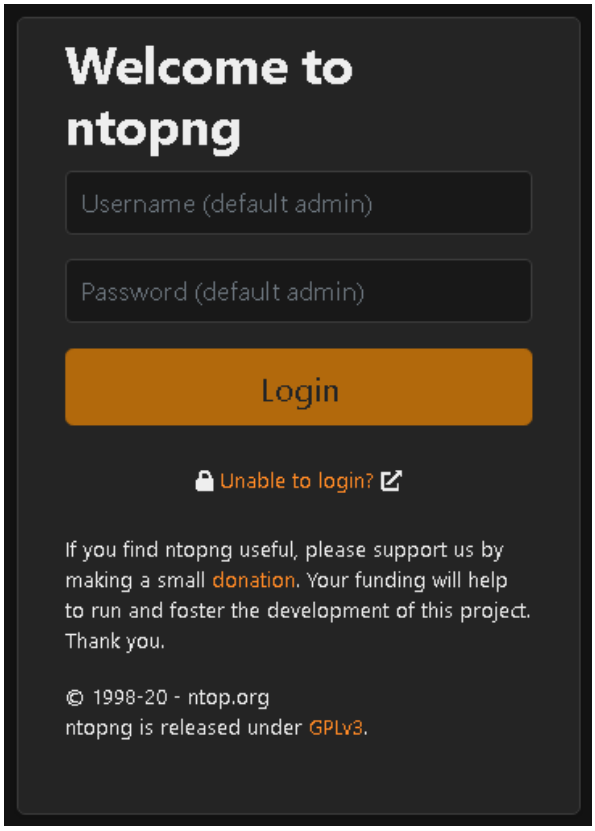

Figura 4.6: Login para *ntopng*

4.1.2. TCPDUMP

Es una herramienta para línea de comandos, la cual se usa para analizar el tráfico de red. TCPDUMP despliega una descripción del contenido de los paquetes; también permite exportar la información a un archivo para analizarlo en otro momento. Funciona en sistemas operativos UNIX, Linux, Solaris, BSD, Windows, entre otros. Utiliza la biblioteca libpcap para capturar los paquetes. Para utilizar tcpdump es necesario tener privilegios de administrador (root).

Ya que pfSense está basado en FreeBSD, esta herramienta ya se encuentra instalada, véase Figura 4.7.

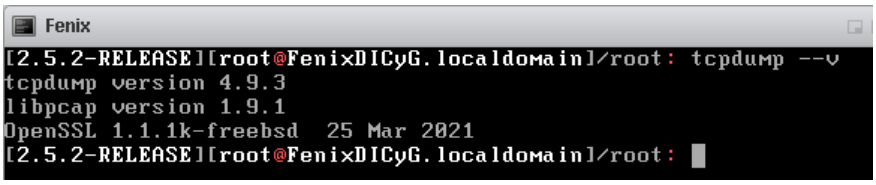

Figura 4.7: Versión de tcpdump y libpacp

4.2. Puesta en marcha del portal WEB

Una vez instalado el sistema operativo, se procedió a instalar Apache, PHP y MySQL, esto para poner en marcha el portal web del Laboratorio de Geomática y Especialidades de Civiles(LGyEC). Se instaló apache, y con ayuda de ufw[3] se configuraron los puertos que necesita apache para su funcionamiento, véase Figura 4.8.

[3]ufw (Uncomplicated Firewall) es una herramienta de configuración de cortafuegos que se ejecuta en la parte superior de iptables, incluidos por defecto dentro de distribuciones de Ubuntu. Proporciona una interfaz optimizada para configurar casos de uso de firewall comunes a través de la línea de comandos.

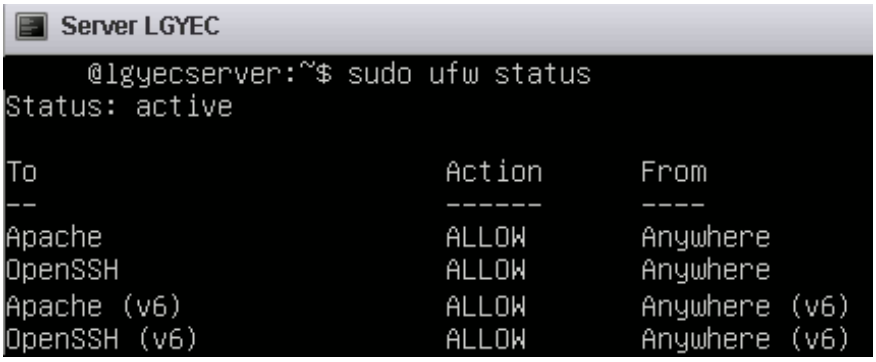

Figura 4.8: Estatus de ufw

Para cargar los archivos necesarios en el directorio **/var/www/html** por medio de SFTP(Protocolo de transferencia de archivos SSH), se asignaron los permisos necesarios al usuario encargado de esa tarea, véase Figura 4.9.

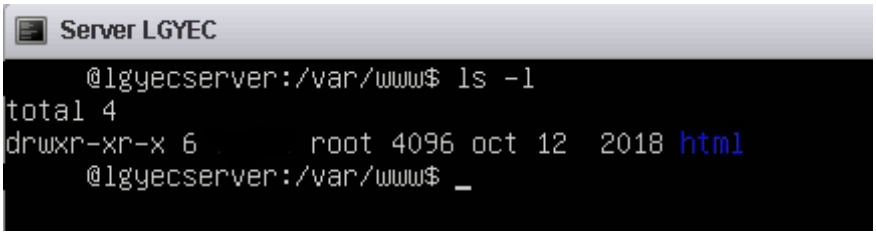

Figura 4.9: Permisos al usuario encargado

Se instaló **MySQL** y el complemento ***mysql_secure***, se ingresó la contraseña para el usuario root. Al final se comprobó la versión de MySQL y el estado del servicio, véase Figura 4.10 y Figura 4.11.

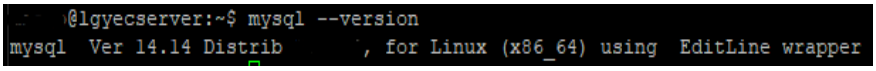

Figura 4.10: Versión de mysql

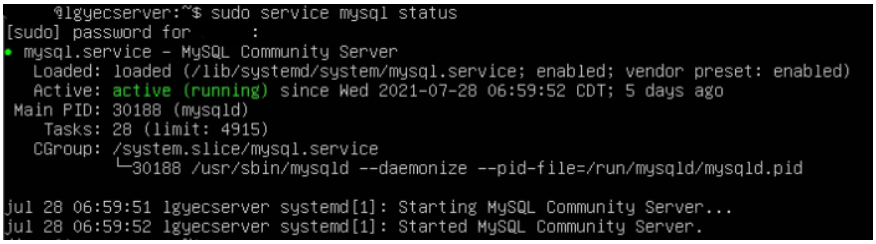

Figura 4.11: Estado de mysql

Como paso siguiente se instaló **PHP** (véase Figura 4.12) y **phpMyAdmin**, con ayuda de este último se configuró y creó la base de datos con credenciales proporcionadas por el superadministrador.

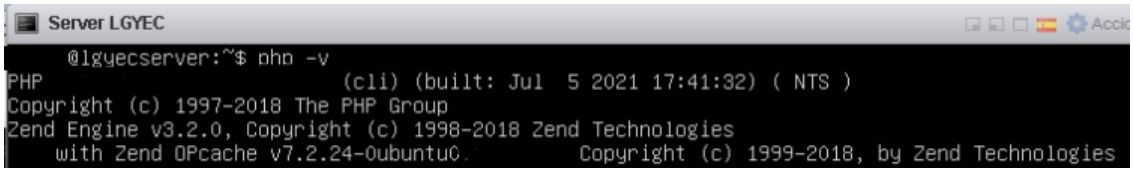

Figura 4.12: Versión de php

Al finalizar las configuraciones se cargó la primera versión de la página del Laboratorio, véase Figura 4.13.

Figura 4.13: Página principal del LGyEC

4.2.1. Accesos y Seguridad

Como se vio en el capítulo anterior se crearon los tres usuarios adicionales, dos para el equipo de Unidad de Cómputo y el responsable del Laboratorio. Estos usuarios se agregaron al archivo *sudoers*, para que tengan los permisos necesarios. Para cada usuario se agregó un *script* en *bash*, el cual se ejecutará en cada inicio de sesión. Se guardará un archivo con el siguiente formato **nombreusuariofecha.log** en la ruta del administrador.

Para las conexiones SSH se pidió a cada usuario generar las claves en sus equipos que destinarán para la conexión, ya que las conexiones SSH solo serán mediante claves públicas, las cuales se copiaran en cada uno de los usuarios en el directorio ***known_hosts***. Y en el archivo config se comentó la línea que permite las conexiones mediante usuario y contraseña.

Para aumentar la seguridad en conexiones a la página de laboratorio, se decidió implementar una conexión segura mediante TLS con ayuda de la Autoridad Certificadora *Let's Encript*[4] y el cliente ACME *Cerbot*[5].

Los requerimientos para poder usar *Cerbot* (véase Figura 4.14)son los siguientes:

- Sitio web HTTP
- Conexión SSH
- Permisos sudo o administrador
- Contar con un dominio válido
- Puerto HTTPS abierto

Para la instalación se siguieron los pasos detallados en la página https://certbot.eff.org/ , en la cual se ingresa el software y sistema operativo que se esté utilizando.

[4]https://letsencrypt.org/es/

[5]Es una herramienta de software de código abierto y gratuita para usar automáticamente certificados *Let's Encrypt* en sitios web administrados manualmente para habilitar HTTPS.

Figura 4.14: Página de *cerbot*

Estos certificados tienen validez por tres meses, CERBOT los renueva automáticamente faltando un mes para que expiren. Para garantizar la renovación, se programó el cron con el usuario administrador. Para programar la renovación, se agregó la siguiente línea **00 23 20 * * /usr/bin/cerbot renew --quiet --post-hook "service apache2 restart"**.

4.2.2. Servicios

Además de ejecutar la página WEB del LGyEC, el servidor también puede implementar bases de datos remotas con las configuraciones adecuadas, ya que actualmente funciona de manera local. Gracias a que el servidor tiene configurado SAMBA cada usuario conectado a la red puede tener acceso a almacenamiento e impresoras, sin necesidad de tener estos servicios de manera individual o física.

4.3. Pruebas

Pruebas VLAN

Todas las pruebas realizadas fueron en tiempos de emergencia sanitaria por lo que no se pudieron crear escenarios óptimos o configuraciones que pudiendo asistir de manera presencial se hubieran realizado, es por eso que las pruebas presentadas en el presente trabajo tuvieron limitaciones de trabajo a distancia.

Se procedió a verificar la asignación de IP's de manera automática, así como la velocidad en cada una de las VLAN creadas, véase de la Figura 4.15 a la Figura 4.19.

Figura 4.15: Asignación de IP y velocidad de internet VLAN 10

Figura 4.16: Asignación de IP y velocidad de internet VLAN 20

Figura 4.17: Asignación de IP y velocidad de internet VLAN 30

Figura 4.18: Asignación de IP y velocidad de internet VLAN 40

Figura 4.19: Asignación de IP y velocidad de internet VLAN 1000

En el apartado ***Status / DHCP Leases*** se visualiza la dirección IP, MAC, *Hostname*, estado de conexión de cada uno de los equipos del LGyEC. En las VLAN se puede visualizar el rango de IP's y el número de equipos, véase Figura 4.20.

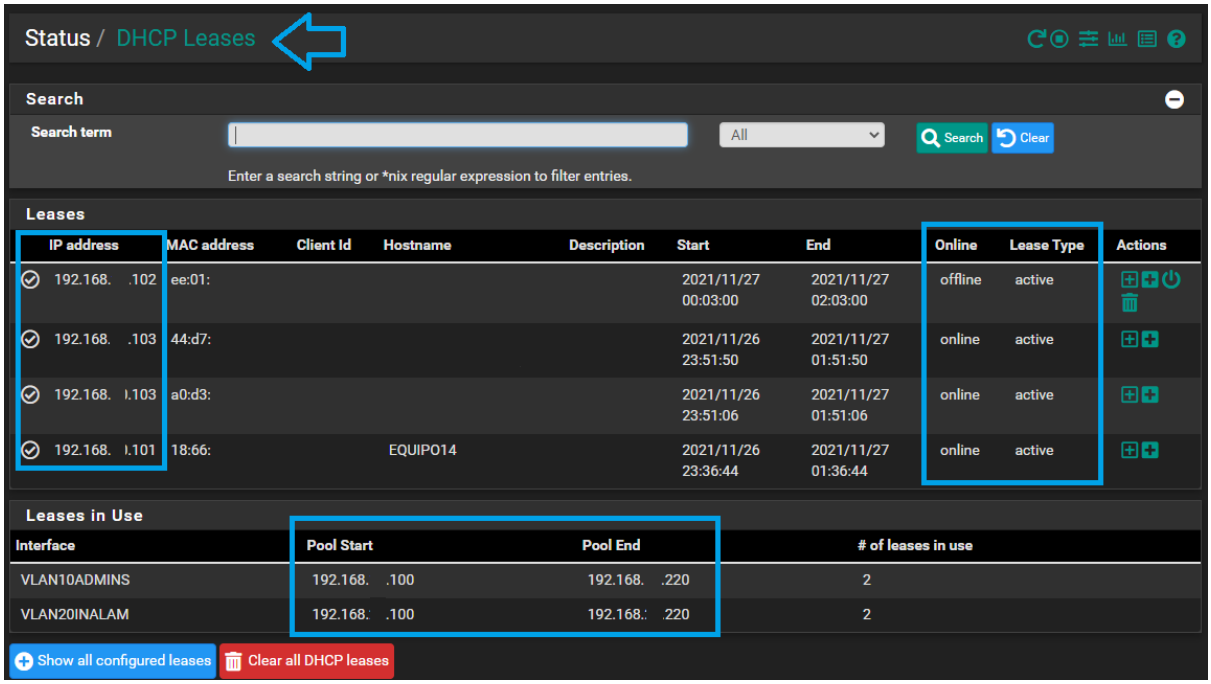

Figura 4.20: DHCP *Leases*

Pruebas VPN

Al instalar el cliente OpenVPN se abrió la interfaz de usuario para conectarse a la VLAN 1000, desde el icono que se encuentra en la parte inferior derecha del escritorio de Windows, véase de la Figura 4.21 a la Figura 4.24.

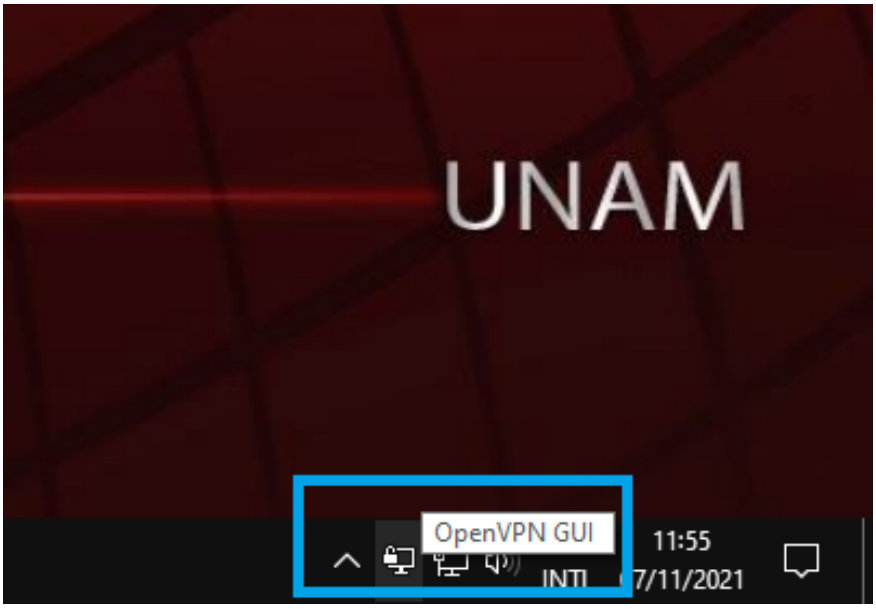

Figura 4.21: Icono OpenVPN

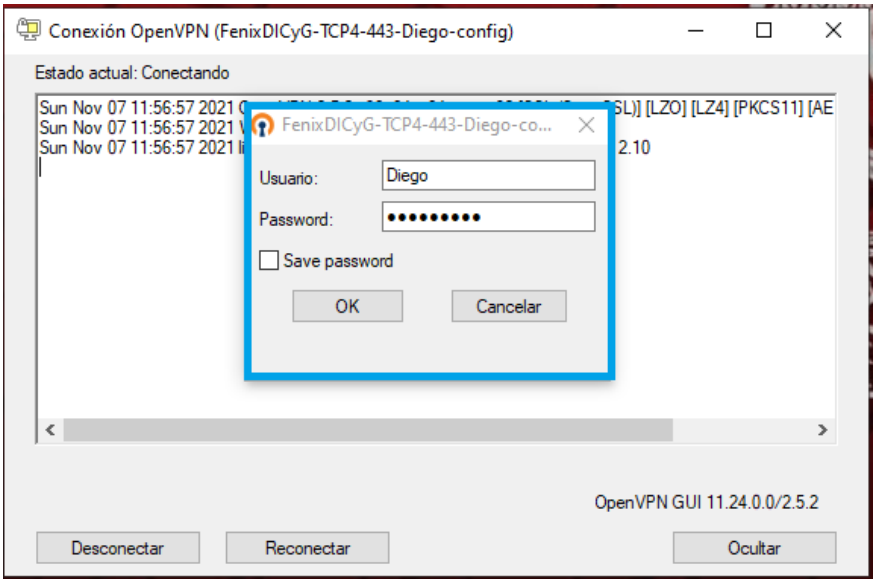

Figura 4.22: Login OpenVPN

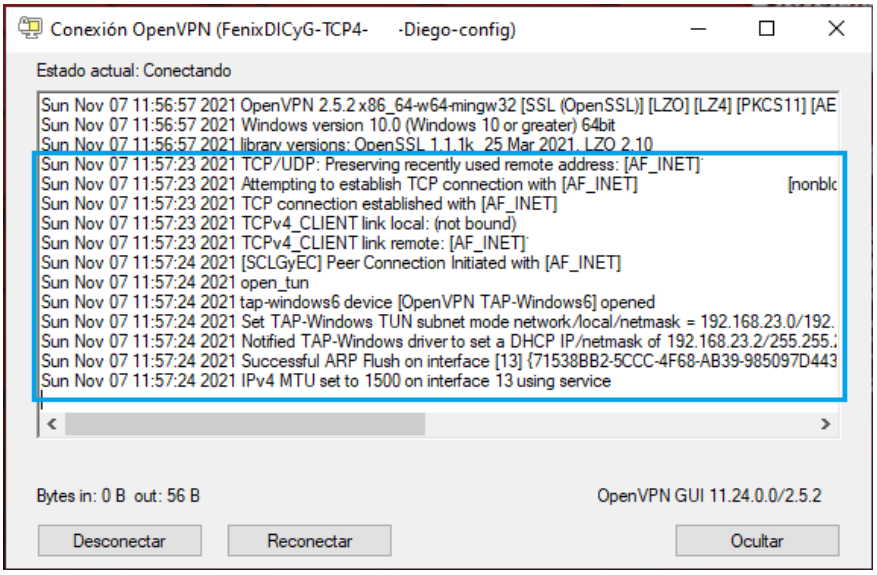

Figura 4.23: Estado de conexión VPN

Figura 4.24: Equipo conectado a VPN

Por último se verificó el acceso a las IP locales de “ESXi, Página Web, NTOPNG y pfSense”, véase de la Figura 4.25a la Figura 4.28.

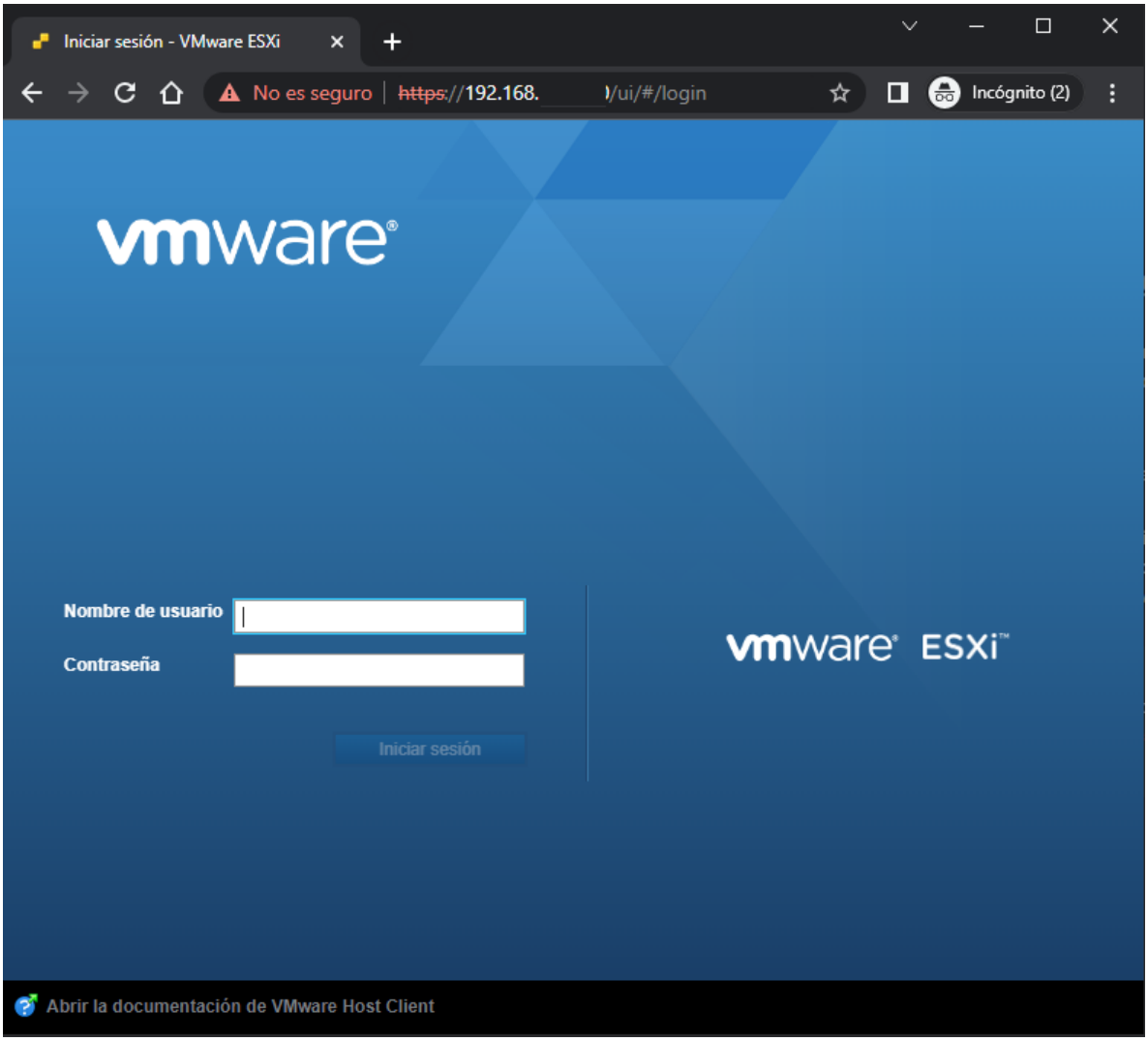

Figura 4.25: Conexión a ESXi

Figura 4.26: Conexión a página web

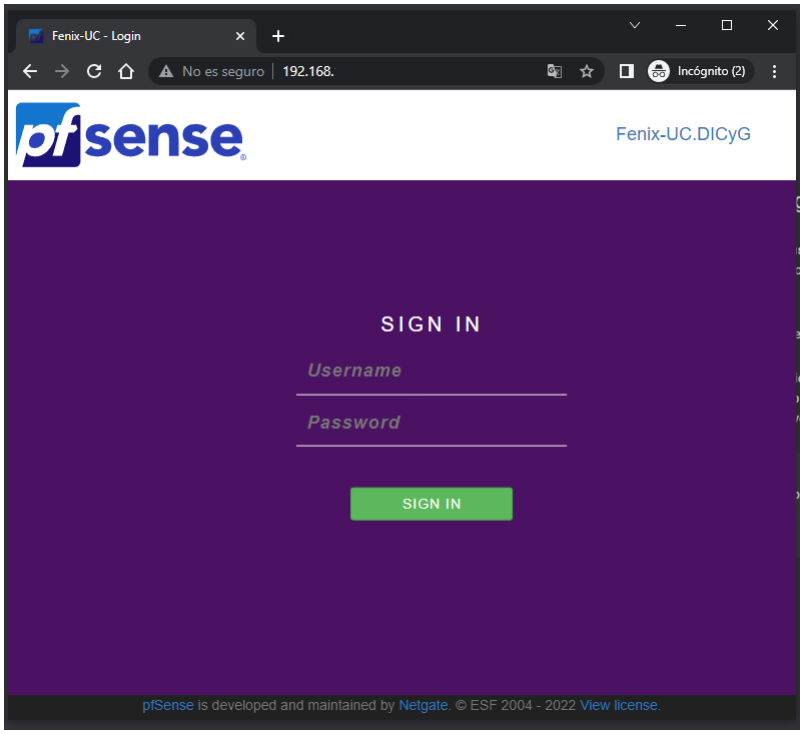

Figura 4.27: Conexión pfSense

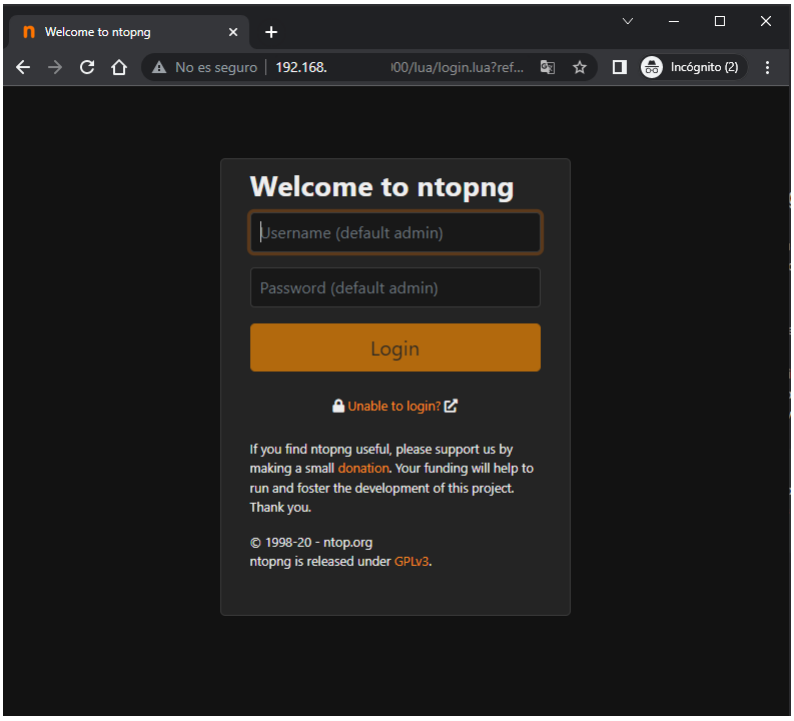

Figura 4.28: Conexión NTOPNG

Pruebas NTOPNG

En este caso se conectaron equipos a las VLAN 20, 30 y 40. Esto para verificar el monitoreo de equipos en estas VLAN. Cabe mencionar que estas pruebas se realizaron de manera extraordinaria, ya que por motivos de la ausencia docente no se refleja el uso ordinario del servicio de internet, como se comentó anteriormente, por motivos de la emergencia sanitaria no se podía asistir presencialmente al Laboratorio de Geomática y Especialidades de Civiles.

La herramienta muestra la dirección IP, el tamaño total de bytes enviados, el tiempo que tiene ese equipo en red, el total de bytes, el nombre del equipo, dirección MAC, entre otros detalles de red, véase de la Figura 4.29 a la Figura 4.31.

Figura 4.29: VLAN 20 loal *hosts*

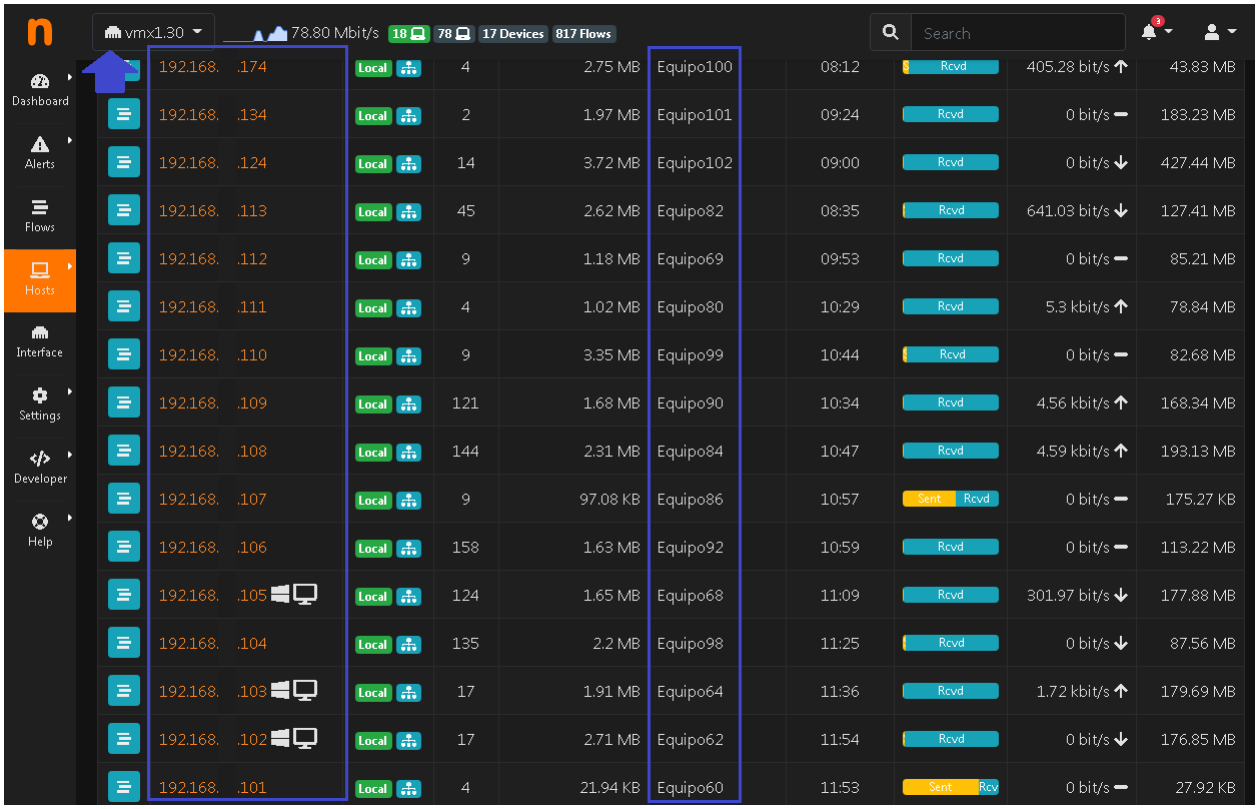

Figura 4.30: VLAN 20 MAC *list*

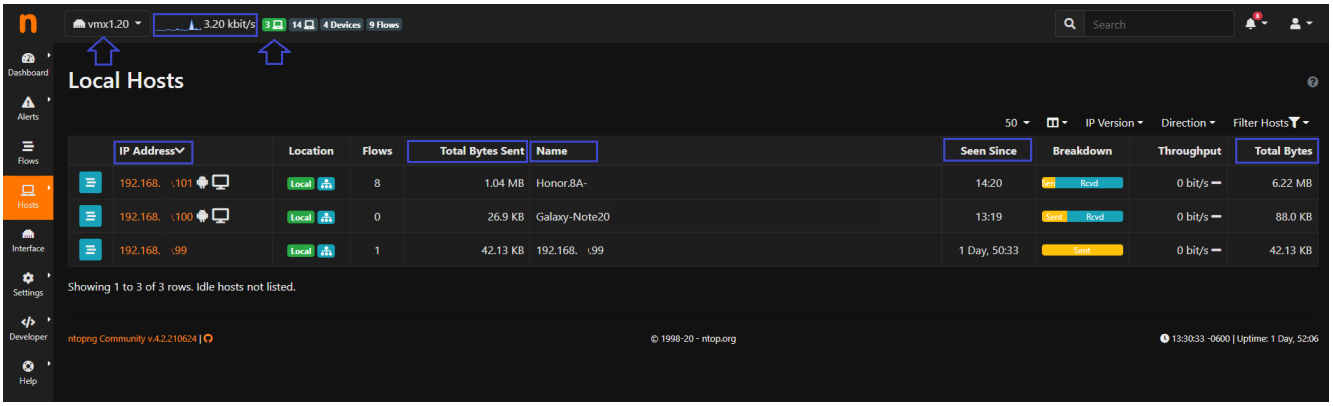

Figura 4.31: VLAN 20 *Active Flows*

4.4. Programa de mantenimiento

El propósito del mantenimiento,es prevenir fallos en el equipo e infraestructura de los Laboratorios de Geomática y Especialidades de Civiles(LGyEC), con la finalidad de proporcionar servicios estables y confiables al personal académico, docente y estudiantil. El mantenimiento será realizado únicamente por personal de la Unidad de Cómputo de la DICyG, los cuales deberán estar debidamente identificados para tener acceso al site.

Mantenimiento preventivo de Hardware

Se recomienda realizar las siguientes actividades cada seis meses:

1. Limpieza Física de Switches y Servidor.
2. Limpieza Física del Quadrarack.
3. Verificación de temperatura y estado del aire acondicionado. En caso de que el equipo de clima artificial opere inadecuadamente contactar con el personal calificado para su mantenimiento[6].
4. Verificar el funcionamiento y estado del cableado horizontal.
5. Verificar el estado de los nodos de red.
6. Verificar el estado del sistema de alimentación ininterrumpida.
7. Verificación de temperatura de procesador(es) del servidor[7].

Se recomienda realizar la siguiente actividad cada dos años:

- Cambio de pasta térmica del procesador o procesadores.

Mantenimiento preventivo de Software

Se recomienda realizar las siguientes actividades cada tres meses:

1. Verificar el estado del almacenamiento en el servidor.
2. Mantener actualizado el sistema operativo del hypervisor, servidor web y *firewall*.
3. Verificar y actualizar cuando existan cambios mayores de software(mysql, apache, php, openvpn-client-export, ntopng).
4. Verificar el rendimiento de las máquinas virtuales.

Para el punto 3 y 4 es conveniente instalar un sistema de monitoreo automático como NAGIOS, Pandora FMS, OP5, Zenoss Core, Zabbix, OpenNMS, PRTG, entre otros , sin embargo, para el alcance de este proyecto no se tiene considerado, pero se puede recomendar para trabajos a futuro.

Se recomienda realizar las siguientes actividades cada seis meses:

[6]Se recomienda verificar que la temperatura del clima artificial esté en el margen de 18 °C a 24 °C
[7]Se recomienda verificar que la temperatura esté en el margen de 10 °C a 35 °C.

- Realizar respaldos de las Máquinas Virtuales.
- Realizar respaldo de configuración de *Firewall*.

Capítulo 5 Manual de operaciones

Capítulo 5

Manual de operaciones

El objetivo de este capítulo es poder generar la información suficiente para que el o los administradores presentes y futuros para el LGyEC puedan contar con las herramientas necesarias para el mantenimiento de dichos laboratorios, por medio de un documento confiable y a la medida.

5.1. Manual de Administrador

El equipo de red se conectó como se muestra en la Figura 5.1 y el detalle en la Tabla 5.1.

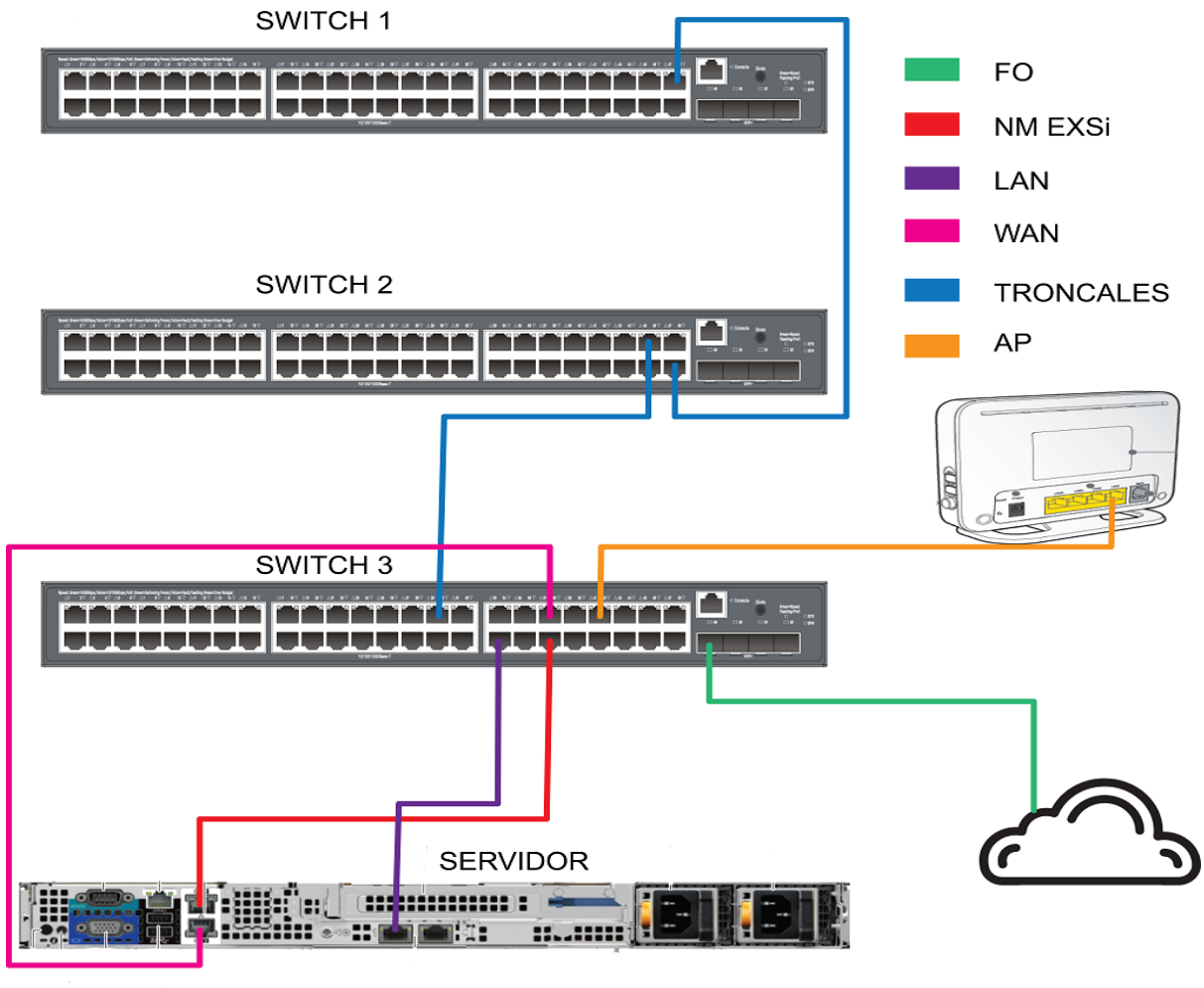

Figura 5.1: Conexiones Físicas del equipo de red

Tabla 5.1: Detalle de conexiones en el servidor

Abreviación	Detalle
FO	Conexión de Fibra Óptica
NM EXSi	Interfaz para la administrración de ESXi
LAN	Interfaz para LAN + VLAN's
WAN	Interfaz para WAN
TRONCALES	Conexión entre switches
AP	Conexión para *Acces Point*

Estas conexiones son las adecuadas y únicas para la configuración existente del equipo de red, ya que, cada puerto de los switch cuenta con la estructura lógica necesaria para el correcto funcionamiento.

Al realizar la instalación de ESXi, se asignó de manera automática las configuraciones de la NIC de VMkernel, véase Figura 5.2.

Figura 5.2: Especificaciones de NIC VMkernel

Las interfaces de red que se utilizaron para las conexiones de la WAN, LAN y *Management Network* fueron wmnic0, vmnic1 y vmnic3, véase Figura 5.3.

Figura 5.3: Interfaces físicas en ESXi

Se tienen tres grupos de puertos y tres switches virtuales, estos se encuentran asignados a cada una de las interfaces físicas de ESXi, véase de la Figura 5.4 a la Figura 5.6.

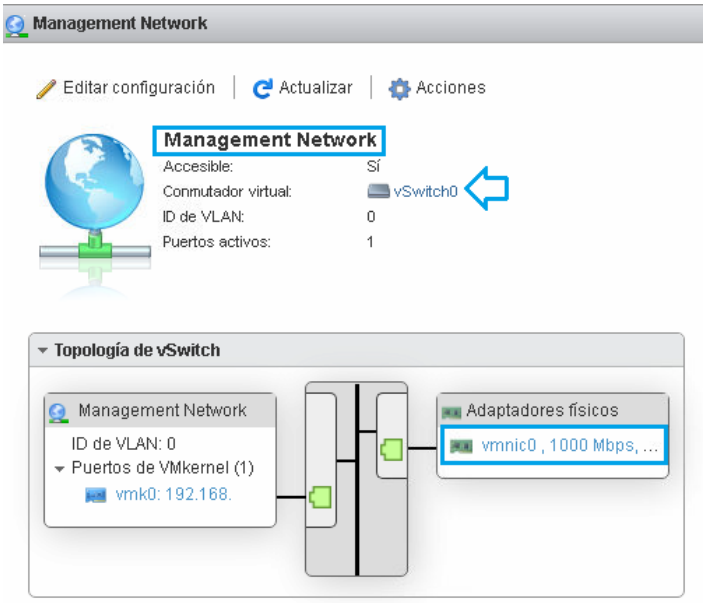

Figura 5.4: Grupo de puertos y *switch Management Network*

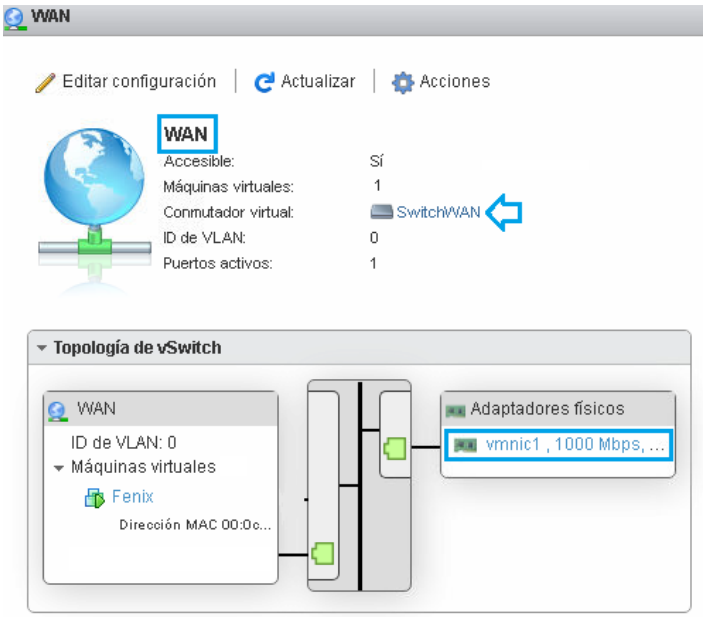

Figura 5.5: Grupo de puertos y *switch* WAN

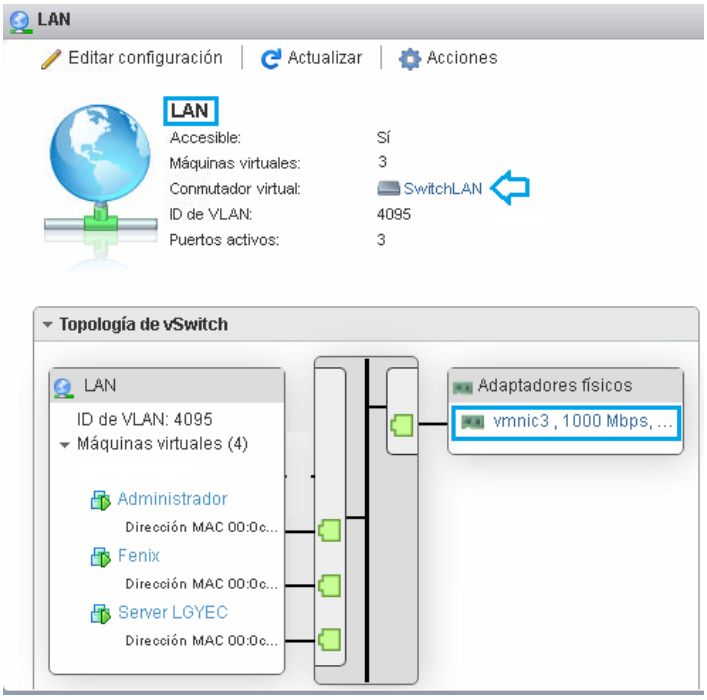

Figura 5.6: Grupo de puertos y *switch* LAN

5.2. Esquema general de red

Al finalizar las configuraciones de la red se obtuvo el siguiente diagrama lógico(véase Figura 5.7).

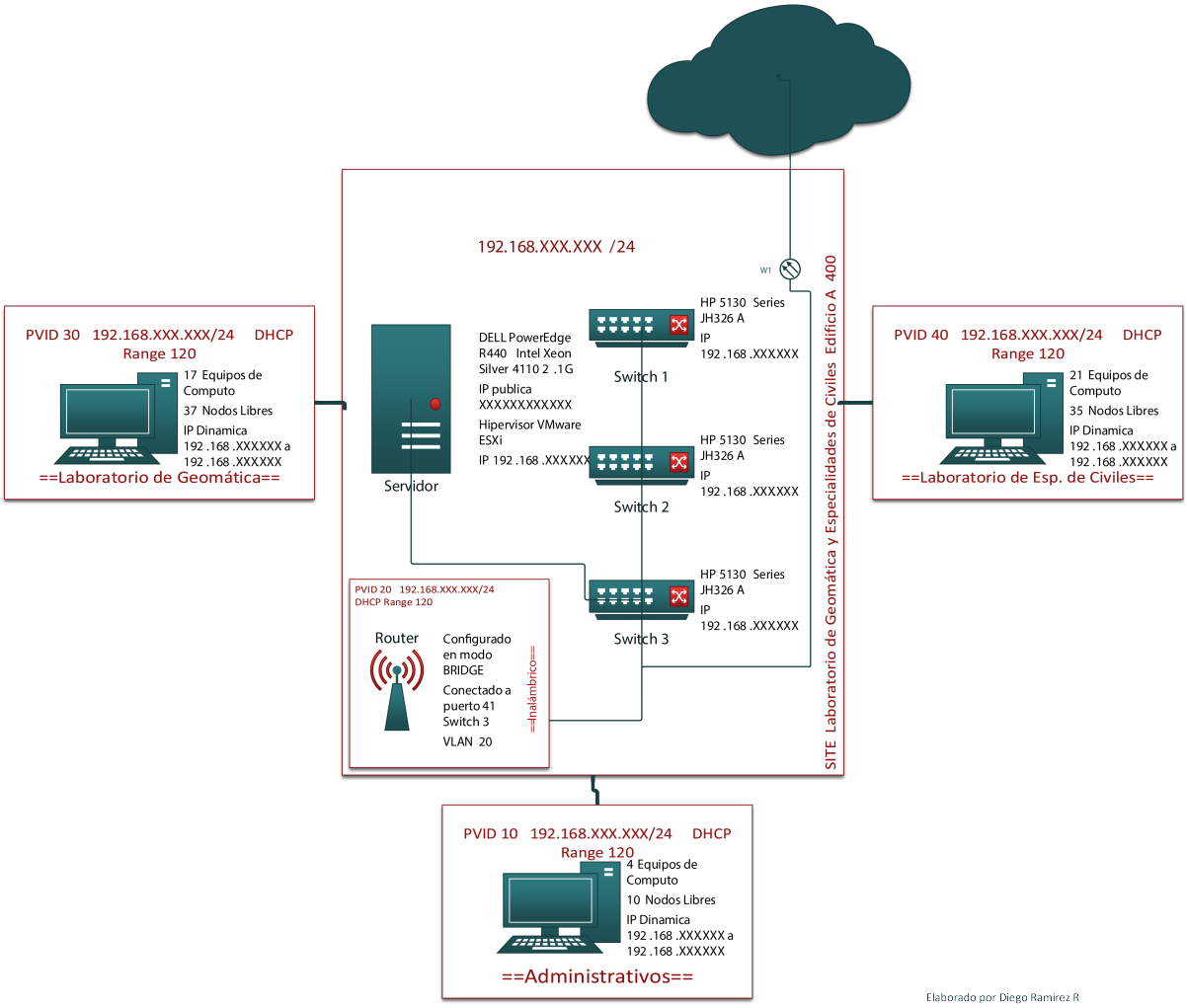

Figura 5.7: Diagrama de red lógico del LGyEC

Conclusiones

Conclusiones

Con la puesta en marcha del servidor de los Laboratorios de Geomática y Especialidades de Civiles(LGyEC) se adquirió seguridad, administración, disponibilidad de servicios y herramientas de control de red. Ofreciendo un servicio de calidad para toda la matrícula docente que utilice los laboratorios pertenecientes a la División de Ingenierías Civil y Geomática(DICyG), aprovechando el área de oportunidad que dejó el sismo ocurrido el 19 de septiembre del 2017.

Gracias a la implementación de servidores virtuales, se gestionaron de mejor manera los recursos de hardware con los que se cuenta, instalando las herramientas necesarias para los servicios requeridos. Por lo que el site cuenta con la posibilidad de escalar sus servicios y/o aplicativos sin ningún inconveniente, así como el aumento de recursos de hardware. Con la implementación de pfSense, se obtuvo una herramienta ágil, segura, confiable y robusta, para poder segmentar y administrar la red, monitorear el consumo de ancho de banda, protección a los equipos de cada área de trabajo y la administración remota de todos los servicios. Al contar con esta herramienta configurada a medida, se pudo notar que tiene la capacidad de instalar paquetes que podremos utilizar en el momento que se necesite, otorgando una alta escalabilidad en sus componentes. Se logró incrementar el ancho de banda pasando de 10 Mb a 270Mb, así como el redireccionamiento del servidor web del laboratorio. Mediante la implementación de VLAN se pudo segmentar la red por cada área de trabajo, encapsulando cada una de ellas para tener independencia lógica e incrementar la seguridad, el monitoreo también se dividió en cada una de las VLAN creadas, se obtuvo el control total de los equipos de red y VLAN's de manera remota.

El laboratorio LGyEC cuenta con todos los estándares en la infraestructura, así como con las herramientas necesarias para proporcionar servicios que satisfagan las necesidades de los usuarios. La administración por parte de la Unidad de Cómputo de la DICyG, contará con un manual de operaciones con las actividades necesarias para mantener y mejorar los servicios prestados por el site.

En este ámbito el laboratorio está listo para una posible solicitud al Sistema de Gestion de la Calidad(SGC), pero se podría solicitar el reconocimiento 'Calidad UNAM' que es una opción para todos aquellos laboratorios que cuenten con un sistema de gestión evaluado, sin la necesidad de que un tercero solicite su certificación. En este punto el responsable del laboratorio y los departamentos involucrados tendrán la labor de realizar los documentos necesarios para que el laboratorio tenga todos los requisitos necesarios para la solicitud de SGC.

Este proyecto fue un reto personal y profesional, ya que se desconocía el manejo de estas herramientas. Gracias a esto, se pudo reforzar el trabajo de investigación a fondo y el trabajo autodidacta. Se consolidaron los conocimientos teóricos adquiridos durante la carrera, implementándolos en un caso práctico adquiriendo experiencia para determinar la mejor solución a algún problema, sin dejar de lado el objetivo principal.

Glosario

Glosario

AC: Es una empresa u organización confiable que valida las identidades de personas o entidades y vincularlas mediante la emisión de certificados digitales.

AES: Acrónimo del inglés Advanced Encryption Standard es un algoritmo de cifrado por bloques, por lo que implementa bloques de entrada de 128 bits de longitud y puede utilizar claves de 128, 192 o 256 bits de ahí las variantes AES-128, AES-192 o AES-256.

Criptografía: Técnicas utilizadas para ocultar la información implementando técnicas matemáticas, para que el intercambio sea entre los actores involucrados.

Certificados Digitales: Son documentos digitales únicos que garantizan la vinculación de una persona o entidad con una clave pública, contiene información del propietario y su clave; así como información del certificado como lo es: periodo de validez, número de serie único, nombre de la AC que lo emitió, entre otros datos.

CCTV: Un circuito cerrado de televisión es una instalación de equipos 25.

Dieléctrico: Se refiere a la propiedad o efecto de alternar campos eléctricos en algún material.

DHCP: Acrónimo del inglés Dynamic Host Configuration Protocol, se encarga de asignar de manera dinámica y automática una dirección IP. Esta información se guarda en un archivo con la relación de IP y la dirección MAC, con esto el DHCP se asegura que la asignación de IP no se duplique.

DNS: Acrónimo del inglés Domain Name System es el encargado de organizar a los equipos en dominios y resolver nombres de host en direcciones IP.

FTP: Acrónimo del inglés File Transfer Protocol, permite transferir archivos de un dispositivo a otro.

FTPS: Acrónimo del inglés File Transfer Protocol, es un protocolo seguro para la trasferencia de archivos de un dispositivo a otro.

Gateway: También conocido como puerta de enlace, su función es establecer la comunicación entre equipos.

ISP: Es la empresa o proveedor del servicio de conexión a Internet.

IDS: Es una aplicación usa para detectar accesos no autorizados o permitidos de un equipo a una red, monitorea el trafico entrante y lo coteja con una base de datos actualizada de firmas de ataques conocidos. Ante cualquier amenaza, emite una alerta.

IPS: Es un software que se utiliza para proteger a una red y sus componentes de ataques e intrusiones.

IMAP: Del inglés Internet Message Acces Protocol, es el principal protocolo que se utiliza para la entrega de correos electrónicos. Para implementar IMAP, el servidor de correos debe ejecutar este protocolo por el puerto 143.

MAC: Es la dirección física de la tarjeta de red, es un identificador único que se asigna a cada interfaz de red.

Máscara de Subred: Es una dirección que enmascara la dirección IP, determina si otra dirección IP pertenece o no a la misma subred.

Máquina Virtual: En esencia es un conjunto de archivos que se ejecutan en un hipervisor y se comportan como un equipo de cómputo físico.

NAT: Del acrónimo del inglés Network Address Translator, se encarga de traducir las direcciones para que sea posible la comunicación entre una red privada y el internet.

NFS: Network File System, permite almacenar y actualizar archivos en un equipo remoto como si estuviera en el equipo. Permite montar una porción de un sistema de archivos en un servidor, la cual puede brindarle acceso a los usuarios.

OpenBSD: Considerado como el sistema operativo de propósito general más seguro, está basado en NetBSD.

POP: Del inglés Post Office Protocol, sirve para sincronizar un servidor de correo electrónico con un cliente de correo compatible con la finalidad de gestionar el envió de correos electrónicos.

SITE: Su traducción al español es sitio, pero también es conocido como cuarto de telecomunicaciones.

SSL: De su acrónimo del inglés Secure Sockets Layer, proporciona un canal seguro entre dos dispositivos como, por ejemplo: un navegador y un servidor web.

SMTP: Acrónimo del inglés Simple Mail Transfer Protocol, es un protocolo que acepta conexiones sujetas a verificaciones de seguridad, además acepta mensajes para su entrega. En caso que no se pueda entregar un mensaje, se envía al emisor un informe de error que contiene la primera parte del mensaje que no se puedo entregar.

SCP: Del inglés Secure Copy Protocol, es un protocolo de transferencia de archivos en la red de manera segura, o entre dos ubicaciones remotas.

SMB: Acrónimo de Server Message Block, protocolo que se emplea para el acceso a archivos y directorios, así como a otros recursos de red.

TI: Acrónimo de Tecnología de la Información.

TOKEN: Pequeño mensaje, puede ser utilizado para otorgar permisos.

TAGGED: Se nombra tagged a un puerto en modo truck donde se le puede indicar el paso de una o varias VLANs.

TLS: Acrónimo del inglés Transport Layer Security, está basado en SSL (Secure Sockets Layer) que significa capa de conexiones seguras. Es un protocolo que hace uso de certificados digitales para que la comunicación sea segura a través de internet.

UNTAGGED: Se nombra untagged a un puerto configurado en modo acceso, por lo que solo puede dejar pasar una VLAN.

UPS: Del ingél Uninterruptible Power Supply, es un dispositivo que puede proporcionar energía eléctrica a equipos de operación critica gracias a que cuenta con baterías y elementos de almacenamiento de energía.

HTTP: Del inglés Hyper Text Transfer Protocol, es un protocolo para la trasmisión de documentos hipermedia, como lo es HTML. Fue creado para la comunicación entre navegadores y servidores web.

HTTPS: Del inglés Hyper Text Trasnfer Protocol Secure, es una actualización del HTTP ya que utiliza seguridad en ambos extremos para que la información se traslade de manera segura, esto mediante el uso de SSL y el puerto 433.

HTML: Acrónimo del inglés Hyper Text Markup Language, es un componente básico de la WEB se utiliza para estructurare y desplegar una página con su contenido.

Referencias

Referencias

1. Data Técnica. (2018). Diagrama de conexion cable de RED UTP conector RJ-45. Junio 20, 2022, de Utiltecnico Sitio web: http://www.utiltecnico.com/diagrama-como-conectar-cable-de-red-utp-conector-rj-45/
2. Eduardo Infante. (2014). Microondas terrestres. Abril 14, 2021, de Personal Sitio web: https://sites.google.com/site/comin14 transmision-no-guiados/microondas-terrestres
3. Guimi. (2009). 1.3 CABLE COAXIAL. Mayo 09, 2020, de Guimi Sitio web: https://guimi.net/monograficos/G-Cableado_estructurado/G-CEnode5.html
4. ISO. (2018). Normas ISO. Abril 12, 2020, de ISO Sitio web: https://www.certificadoiso9001.com/que-es-iso/
5. IEEE.Acerca de e HIstoria. Abril 12, 2020, de IEEE Sitio web: http://www.ieee.org.mx/index.html
6. J. Postel. (1980). Protocolo de Datagramas de Usuario. Marzo 03, 2020, de ISI Sitio web: https://www.rfc-es.org/rfc/rfc0768-es.txt
7. Know How. (2019). File server: definición y aspectos básicos. Marzo 09, 2020, de IONOS by 1&1 Sitio web: https://www.ionos.mx/digitalguide/servidores/know-how/file-server/
8. Know How. (2019). Qué es un servidor?. Marzo 10, 2020, de IONOS by 1&1 Sitio web: https://www.ionos.mx/digitalguide/se how/que-es-un-servidor-un-concepto-dos-definiciones/
9. Kionetworks. (S/A). Conoce los tipos de VPN y sus protocolos. Junio 22, 2022, de Kionetworks Sitio web: https://www.kionetworks.com/blog/data-center/tipos-de-vpn-y-sus-protocolos
10. Pedro J. Ponce de León. (2002). Protocolo de Control de Transmisión. Abril 09, 2020, de Defense Advanced Research Projects Agency Sitio web: https://www.rfc-es.org/rfc/rfc0793-es.txt
11. Proyectos Wikimedia. (s.f.). Cableado estructurado. Abril 24, 2020, de Wikimedia Sitio web: https://es.wikipedia.org/wiki/C
12. PROMAX TEST & MEASUREMENT. (Septiembre 26, 2019). Tipos de conectores de fibra óptica: Guía sencilla. Mayo 24, 2020, de PROMAX TEST & MEASUREMENT Sitio web: https://www.promax.es/esp/noticias/578/tipos-de-conectores-de-fibra-optica-guia-sencilla/#:~:text=Las %20siglas %20SC %2C %20LC %2C %20FC,l %C3 %A1ser %20entr
13. R. Braden. (1989). Requirements for Internet Hosts -- Communication Layers. Abril 10, 2020, de Internet Engineering Task Force Sitio web: https://tools.ietf.org/html/rfc1122\#section-4.2
14. Rouse. Margaret. (2010). Virtualización. Marzo 12, 2020, de TechTarget Sitio web: https://searchdatacenter.techtarget.com/
15. RFcell. (s.f.). TMW antennas. Abril 14, 2020, de RFcell Sitio web: http://www.rfcell.com/tmw-antennas
16. S.Tanenbaum, Andrew y J.Wetherall, David. (2012). Redes de computadoras. México: Pearson Educación.
17. Stalling, William. (2008). Comunicaciones y redes de computadores. México: Prentice Hall.
18. Vinton G. Cerf and Robert E. Kahn. (1974). A Protocol for Packet Network Intercommunication. Junio 17, 2022, de IEEE Sitio web: https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf

Referencias de Figuras

Referencias de Figuras

1.1. Modelo Cliente-Servidor - Autoría propia
1.2. Servidor de Correo - Autoría propia
1.3. Servidor Web - Autoría propia
1.4. Servidor de Archivos - Autoría propia
1.5. Herramientas para la virtualización
1.6. Topología Estrella - Autoría propia
1.7. Topología Bus - Autoría propia
1.8. Topología Árbol - Autoría propia
1.9. Topología Anillo - Autoría propia
1.10. Topología Malla - Autoría propia
1.11. Capas del modelo OSI - Autoría propia
1.12. Capas del modelo TCP/IP - Autoría propia
1.13. Datagrama de TCP - Autoría propia
1.14. Datagrama UDP - Autoría propia
1.15. Datagrama IP - Autoría propia
1.16. Vista seccionada de un cable coaxial - Guimi. (2009). 1.3 CABLE COAXIAL. Mayo 09, 2020, de Guimi Sitio web: https://guimi.net/monograficos/G-Cableado_estructurado/G-CEnode5.html
1.17. Cable UTP - Marketing. (2017). Diferencias entre los cables de par trenzado UTP, STP y FTP. Mayo 09, 2020, de telecocable Sitio web: https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374
1.18. Cable STP - Marketing. (2017). Diferencias entre los cables de par trenzado UTP, STP y FTP. Mayo 09, 2020, de telecocable Sitio web: https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374
1.19. Cable FTP- Marketing. (2017). Diferencias entre los cables de par trenzado UTP, STP y FTP. Mayo 09, 2020, de telecocable Sitio web: https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374
1.20. Elementos de la fibra óptica - S.Tanenbaum, Andrew y J.Wetherall, David. (2012). Redes de computadoras. México: Pearson Educación.
1.21. Conectores de fibra óptica- PROMAX TEST & MEASUREMENT. (Septiembre 26, 2019). Tipos de conectores de fibra óptica: Guía sencilla. Mayo 24, 2020, de PROMAX TEST & MEASUREMENT Sitio web: https://www.promax.es/esp/noticias/578/tipos-de-conectores-de-fibra-optica-guia-sencilla/#:~:text=Las%20siglas%20SC%2C
1.22. Propagación de baja y alta frecuencia - S.Tanenbaum, Andrew y J.Wetherall, David. (2012). Redes de computadoras. México: Pearson Educación.
1.23. Conexión extremo a extremo de microondas - Eduardo Infante. (2014). Microondas terrestres. Abril 14, 2021, de Personal Sitio web: https://sites.google.com/site/comin1415im/home/medios-transmision-no-guiados/microondas-terrestres
1.24. Antena repetidora de microondas - RFcell. (s.f.). TMW antennas. Abril 14, 2020, de RFcell Sitio web: http://www.rfcell.com/tmw-antennas
1.25. Subsistemas del Cableado Estructurado - Proyectos Wikimedia. (s.f.). Cableado estructurado. Abril 24, 2020, de Wikimedia Sitio web: https://es.wikipedia.org/wiki/Cableado_estructurado
1.26. (a) Cable Cruzado y (b) Directo - Data Técnica. (2018). Diagrama de conexion cable de RED UTP conector RJ-45. Junio 20, 2022, de Utiltecnico Sitio web: http://www.utiltecnico.com/diagrama-como-conectar-cable-de-red-utp-conector-rj-45/
2.1. Topología inicial de red - Autoría propia
2.2. Rack con equipo de red- Autoría propia
2.3. Cableado horizontal - Autoría propia
2.4. Detalle de cable UTP- Autoría propia
2.5. Switch NETGEAR - Autoría propia

2.6. Equipo de Cómputo - Autoría propia
3.1. Colocación de piso falso - Autoría propia
3.2. Detalle de cable UTP - Autoría propia
3.3. Tendido de cableado de red y electricidad - Autoría propia
3.4. Cableado horizontal - Autoría propia
3.5. Cableado horizontal dirección SITE - Autoría propia
3.6. Aire acondicionado - Autoría propia
3.7. Cuadra rack con todo el equipo de red - Autoría propia

Para las figuras 3.8 a la 3.102 se refieren a pantallas capturadas durante la instalación y configuración del servidor

Para las Figuras 4.1 a la 4.14 se refieren a pantallas capturadas durante la instalación y configuración de herramientas de monitoreo.

Para las Figuras 4.15 a la 4.31 se refieren a pantallas capturadas durante las pruevas.

Para las Figuras 5.1 a la 5.6 se refieren a pantallas capturadas de detalles de configuracion.

5.7. Diagrama de red lógico del LGyEC - Autoria propia