UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Rediseño de una red de un centro de cómputo de una institución de estudios superiores

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Ángel Abarca García

DIRECTOR DE TESIS

M.A. Víctor Damián Pinilla Morán

Ciudad Universitaria, Cd. Mx., 2019

Agradecimientos

A mis padres, por todo su apoyo, paciencia y todos los sacrificios hechos para que yo tenga una formación académica. Sin ellos nada de esto sería posible.

Al M.A. Víctor Damián Pinilla Morán por todo su apoyo, tiempo, paciencia y el seguimiento brindado en la dirección del presente proyecto.

Al Ing. Francisco López Mendieta por depositar su confianza y darme la designación que dio pie para el presente proyecto.

En lo académico a la Universidad y la Facultad de Ingeniería que fueron fundamentales para el desarrollo de mi conocimiento y habilidades.

A todas las personas que coincidieron conmigo y compartido diferentes vivencias.

Ángel Abarca Garcia

Índice de contenido

Introducción

Problema

El centro de cómputo tras su rehabilitación en la que incluyó una nueva infraestructura de red, se encontraron problemas que impedían el correcto funcionamiento de la red al crear un problema de disponibilidad y en consecuencia la reanudación de actividades sin los servicios de red, así como la negación del uso de los equipos de cómputo ya que estos emplean software de monitoreo por red.

La implementación de la nueva red para la rehabilitación del centro se realizó con falencias derivadas de la planeación al no seguir una metodología que garantice su correcto funcionamiento. Con lo anterior nace el presente proyecto para diagnosticar y analizar cuáles son los problemas existentes y con ello diseñar una solución viable.

Para el desarrollo se utiliza una metodología propuesta compuesta por tres fases: planear, construir y ejecutar.

Objetivo

Rediseñar la red del centro de cómputo con la finalidad de rehabilitar los servicios de red al tomar en cuenta la escalabilidad y adaptabilidad a futuro al seguir una metodología mixta propuesta en el presente proyecto.

Objetivos específicos

- Diseñar una metodología mixta a seguir para el diseño de una red.
- Aplicar la metodología propuesta.
- Validar el correcto funcionamiento de la red con el rediseño propuesto.

El documento se divide en 5 capítulos y un apéndice que son:

Capítulo 1: en el capítulo se describe al centro de cómputo y los eventos que fueron la causa de realizar una remodelación en la que se incluyó una nueva red, así como la problemática que se obtuvo al término de ésta.

Capítulo 2: se da un breve repaso a los fundamentos teóricos, se presentan equipos, topologías, protocolos y metodologías necesarias para la elaboración del proyecto. Se incluyen una nueva la metodología mixta a usar para resolver la problemática.

Capítulo 3: se desarrolla la propuesta del diseño para resolver los fallos presentes en la red de del centro de cómputo con la metodología propuesta para el presente proyecto.

Capítulo 4: se muestra la solución del desarrollo de la propuesta y se indican los cambios y las causas del porqué de los cambios.

Capítulo 5: se finaliza con las conclusiones del proyecto.

Apéndice A: se detalla el procedimiento referente a la simulación de la red al tener como base el diseño propuesto.

Capítulo 1. Descripción del centro de cómputo

La Facultad de Ingeniería está compuesta por diferentes departamentos y divisiones como lo son: dirección, consejo técnico, coordinación, administración, planeación y desarrollo, Divisiones entre otras como se puede ver en la figura 1-1. La institución posee múltiples programas académicos para la formación de los profesionistas, estas se encuentran agrupadas con programas afines en diferentes divisiones.

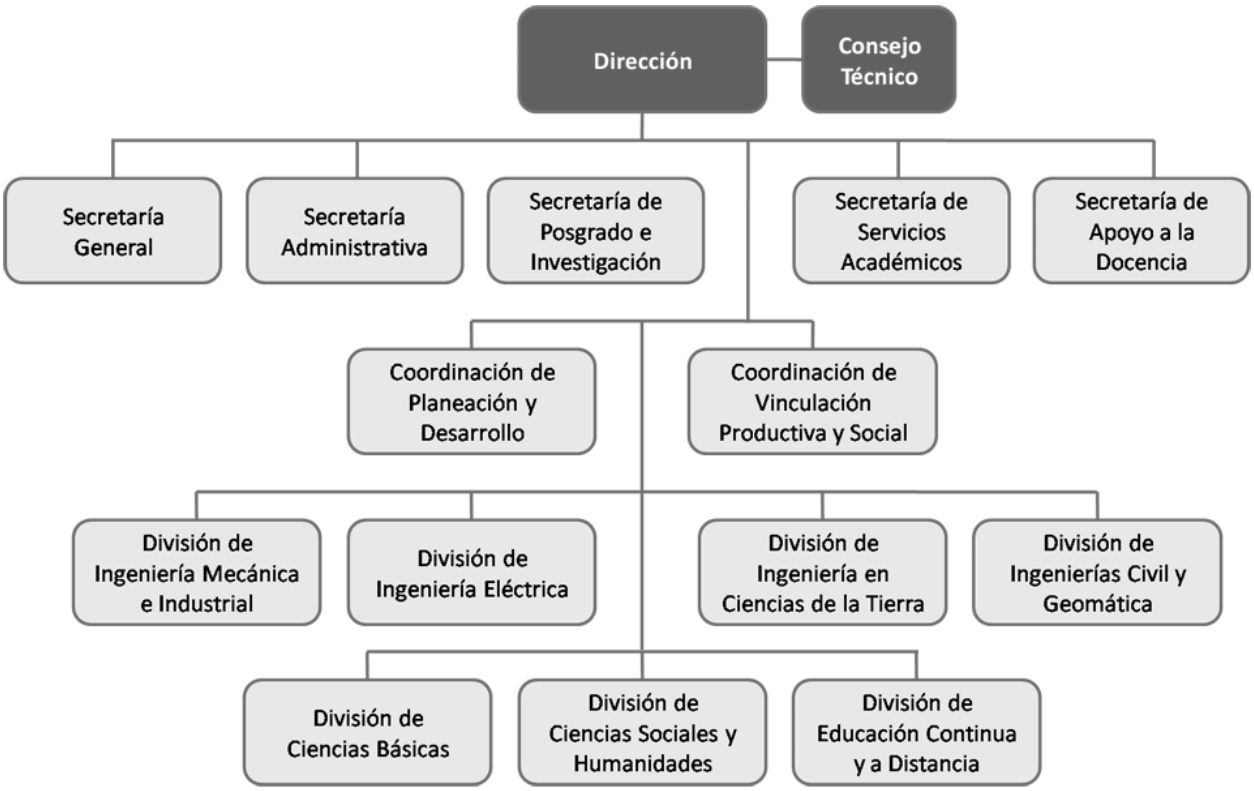


Figura 1-1 Organigrama de la institución (Facultad de Ingeniería, 2019)

La División de Ingenierías Civil y Geomática de la que depende el centro de cómputo está conformada por una jefatura, dos secretarías, seis coordinaciones, ocho departamentos y unidad de cómputo, estas se pueden apreciar en la figura 1-2.

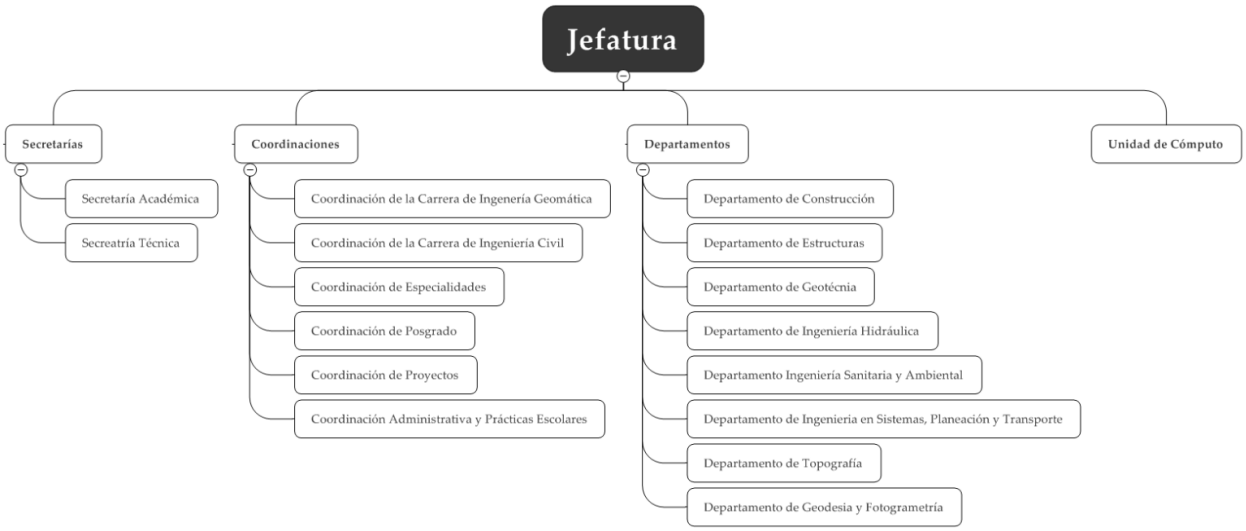


Figura 1-2 Organigrama de la división de Ingeniería Geomática y Civiles (Portal DICyG, 2019)

El centro de cómputo al ser parte de la división Ingenierías Civil y Geomática rinde cuentas a su jefatura como se muestra en la figura 1-3.

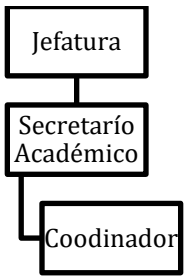


Figura 1-3 Organigrama del centro de cómputo (propia)

El centro de cómputo se encuentra dividido en dos laboratorios el Laboratorio de Geomática y el Laboratorio de Especialidades de Civiles.

1.1 Objetivos del centro de cómputo

Los objetivos de cada laboratorio pertenecientes al centro de cómputo se indican a continuación.

El objetivo principal del Laboratorio de Geomática es dar apoyo académico a los departamentos de cada área de Ingeniería para la comunicación en red interna, red externa e Internet mediante una serie de protocolos de servicios topológicos, en los que se complementan los conceptos

teóricos expuestos frente al grupo y prácticas de campo, para transferirlos a un software especializado.

Así mismo se apoya la realización de proyectos de investigación solicitados por la Facultad de Ingeniería, la iniciativa privada y el sector público. Con esta acción se consigue la participación de los alumnos en el final de sus estudios, que en algunos casos pueden emplear dichos proyectos como tema de tesis.

El objetivo principal del Laboratorio de Especialidades de Civiles es dar apoyo académico a los departamentos de la División de Ingenierías Civil y Geomática, Estructuras, Construcción, Geotecnia, Ingeniería de Sistemas y Planeación, Ingeniería Hidráulica, Ingeniería Sanitaria y Ambiental, para la comunicación en red interna, red externa e Internet, mediante una serie de protocolos de servicios topológicos, en los que se complementan los conceptos teóricos expuestos frente al grupo para transferirlos a un software especializado; apoyando así la realización de proyectos de investigación solicitados por la Facultad de Ingeniería, la iniciativa privada y el sector público para conseguir la participación de los alumnos en la etapa terminal, que en algunos casos pueden emplear dichos proyectos como tema de tesis.

1.2 Local del centro de cómputo

La ubicación del centro de cómputo es parte del nivel cuatro en el extremo sur del edificio “A” perteneciente a la institución y se compone por dos áreas laterales y una central (figura 1-4).

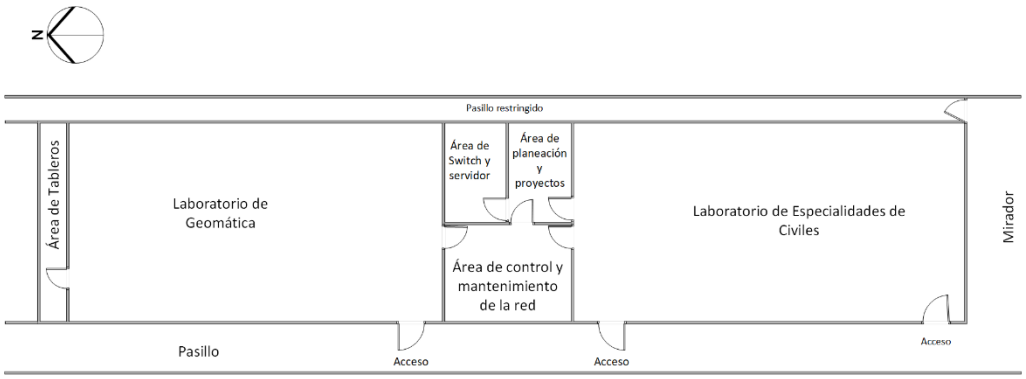


Figura 1-4 Distribución de áreas del centro de cómputo (propia)

El área lateral norte está dividida en dos partes:

- Laboratorio de Geomática de aproximadamente 120 m^2 donde laboran alumnos y profesores con capacidad hasta 52 usuarios conectados a la red, se tiene acceso desde el exterior.
- Área de tableros generales al fondo norte para el control de la energía general con acceso a través del Laboratorio de Geomática.

El área lateral sur Laboratorio de Especialidades de Civiles de aproximadamente 120 m^2 donde laboran alumnos y profesores con capacidad de hasta 54 usuarios conectados a la red, tiene dos accesos del exterior del centro de cómputo.

Un área central divide el centro de cómputo y está dividida en tres partes:

- Control y mantenimiento de la red del Centro donde laboran los encargados y los prestadores de servicio social, con dos accesos uno por el Laboratorio de especialidades de civiles y otro por el Laboratorio de Geomática.
- Planeación y proyectos donde labora el coordinador del centro de cómputo con dos accesos uno por el Laboratorio de especialidades de civiles y el otro a través de control y mantenimiento.
- Cuarto de telecomunicaciones denominado área de switch y servidor donde se ubica la entrada de servicios, el bastidor (rack), los conmutadores (switch), el servidor y la unidad de respaldo de energía. Se tiene acceso a esta área única y exclusivamente por el área de planeación y proyectos.

1.3 La red de cómputo

El centro de cómputo tuvo una actualización en su red que fue un elemento de la reparación coyuntural del laboratorio. Se busca: incrementar el número de usuarios, velocidad y rendimiento.

El diseño de la red estuvo a cargo del jefe de la unidad de cómputo de la división de ingenierías civil y geomática; se le encargó a una empresa la instalación del cableado estructurado.

El diseño de la topología de red se puede apreciar en la figura 1-5.

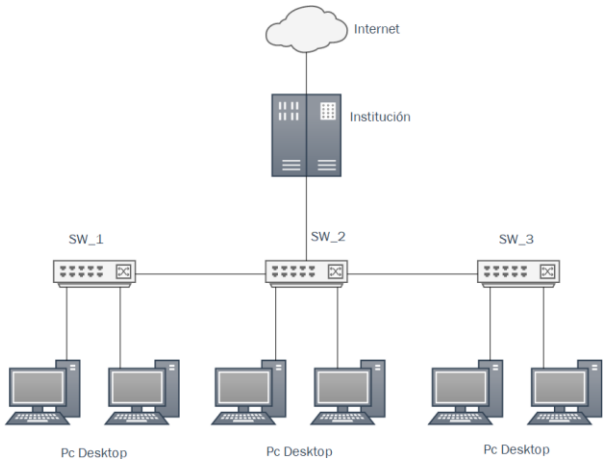


Figura 1-5 Topología de la red (propia)

La nueva instalación de voz y datos contempla: un nuevo punto de distribución por la reasignación de las áreas, la separación de las instalaciones de voz y datos con la eléctrica, el remplazo por obsolescencia del medio de transmisión del cableado estructurado constituido por cable UTP cat. 5 por cable UTP cat. 6a para el cableado horizontal y fibra óptica multimodo OM3 para el cableado vertical la comparación de los diferentes medios se puede ver en la tabla 1-1, la ampliación de nodos disponibles para el centro de cómputo de 60 a 120, remplazo de equipos para soportar las nuevas tecnologías. Se conservaron algunas canaletas laterales desde donde se distribuyen algunas salidas de conexiones por las diferentes áreas del centro desde punto central de distribución del área de switch y servidor.

Tabla 1-1 Comparación de medios de transmisión

Característica	**UTP cat. 5**	**UTP cat. 6a**	**Fibra óptica OM3**
Distancia	100 m	100 m	550 m
Inmunidad electromagnética	Limitada	Limitada	Alta
Seguridad	Baja	Baja	Alta
Ancho de banda	100 MHz	250 MHz	500 MHz
Velocidad	100 Mbps	100 Mbps	1 Gbps

En el área de switch y servidor están instalados tres switch’s de donde parten las conexiones para las diferentes áreas que conforman el centro de cómputo, el servidor opera como nodo central y cortafuegos. Estos equipos remplazaron a los anteriores de la instalación anterior por

obsolescencia. La conexión con la infraestructura de red de la institución es a través de fibra óptica.

La red de cómputo utiliza cableado estructurado con tramas que pasan por debajo del piso falso con un total de 120 nodos repartidos entre las diferentes áreas (figura 1-6).

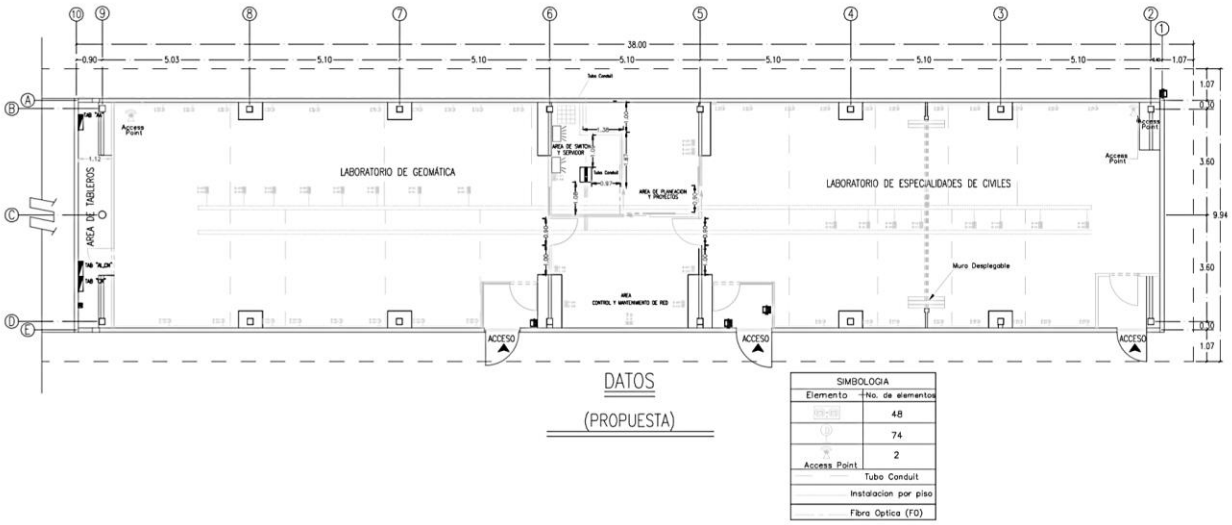


Figura 1-6 Plano (Centro de cómputo, 2018)

El rack de comunicaciones es de cuatro postes remplaza al anterior de dos postes y ahí se montaron el servidor, switch's, paneles de conexiones para fibra óptica y cable par trenzado (*UTP*), organizadores y una unidad de respaldo de energía (UPS). Tiene conexión a tierra física.

El cable UTP es de Cat 6A y el estándar de conexiones en los jacks es el T568B, la distribución de los cables para el estándar se puede apreciar en la figura 1-7.

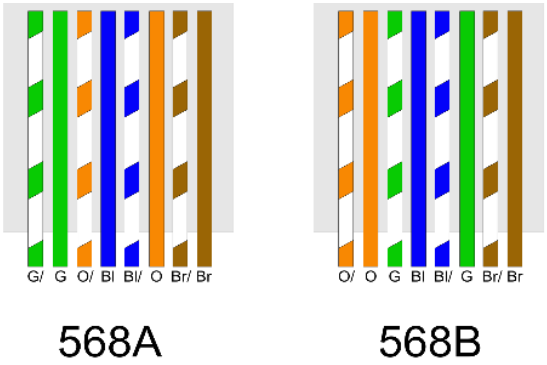


Figura 1-7 Estándares TIA-568B (568 A 568 B, s.f.)

La instalación de acondicionado (*minisplit*) es la siguiente:

- Los dos laboratorios con dos unidades minisplit cada una.
- El área de switch y servidor con dos unidades minisplit.

La red está conformada por tres switch's administrables que dan servicio a las cinco áreas: uno para el Laboratorio de Geomática, otro para el Laboratorio de Especialidades de Civiles y un tercero para las áreas de control y mantenimiento, planeación y proyectos y servidor y switch.

Los equipos instalados en el rack son:

- Un servidor DELL PowerEdge R440 (16 GB RAM, 4 TB HDD, Xeon).
- Tres switch's HPE 5130 (48 puertos RJ45 y 4 puertos para los transceptores (*transceiver*) SFP+.

Los equipos anteriores y otros componentes en el rack se pueden ver en la tabla 1-2.

Tabla 1-2 Equipo montados en el rack

Dispositivo	**Marca**	**Característica**	**Cantidad**	**Estado**
Switch	HPE	48 puertos	3	Nuevo
Servidor	DELL		1	Nuevo
Cableado		6A	N metros	Nuevo
UPS	APC	1500 VA	1	Nuevo
Patch panel	SBE	24	5	Nuevo
Distribuidor fibra	SBE	6	1	Nuevo

1.3.1 Distribución del equipo de cómputo.

En el Laboratorio de Especialidades de Civiles están instalados 15 equipos para uso de los alumnos y uno más para el profesor; en el Laboratorio de Geomática tiene 12 equipos para alumnos y uno para el profesor. Todos los equipos disponibles obedecen a tres configuraciones:

- HP Workstation Z210 (Intel i3 1st Gen., 4 GB RAM, 500GB HDD).
- Lenovo ThinkCentre (Intel i5 6th Gen., 8 GB RAM, 1T HDD).
- Dell Optiplex 7400 (Intel i7 6th Gen., 8 GB RAM, 1T HDD).

En el área de control y mantenimiento se dispone de 3 computadoras personales y una impresora para el personal que labora en el área. La distribución de equipos se puede apreciar en la tabla 1-3.

Tabla 1-3 Distribución de equipos

Lugar	**Computadoras**	**Impresoras**
Laboratorio de Especialidades de Civiles	16	
Laboratorio de Geomática	13	
Área de control y mantenimiento	3	1
Área de planeación y proyectos	1	
Área de switch y servidor	1	

Todos estos equipos de cómputo son los mismos que los utilizados antes de la remodelación.

1.4 Personal, usuarios y servicios

El personal del centro se conforma de un coordinador, su asistente y el auxiliar. El personal auxiliar está conformado por prestadores de servicio social, se encargan de realizar distintas tareas: supervisar los horarios de las actividades que se realizan en el centro, atención a usuarios, mantenimiento preventivo y correctivo a los equipos, la administración de la red y actualización de la página web, administración de la red, entre otras.

Por otra parte, los servicios que se ofrecen en el centro son: software especializado de las carreras de ingeniería civil e ingeniería geomática para apoyar la impartición de clases tales como: Autocad, Revit, Robot, Sap, Etabs, Mathcad y STAAD.

Los usuarios del centro son alumnos y profesores de las carreras de ingeniería civil e ingeniería geomática. Los profesores interesados en hacer uso del Centro solicitan al jefe del departamento de la carrera respectiva una reservación la cual se hace de acuerdo con la disponibilidad.

1.5 Contexto de la problemática del centro de cómputo

En el centro de cómputo se prestan los servicios para la impartición de clases, aplicación de exámenes y otras actividades de apoyo para las carreras de Ingeniería Civil e Ingeniería Geomática. Éstos van, desde el uso del aula, uso de equipos con acceso a la red para el uso académico con software especializado, así como otras actividades que requieran de recursos de cómputo.

El 19 de septiembre de 2017, el centro de cómputo realizó sus actividades con normalidad hasta el momento en que un sismo sacudió la Ciudad de México. Por lo anterior, se aplicó el protocolo de protección civil y se evacuó al personal e impidió el reingreso a toda persona hasta dictaminar el estado estructural del inmueble y así aprobar o no la reanudación de las actividades.

El 24 de septiembre 2017, tras concluir las revisiones al inmueble se dictaminó que las instalaciones del centro no eran seguras ya que presentaron daño estructural; este ocurrió en la zona sur de la planta por lo que sólo el centro de cómputo fue afectado. Por lo anterior, se clausuraron las instalaciones y áreas aledañas al centro como medida de precaución.

La institución reanudó actividades el 25 de septiembre de 2017; fue hasta entonces que el personal ingresó al centro para extraer equipos y mobiliario que fueron trasladados a un aula aledaña en una planta inferior.

Un especialista estructural realizó un estudio y determinó las acciones necesarias para la rehabilitación de las instalaciones. El Coordinador del Centro fue el responsable de supervisar y aprobar estas acciones.

En el mes de diciembre de 2017 iniciaron las actividades de rehabilitación de las instalaciones. Se retiró el escombro, vidrios, canceles de aluminio, Tablaroca, piso falso, divisiones entre áreas. Posteriormente se reforzó la estructura del inmueble con elementos metálicos en los pilares y se retiró una plancha de concreto sobre la losa de la planta inferior para aligerar el peso.

En abril de 2018 se terminaron a las reparaciones. Se verificó que las instalaciones fueran seguras de nuevo y se comenzó a preparar las aulas para reiniciar el servicio del centro.

Fue entonces que se instaló el piso falso, las divisiones de áreas con perfiles de aluminio, de acuerdo con la figura 1-8. Asimismo, se dio mantenimiento a los equipos de aire acondicionado y se colocó una línea nueva de desagüe.

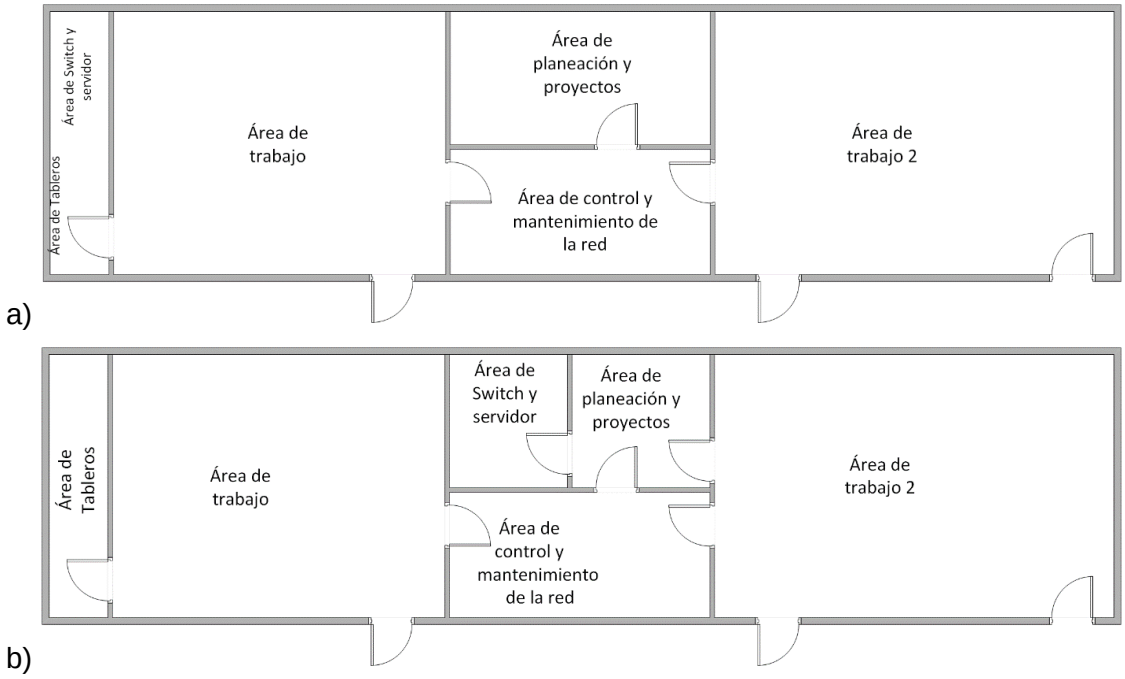


Figura 1-8 División de las diferentes áreas a) Antes de remodelación b) Después de remodelación (propia)

Se dio mantenimiento a los equipos de aire acondicionado y se instalaron dos nuevos equipos.

La jefatura de la División decidió que como parte de la rehabilitación del centro de cómputo se hiciera una actualización de la red. Se nombró como responsable de ésta al jefe de la Unidad de Cómputo de la División.

Para la actualización de la red se hizo un proyecto ejecutivo que incluye la instalación de nuevo cableado estructurado. La propuesta seleccionada quedó a cargo de una empresa especializada que tuvo 20 días para hacer su instalación.

En mayo de 2018 se dio inicio con las actividades para la actualización de la red. Se realizó la canalización del cableado estructurado con ruta a través del piso falso con charolas, tubos y canaletas de la antigua instalación de red, se puede apreciar en la figura 1-9.

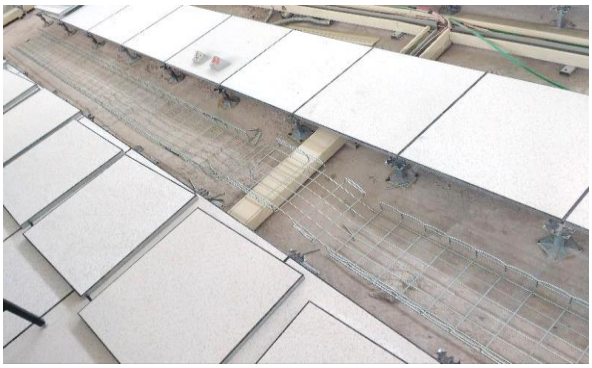


Figura 1-9 Charolas para canalización (propia)

Se instaló el cableado hacia los diferentes puntos de conexión con cable UTP cat. 6A a partir de un punto central de distribución ubicado en el área de switch y servidor figura 1-10.

Figura 1-10 Instalación de cable Cat 6A (propia)

Se instaló el rack en el área de switch y servidor figura 1-11.

Figura 1-11 Rack (propia)

Se conectó el rack a la tierra física, se adecuó la red eléctrica para nuevos puntos de conexión y el peinado y parcheo del cableado en los paneles de parcheo (patch panel) en el rack figura 1-12 como en las rosetas de las diferentes áreas figura 1-13.

Figura 1-12 Conexiones en patch panel (propia)

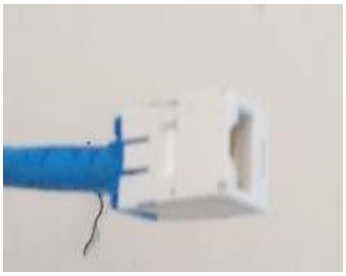


Figura 1-13 Conexión en jacks (propia)

En este punto se consideró pertinente aumentar el número de nodos de los planeados inicialmente en el proyecto de actualización de la red, lo que representó un retraso en la fecha de entrega por parte de la empresa encargada en la instalación.

Se realizó la instalación de fibra óptica del punto de distribución por parte de la institución a la entrada de servicio en el centro de cómputo.

Se hicieron pruebas para detectar problemas de conexión extremo a extremo de los diferentes nodos a su ubicación en el rack.

En junio de 2018 se finalizó la instalación de la infraestructura de red del centro de cómputo

A finales de junio de 2018 llegan los equipos para el área de switch y servidor, los cuales están conformados por un servidor, tres switch's, cuatro módulos SFP+ para fibra óptica y un UPS. Se realizó el montaje sobre el rack en donde un módulo SFP+ fue instalado en cada switch. Se conectó uno de los switch con la conexión a la red de la institución.

El orden de los equipos montados en el rack es de arriba hacia abajo con los equipos de mayor peso colocándose en la parte inferior el orden es mostrado en la figura 1-14.

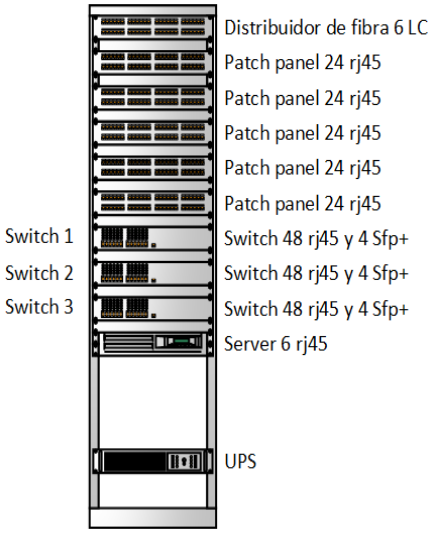


Figura 1-14 Orden en rack (propia)

Se colocaron las computadoras y demás equipos en el mobiliario respectivo donde se hizo una prueba de funcionamiento ya que se temía se hubieran dañado durante su almacenamiento, afortunadamente ninguno presentó fallas.

1.6 Definición del problema

Después de la instalación realizada y concluida en junio de 2018 se probaron las conexiones en la red con los equipos presentes. Se utilizó un firewall con la configuración otorgada por la institución para la conexión a internet, se presentaron dos problemas.

1.6.1 Primer problema.

Segmentación en la red LAN sin que ésta fuera una característica planeada de la red; se tienen 3 segmentos de red que aíslan el tráfico entre ellos y en consecuencia el software de monitoreo de los equipos de los usuarios no funciona de manera correcta ya que requiere que todos los equipos se encuentren en el mismo segmento, la imposibilidad de compartir archivos entre los equipos pertenecientes a diferentes segmentos, acceso a dispositivos compartidos en la red, entre otros.

Posible causa: se encuentra relacionada con la interconexión de los switch's, éstos no pueden realizar la conexión entre ellos ya sea por un fallo en su configuración o en el medio de transmisión que se utilizó para conectarlos.

1.6.2 Segundo problema

Fallo de conexión con la red de la institución la cual es responsable de proporcionar la conexión al exterior, en consecuencia, no se puede acceder a redes externas de la institución (Internet).

Posible causa: esta puede estar localizada en el nodo central que se encarga de recibir la conexión por parte de la institución, el medio por el que se realiza la conexión o no se proporciona el servicio.

A los problemas anteriores se suma que el responsable de dirigir la actualización de la red aludió sobre equipo faltante después de la llegada de los switch's y servidor posteriormente se dejó a observación.

1.6.3 Análisis de los problemas

Al realizar una comprobación física del estado de conexiones se encontraron los siguientes puntos relacionados con cada uno de los problemas:

- Para el primer problema: no se posee ningún tipo de conexión física para mantener comunicación entre los diferentes switch's.

- Para el segundo problema: la conexión por fibra óptica a la infraestructura de la institución se encuentra colocada sobre uno de los puertos de los módulos SFP+ de uno de los switch en donde el led de estatus se encuentra apagado. Al no poder establecer conexión del switch al dispositivo que proporciona la conexión por parte de la institución, se puede suponer que el problema con la conexión esté relacionado con la configuración del switch, el medio de conexión (fibra óptica) presenta fallos o no se presten los servicios por parte de la institución.
- El servidor dedicado a nodo central se encuentra fuera de servicio ya que éste no posee ningún tipo de software instalado en el equipo a excepción del firmware del equipo, se desconoce el tipo de configuración planeada para el servidor.

La representación de los fallos se puede apreciar en la figura 1-15:

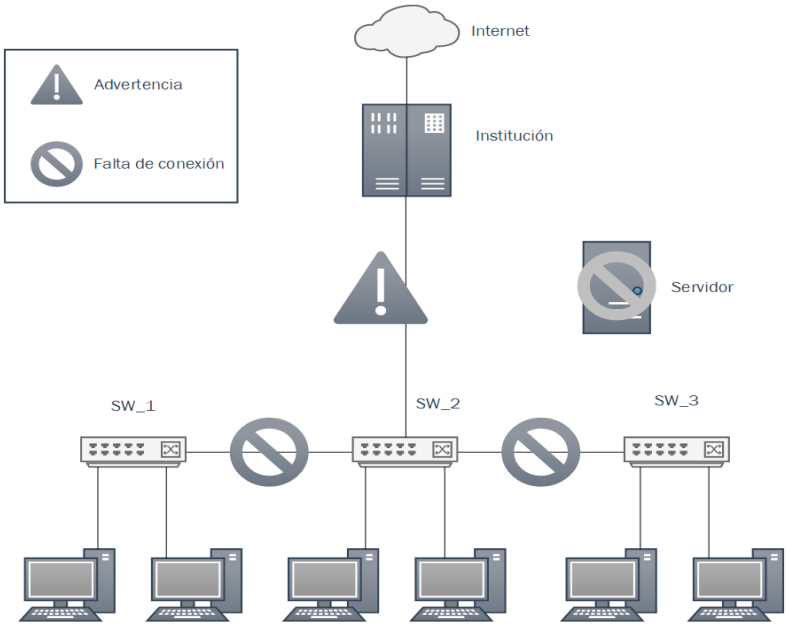


Figura 1-15 Puntos de fallo en conexión (propia)

Con los puntos anteriores y la información proporcionada sobre la actualización de la red se puede determinar que la planificación no contempló algunos detalles y en consecuencia derivó en:

1. La falta de adquisición de dispositivos y medios de conexión ya sea por no contemplar su adquisición en la elaboración del proyecto por un error en la elaboración del presupuesto o porque el presupuesto no fue flexible a los cambios efectuados sobre la marcha.

2. Entregar un proyecto inconcluso que retrasó la reanudación de las actividades del centro de cómputo al reducir los servicios prestados en éste.

Capítulo 2. Marco teórico

En el presente capítulo en primera parte se dará una breve explicación sobre las bases teóricas de redes para el desarrollo del proyecto, aspectos referentes a diferentes metodologías, así como la propuesta de una metodología mixta con base en las metodologías expuestas.

2.1 Redes de datos

Es un sistema de comunicación que permite la interconexión de un conjunto de equipos para intercambiar, almacenar y procesar información.

Los objetivos de las redes de datos son:

- Compartir recursos, información de forma local o remota.
- Transmitir información entre los usuarios de forma rápida y eficiente.

2.1.1 Clasificación de las redes.

Las redes de datos se clasifican de acuerdo con su alcance y tamaño. Algunas de ellas son las siguientes (Joskowicz, Redes de datos, 2007):

- LAN: por sus siglas (Local Area Network), son las redes de alcance limitado generalmente a una red de ordenadores dentro de un área como lo son edificios o campus.
  Ethernet: el IEEE organismo encargado de regular las redes LAN por su estándar 802.3, distingue a las redes LAN de las otras a un área limitada en el que pueden depender de un canal físico con una alta velocidad de transferencia y poca tasa de errores (Jiménez Moreno & Rojas Arteaga, 2015).
  *"*Es un estándar físico y de enlace de datos para la transmisión de tramas en una LAN*"* (Oppenheimer, 2011).
- WLAN: por sus siglas (Wireless Local Area Network), son las redes inalámbricas de alcance limitado, se hace uso de bandas de frecuencia sin licencia.
- WAN: por sus siglas (Wide Area Network) son las redes con un amplio alcance, donde una característica es la interconexión de dos o más redes LAN

- WWAN: por sus siglas (Wireless Wide Area Network) son las redes inalámbricas con un amplio alcance, conecta diferentes localidades por satélites o antenas de radio microondas.

Algunas de las características de las redes se pueden apreciar en la tabla 2-1.

Tabla 2-1 Tipos de redes por extensión geográfica

Nombre	Tipo de Acceso	Alcance	Estándares*
LAN	Privado	10-100 m	IEEE 802.3 - Ethernet
WLAN	Privado	<100 m	IEEE 802.11 a/b/g/n Wi-Fi
WAN	Publico	100-1,000 Km	EIA/TIA-449
WWAN	Publico	<15 Km	IEEE 802.20 GSM, 3GPP, EDGE

**Los estándares son sólo algunos para el tipo de red que se especifica.*

2.1.2 Medios de transmisión.

Son las vías por las cuales el emisor y receptor pueden comunicarse o transmitir datos. Se clasifican en dos tipos (figura 2-1) (Medios de Transmisión de Cobre, s.f.):

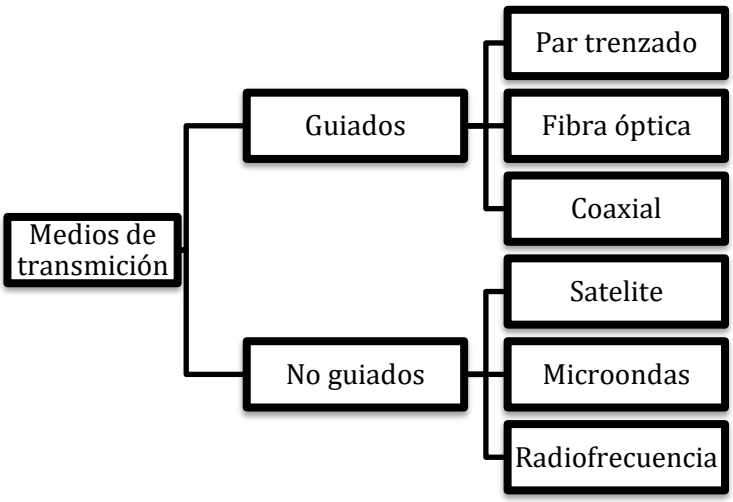


Figura 2-1 Medios de transmisión (ibídem)

A continuación, se mencionan algunos de los medios guiados válidos para este proyecto.

Par trenzado: es un medio guiado donde la información se transmite con señales eléctrica, conformado por grupos de hilos de cobre recubiertos por una capa plástica entrelazados de forma helicoidal. El más utilizado es el UTP (Unshielded twisted pair) que es un cable de par trenzado sin blindar (figura 2-2). De acuerdo con la categoría y el estándar que se usa trabaja a diferentes anchos de banda y velocidades.

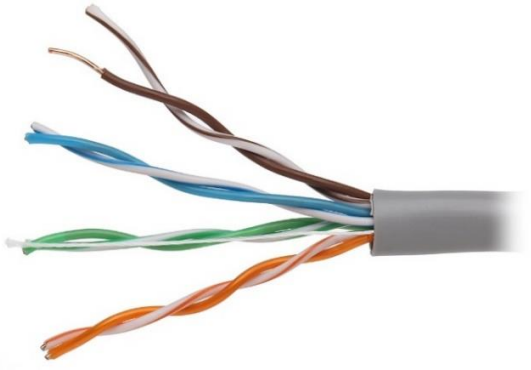


Figura 2-2 Cable UTP (Delta, 2019)

Fibra óptica: es un medio guiado donde la señal que se transmite en forma de luz permite la transmisión a largas distancias con menor atenuación que un medio eléctrico (figura 2-3).

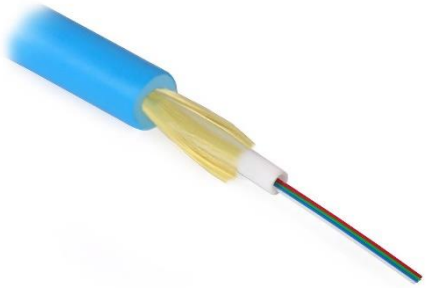
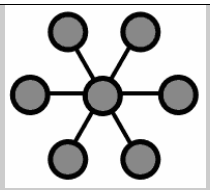
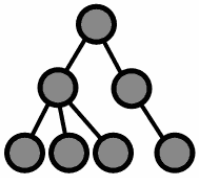
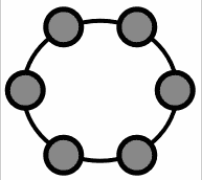
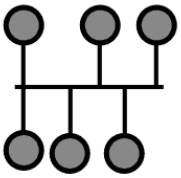
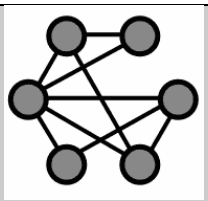


Figura 2-3 Fibra óptica (Delta, 2019)

2.1.3 Topología.

Es el mapa físico de los nodos y concentradores que conforman la red, así como el método de transmisión de datos a su diseño lógico o virtual de los nodos. Algunas de ellas se muestran en la tabla 2-2 (Serrano Macías, 2014).

Tabla 2-2 Topologías de red

Topología	Características	Imagen
Estrella	Cada nodo está conectado a un nodo central.	
Árbol	Conjuntos de redes estrella conectados a un nodo troncal.	
Anillo	Los nodos están conectados a un nodo adyacente y se crea un anillo de forma lógica.	
Bus	Los nodos están conectados a un único canal denominada bus.	
Malla	Todos los nodos se conectan entre sí.	

**fuente de imagen* (Topología de red, 2004)

2.1.4 Cableado estructurado.

Consiste en una estructura de conexión física entre las zonas de trabajo, es dinámica tiene la capacidad de adaptarse a los cambios en las instalaciones, tecnologías, estándares, cambios en tecnologías, etc. (Joskowicz, Cableado Estructurado, 2006)

Estándar ANSI/TIA/EIA-569.

Provee las especificaciones para el diseño de las instalaciones y la infraestructura para el cableado de telecomunicaciones en edificios comerciales. Sus componentes son:

- Instalación de entrada.
- Sala de equipos.
- Back-bone.
- Armario de telecomunicaciones.
- Canalización horizontal.
- Áreas de trabajo.

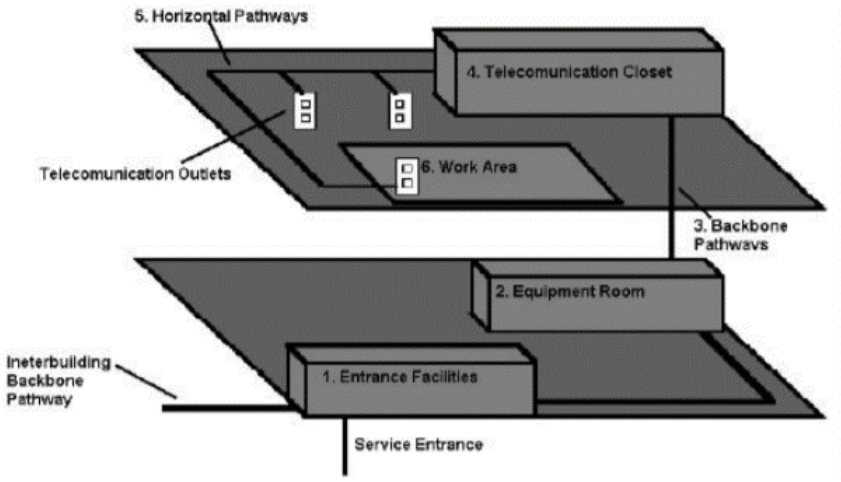


Figura 2-4 Componentes Estándar ANSI/TIA/EIA-569 (Joskowicz, Cableado Estructurado, 2006)

Estándar ANSI/TIA/EIA-568.

Especifica los requerimientos de un sistema de cableado estructurado. Sus componentes son:

- Instalaciones de entrada.
- Main/ Intermediate Cross-Conect.
- Back-bone distribution.
- Horizontal Cross-Conect.
- Horizontal distribution.
- Área de trabajo.

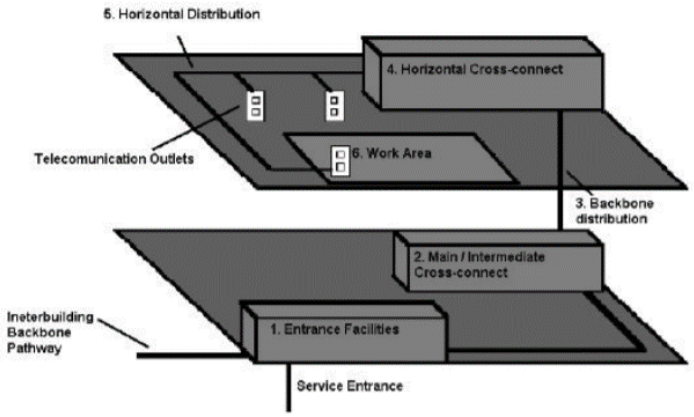


Figura 2-5 Componentes Estándar ANSI/TIA/EIA-569 (ibídem)

2.1.5 Dispositivos de interconexión de red.

En una red existen diferentes dispositivos que la conforman los cuales se clasifican en finales e intermedios. Los dispositivos finales son aquellos que los usuarios hacen uso para el intercambio de información o recurso, en cambio los intermedios son aquellos que interconectan y efectúan la comunicación con los dispositivos finales. A continuación, se una breve explicación sobre algunos de ellos (Jiménez Moreno & Rojas Arteaga, 2015).

Hub: se encarga de recibir una señal, regenerarla y enviarla a todos los puertos, se crea un bus lógico y se usa un método de ancho de banda compartido y normalmente se genera una disminución en el rendimiento en consecuencia a las colisiones que se generan.

Switch: interconecta equipos cercanos por medio de cables, su función es la de unificar redes entre sí, sin examinar a fondo la información ya que se hace uso de una dirección MAC como destino.

Router: se encarga de encaminar los paquetes a sus destinados en redes locales y remotas al utilizar tablas de enrutamiento para determinar la mejor ruta para enviar los paquetes. Los paquetes que recibe los examina la dirección IP destino, busca la mejor ruta y envía el paquete

por la interfaz correspondiente, en caso de que no encuentre coincidencias este la envía a otro router.

2.1.6 Servicios de red locales.

Son servicios que se utilizan en una red local para obtener complementos para el mantener seguridad o una operación amigable de recursos. Algunos de ellos son (Servicio de red, s.f.).

- DHCP: de sus siglas (Dynamic Host Configuration Protocol) es un protocolo que proporciona los parámetros de configuración de la red a los hosts al asignar las IP de forma dinámica.
- FTP: de sus siglas (File Transfer Protocol) es un protocolo para transferencia de archivos basado en la arquitectura cliente-servidor.
- DNS: de sus siglas (Domain Name System) es un servicio que traduce el nombre o dominio de un sitio web en una dirección IP, en la cual procesa la cadena URL con una base de datos para realizar la conversión en una dirección IP.

2.2 Seguridad informática

Es el conjunto de estándares, protocolos, procedimientos y herramientas que permiten asegurar la preservación, disponibilidad, integridad y privacidad de un sistema informático (Jiménez Moreno & Rojas Arteaga, 2015).

Existen dos tipos de seguridad:

- Activa: son las medidas usadas para la detección de amenazas y generar mecanismos adecuados para evitar el problema en caso de su detección.
- Pasiva: son las medidas utilizadas para mitigar el problema generado y con ello el impacto sea menor al usar mecanismos de recuperación.

La seguridad informática maneja dos conceptos de acuerdo con la fuente de la amenaza las cuales se dan a nivel físico y lógico ver figura 2-6.

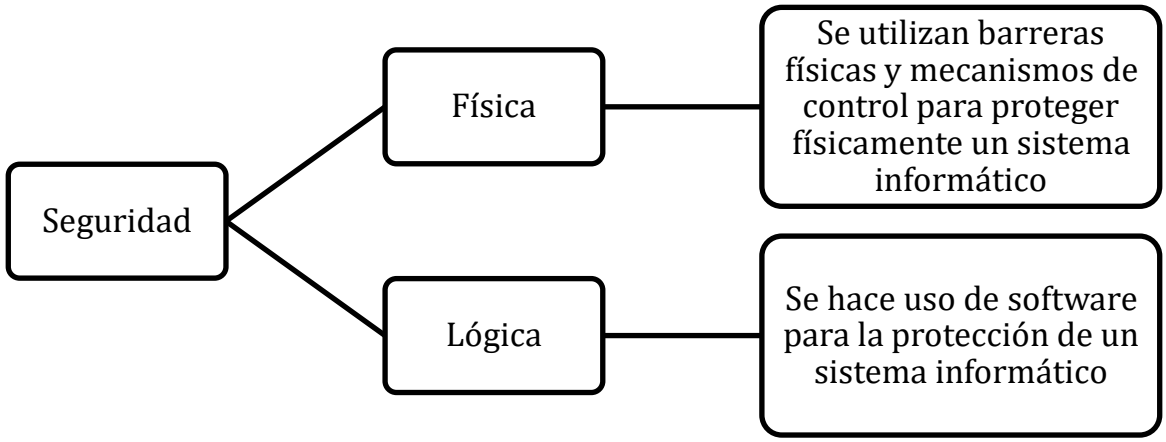


Figura 2-6 Niveles de seguridad (ibídem).

La seguridad informática tiene como objetivo cumplir con seis objetivos referentes a todos los aspectos a proteger para considerar un sistema de información como seguro (ver figura 2-7).

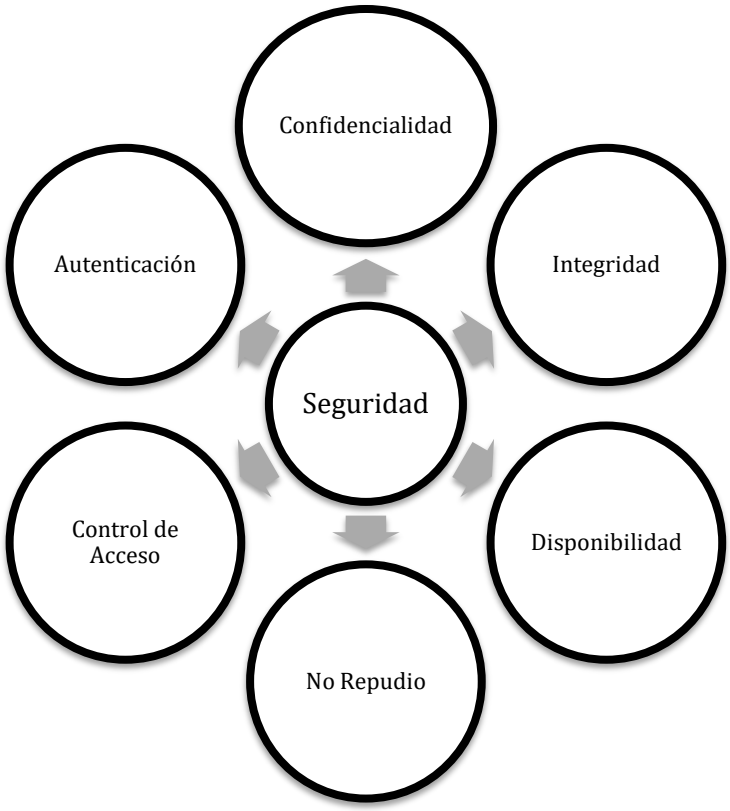


Figura 2-7 Objetivos de seguridad (ibídem).

Una breve descripción de los objetivos anteriores son las siguientes:

- Confidencialidad: la información sólo debe de estar disponible a una entidad autorizada en tiempo y forma.
- Autenticación: asegurar que la entidad sea quien informa ser.
- Integridad: asegurar que la información no ha sido alterada ni destruida sin autorización
- No repudio: proporcionar evidencia sobre la autoría de un hecho.
- Control de acceso: controlar el acceso a la información entre los usuarios y un recurso.
- Disponibilidad: garantizar el acceso a la información en tiempo y forma a un usuario autorizado.

2.2.1 Firewall.

Es un dispositivo que controla la comunicación de acceso no autorizado de usuarios entre una red externa a una red interna, todo el tráfico de red de entrada y salida es filtrado se permite y niega la transferencia de información de acuerdo con una serie de criterios denominados reglas o políticas. Éste se encuentra generalmente entre la red interna y externa para garantizar el intercambio de información de manera segura figura 2.8, así mismo es utilizado para crear deferentes áreas de seguridad. (ibídem).

Figura 2-8 Relación firewall red (propia)

Existen diferentes dos tipos de firewall de acuerdo con los diferentes tipos de infraestructura y tamaños de una red que está destinado, éstos son:

- Software: es el software instalado en los equipos finales como lo son computadoras de escritorio, computadoras portátiles o servidores, donde analiza el tráfico de entrada y salida por medio de protocolos, puertos aplicaciones y demás.
- Hardware: es un dispositivo dedicado para la seguridad perimetral con el que se protegen todos los equipos conectados a la red.

Algunos de los beneficios que se obtienen por utilizar un firewall son (Hernández Sánchez, 2014):

- Administrar los accesos de la red externa a la interna.
- Mantener a usuarios no autorizados fuera de la red.
- Protección para posibles ataques.
- Mejora en los trabajos de administración de la red.

2.3 Virtualización

Es el proceso de crear una representación por emulación vía software de un recurso tecnológico. La virtualización permite ejecutar múltiples sistemas operativos como máquinas virtuales en un único servidor físico. (Domínguez Sanjuán, 2018)

Un *hipervisor* es una plataforma por la que se permite aplicar la ejecución de distintos sistemas operativos alojados en una computadora física denominada *Host* por medio de entornos aislados denominados *Máquinas virtuales*. La administración y gestión del acceso a los recursos de hardware que posee el equipo es a través de monitores la una máquina virtual. (Serrano Macías, 2014)

Existen dos tipos de hipervisores:

- Hipervisor tipo 1: denominado nativo, unhosted o bare metal, es el software que se ejecuta sobre el hardware del equipo anfitrión. Los sistemas operativos invitados se ejecutan sobre máquinas virtuales sobre la capa del hipervisor.
- Hipervisor tipo 2: denominado hosted, es el software que se ejecuta sobre un sistema operativo instalado en el equipo anfitrión. Los recursos para el hipervisor son administrados por el sistema operativo.

Para una mejor referencia sobre los hipervisores ver la figura 2-9.

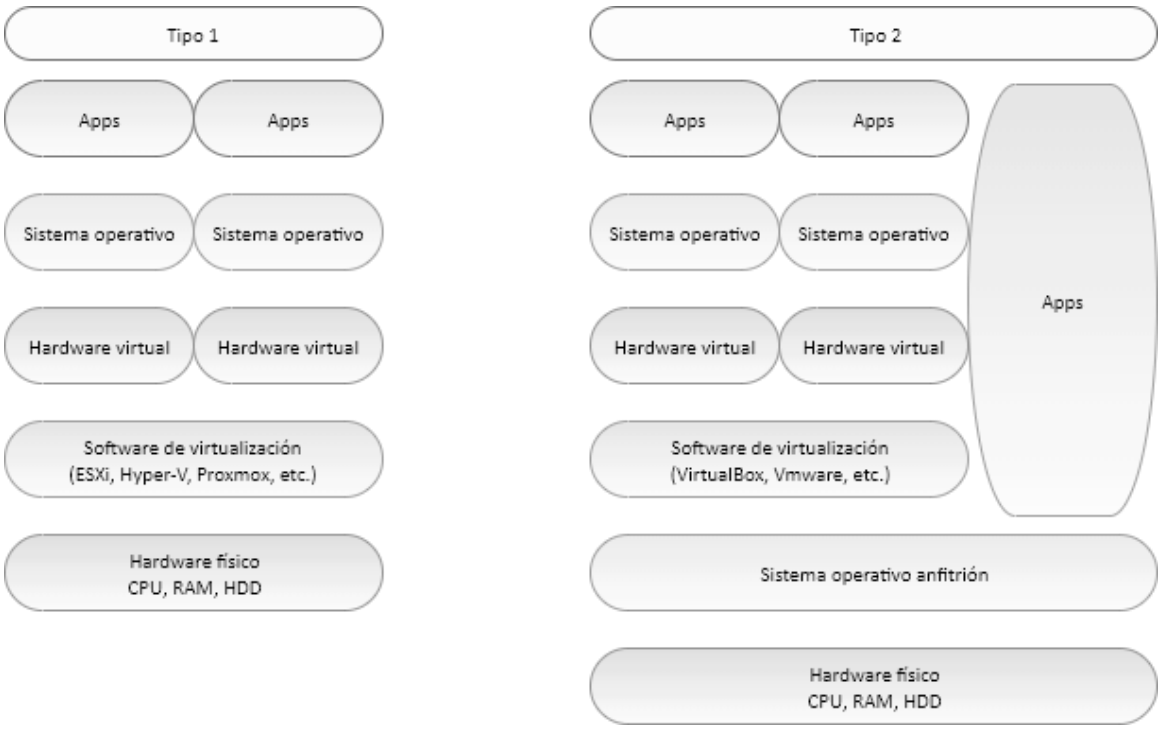


Figura 2-9 Tipos de hipervisores (Domínguez Sanjuán, 2018)

2.4 Metodologías de desarrollo de redes

Las metodologías son procesos ordenados y sistemáticos que permiten lograr un objetivo, en este caso, el diseño de una red que satisfaga una serie de necesidades y requisitos preestablecidos. A continuación, se mencionan ejemplos de ellos.

2.4.1 Metodología Kendall y Kendall.

La metodología Kendall y Kendall se enfoca el en el ciclo de vida del desarrollo de sistemas o SDLC (*Systems Development Life Cycle*); es un enfoque por fases para el análisis y el diseño de redes de cómputo. Su premisa principal consiste en que los sistemas se desarrollan mejor al utilizar un ciclo específico de actividades realizadas por el analista y el usuario. La metodología consta de un total de siete fases (Fajardo Guatarasma & Marcano, 2012):

1. Identificación de problemas, oportunidades y objetivos: se aclara cada problema y su entorno, con base en las oportunidades y objetivos, y se establece un informe con la definición de los problemas y un resumen de los objetivos. (Callata Olivera, 2016)

2. Determinación de los requerimientos de la información: se recolecta la información relativa a cada problema o situaciones con el uso de herramientas que ayudan a determinar los requerimientos de información.
3. Análisis de las necesidades del sistema: los resultados de evaluar las fases anteriores, tomar los aspectos técnicos, operacionales y financieros, arrojan como resultado el análisis de las necesidades del sistema.
4. Diseño del sistema recomendado: conforme a las necesidades planteadas, se construye el sistema.
5. Desarrollo y documentación de software: se construyen los procedimientos del sistema y se documenta su funcionamiento por si es necesario retomar alguna parte del diseño que pudiera producir algún error.
6. Pruebas y mantenimiento del sistema: se ejecuta una evaluación del sistema con el fin de verificar su rendimiento y detectar problemas. Se inicia el mantenimiento del sistema este se realiza constantemente hasta que expire la vida útil del sistema.
7. Implementación y evaluación del sistema: se pone en funcionamiento el sistema y se monitorea con el fin de evaluar su rendimiento.

2.4.2 Metodología James McCabe.

La metodología propuesta por James McCabe para el diseño de redes se enfoca en el área de redes, lo que permite un mejor análisis de requerimientos específicos y flujos de transferencia para las necesidades del sistema de telecomunicaciones. La metodología está compuesta por dos fases (Fajardo Guatarasma & Marcano, 2012).

1. Fase de análisis: consiste en recabar los requerimientos, definir aplicaciones de uso, caracterizar el uso de aplicación, definir los requerimientos de servicio y definir flujos (Callata Olivera, 2016).
2. Fase de diseño: establece las metas del diseño, la selección del tipo de tecnologías, mecanismos de conexión, análisis de riesgos, optimización de flujos, creación de diagramas de la red.

2.4.3 Metodología de diseño top-down network.

Proporciona procesos y herramientas probados para ayudar a cumplir con los requisitos técnicos en cuanto a funcionalidad, disponibilidad, escalabilidad, accesibilidad y seguridad (Oppenheimer, 2011).

1. Análisis de requerimientos: se realiza una entrevista para la comprensión de los objetivos y detallar las tareas. Se realiza un análisis de tráfico actual y futuro, carga y flujo de tráfico, así como el comportamiento de los protocolos y requisitos de calidad.
2. Diseño lógico de la red: esta fase trata sobre la elaboración de una topología nueva y mejorada, direccionamiento de la capa de red, determinar los protocolos de conmutación y enrutamiento al igual que la planificación de la seguridad.
3. Diseño de la red física: se seleccionan las tecnologías y productos sobre el diseño lógico.
4. Pruebas, optimización y documentación del diseño de la Red: la fase final donde se documenta e imprenta un plan de prueba, se crean prototipos y se optimiza el diseño de la red.

2.4.4 Metodología PPDIOO.

Es el conjunto de actividades basadas en metas y necesidades de la empresa para el diseño de una red dentro de un ciclo de vida, como se muestra en la figura 2-10 (ibídem).

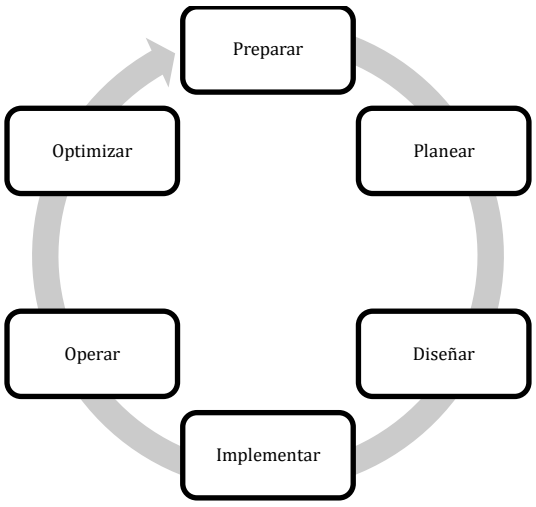


Figura 2-10 Ciclo PPDIOO (Oppenheimer, 2011)

Fases PPDIOO.

1. Preparar: se establecen los objetivos para una inversión, lo que involucra la justificación del tipo de estrategias, tecnologías, costos, entre otros para que ésta sea aprobada.
2. Planear: se identifican los requisitos para la caracterización de la red con el análisis en usuarios, servicios requeridos, áreas de instalación, entre otras, así como las especificaciones de una red existente y la adecuación de ésta. El plan obtenido en esta fase se encuentra presente durante el ciclo de vida del proyecto.
3. Diseñar: se realiza el diseño lógico y físico con base en los requisitos para proporcionar: disponibilidad, escalabilidad, fiabilidad, rendimiento y seguridad con base en los obtenidos en las fases anteriores. Se realizan los diagramas de red y la lista de equipos, con esto el diseño pasa a ser refinado con las peticiones del cliente. Cuanto el diseño es aprobado se puede dar pie al inicio de la siguiente fase.
4. Implementar: comienzo de la implementación al realizar la construcción de acuerdo con las especificaciones del diseño, en esta fase se puede realizar la verificación del diseño. Se da un seguimiento a la implementación para así detectar cambios necesarios e informar de ellos para obtener una aprobación. Todos los pasos de la implementación deben ser documentados para poder dar paso atrás en caso de que se presenten fallos o inconvenientes.
5. Operar: prueba del día a día del funcionamiento de la red, se realiza el monitoreo para detectar problemas en el rendimiento y fallas en la red. En esta fase se pone a prueba el diseño de la red.
6. Optimizar: administración proactiva de la red donde se identifican y resuelven los problemas surgidos en la red. En caso de que la presencia de problemas debido a errores en el diseño, un pobre rendimiento o difiere en la capacidad se tiene que optar por el rediseño de la red y lo que esto implica.

De acuerdo con Cisco, las fases de la metodología PPDIOO se pueden consolidar en tres grupos de acuerdo con los servicios que el cliente puede esperar (figura 2-11). Los tres grupos y las fases que lo componen son las siguientes:

1. Plan: Preparar, planear y diseñar.
2. Construir: Implementar.
3. Ejecutar: Operar y optimizar.

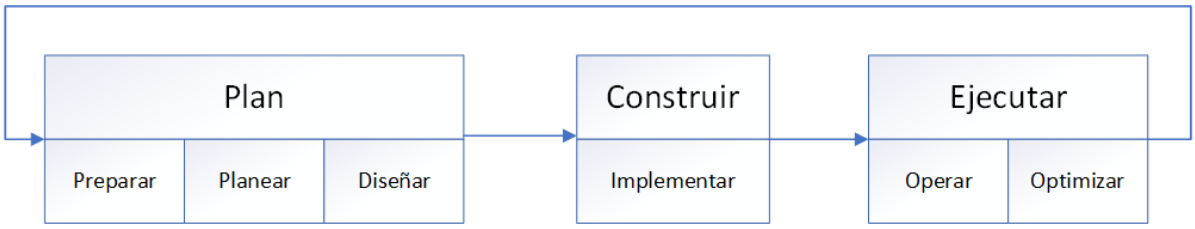


Figura 2-11 Simplificación en tres grupos (CISCO, 2019)

2.5 Metodología a seguir

La metodología propuesta no trata de hacer a un lado las anteriores expuestas, tiene el objetivo de generar una a la medida para la solución de la problemática en el centro de cómputo.

La metodología parte de la idea de Cisco de tener fases transparentes al cliente sobre qué es lo que se va a realizar y que se puede esperar. Las diferentes metodologías antes mencionadas, a excepción de la metodología James MacCabe que termina en el diseño, abarcan el ciclo de vida de un proyecto y si bien cada una maneja diferentes fases en todas se realizan las mismas acciones.
Las metodologías son en apariencia diferentes, sin embargo, si se miran a detalle se observará que se constituyen de pasos similares que cada autor agrupa en fases.

Se propone tomar los pasos pertinentes y agruparlos en tres fases que son las siguientes:

1. Planear: se realiza la investigación sobre el estado físico y lógico para obtener un diagnóstico de la situación actual, si es posible realizar una solución sobre la red existente o se amerita cambios mayores, así como proponer una solución al señalar los costos para efectuarla y por consiguiente evaluarla para encontrar fallas o aspectos omitidos.
2. Construir: con la solución propuesta se prosigue con su implementación se realizan las actividades de documentar los cambios sobre la anterior instalación, así como la nueva configuración implementada. Se realiza un reporte de fallos.
3. Ejecutar: se pone a prueba la solución propuesta con la puesta en funcionamiento de la red, se realiza un monitoreo proactivo para la detección de fallas y si se realiza la optimización necesaria.

En la tabla 2-3 se muestran las actividades realizadas que forma la metodología mixta para el desarrollo del proyecto de diseño de la red de cómputo del centro:

Tabla 2-3 Cuadro operativo

	Objetivos	**Metodologías**	**Actividades**
Fase I	Planear	Fase I, II y II Kendal y Kendal. Fase I, II y III PPDIOO. Fase I y II James McCabe	1. Observar el área 2. Recolección de información 3. Identificación de los equipos 4. Realizar diagramas físico y lógico de la red 5. Evaluar la red existente 6. Solución lógica: topología, direccionamiento y servicios 7. Selección de equipos 8. Presupuesto. 9. Simulación de implementación
Fase II	Construir	Fase IV PPDIOO. Fase II y III Top Down	1. Implementación 2. Documentación de cambios 3. Informe de errores
Fase III	Ejecutar	Fase V y VI PPDIOO. Fase IV Top Down	1. Puesta en marcha 2. Monitoreo 3. Corrección de errores

Capítulo 3. Desarrollo de la solución

Con base en la metodología planteada, se plantean los diferentes puntos que lo conforman para el diseño propuesto de la red de centro de cómputo con la información recolectada y estado del proyecto.

3.1 Planear

Observación del área: se acudió a las instalaciones para recabar el estado de las instalaciones y obtener un panorama general de la situación, se detalla en el capítulo 1.

La información recolectada: para el diseño de la red consiste en las necesidades, fallas, requerimientos que satisfagan el buen funcionamiento de la red en el centro de cómputo (ver tabla 3-1).

Tabla 3-1 Necesidades, fallas y requerimientos

Necesidades	**Fallas**	**Requerimientos**
Red LAN unificada.	No se tienen los medios de conexión entre los diferentes switch's	Unificar la red sin afectar el servicio de monitoreo u otros servicios futuros a implementar
Configuración de punto de acceso	El servidor no tiene la configuración para funcionar como punto de acceso	Configurar el punto de acceso implementado nuevas formas de seguridad en el tráfico de la red
Acceso a internet	No se dispone del servicio	Aprovechar el máximo ancho de banda proporcionado por la institución
Políticas de seguridad	No se dispone de ninguna política de seguridad	Políticas para el acceso físico y lógico de los recursos

Necesidades	Fallas	Requerimientos
Mejorar el tiempo para realizar conexiones para equipos externos al centro de cómputo	No se dispone de servicios que faciliten la conexión a internet	Implementar servicio de automatización en asignar direcciones IP
Facilitar al área de control y mantenimiento de las tareas referentes a la administración de la red	Se dispone de software poco amigable y desactualizado	Implementar una alternativa amigable y confiable para la administración de la red

Identificación de los equipos: el centro tiene un área de telecomunicaciones con un rack un servidor de la marca DELL para implementar diferentes servicios, 3 switch's HP administrables, Una unidad UPS para los equipos. La información se encuentra detallada en el capítulo 1.

Diagrama físico y lógico: los diagramas físico y lógico se realizó con la información proporcionada por el coordinador del centro y lo recabado con la información recopilada. Las figuras representativas son 1-4, 1-5 y 1-6 ubicadas en el capítulo 1.

3.1.1 Evaluar la red existente.

Se requiere saber cuál es el funcionamiento de la red con los problemas principales que derivaron con la creación del presente proyecto para poder trabajar sobre ello.

Pruebas de conexión a la red.

Para la prueba de conexión con la red de la institución se utilizó el equipo usado como firewall que posee las configuraciones para la conexión con la red de la institución, este equipo se almacenó para dar uso al servidor que se adquirió.

La configuración del firewall en cuestión es de un equipo modificado Pentium III, 256 MB, dos interfaces de red y sistema operativo OpenBSD 2.7.

Las pruebas de conexión se realizaron con un switch para pasar de medio óptica a eléctrico ya que el equipo no posee una interfaz con soporte a medios ópticos. El firewall no pudo establecer

conexión con la red de la institución. Se realizó la revisión con los leds de estatus y éste se encontraba inactivo.

Para la revisión de la configuración vía navegador de los switch's ya que no poseían una configuración para poder realizar su administración por otra vía que no es por consola, al no tener IP asociada para un control por el administrador de red se realizó la configuración realizada fue la siguiente: con el software PUTTY (xterm terminal emulator), con la ayuda de un cable de consola de RS232 a RJ455 y la configuración predeterminada del software para puerto serial se ingresó:

```
$ system-view
$ interface vlan-interface 1
$ ip address 192.168.199.XXX 255.255.255.0
$ quit
$ local-user "admin"
$ service-type http
$ authorization-attribute user-role network-admin
$ password simple "contraseña"
$ ip http enable
$ ip https enable
```

Resultados: se comprobó que la configuración no afectaba a la conexión por fibra óptica ya sea por incompatibilidad de los transceiver, inhabilitación de la interfaz, o fallo en los dispositivos. Se realizó prueba de la fibra por medio tradicional al revisar el haz de luz en los conectores para comprobar si se tiene colisión o si este es tenue o inexistente, se tienen como resultados: no se recibía ningún haz de luz por parte del proveedor de servicios.

Posibles problemas:

- El cableado de la fibra óptica presenta problemas en la trama o conectores.
- El puerto del proveedor de servicios se encuentra apagado o deshabilitado.
- Se tiene una configuración incorrecta por parte del proveedor de servicios.

Se realizó el reporte a las personas responsables del subministro de la red.

Al tener que la prueba por medio de fibra óptica no se podía realizar se realizó la rehabilitación del cable UTP que provee el servicio de red anterior a la remodelación, con un cable utp cat. 5

se creó una extensión del área de tableros al área de switch y Servidor como medida temporal. La prueba de conexión se realizó satisfactoriamente

La velocidad máxima de descarga es de 97 MB y la velocidad máxima de subida es 92 MB., estas pueden variar de acuerdo con la carga en la red que tenga la institución.

Análisis de los equipos.

Los equipos a usuarios finales presentes en el Laboratorio de especialidades de civiles son obsoletos para el manejo de las actividades y el uso de software que se utiliza.

El servidor se encuentra montado en el rack, no se encuentra en operación a falta de una configuración y la existencia de una interfaz que soporte un medio óptico. El equipo es nuevo y con prestaciones suficientes. Los switch's se encuentran montados en el rack.

3.1.2 Solución lógica.

La solución se da en relación con el análisis realizado de la información recolectada anteriormente. Se explica el por qué se realizó la selección de las soluciones.

Topología propuesta.

Se opta por una topología basada en árbol ya que esta satisface los objetivos de escalabilidad, operación entre otros. Las ventajas son:

- Los costos de rediseño son reducidos ya que toma gran parte de la red existente y solo se adquieren los medios de conexión y dispositivos que permitan la conexión.
- Separa la red interna de la red externa compartida por la institución.
- La velocidad no se ve rezagada en los switch's al contar con uno principal al que se distribuyen los demás en comparación a la que se tendría con una conexión en cascada.
- El costo es menor al que se tendría con una configuración en pila entre los switch's.
- Facilita la gestión de la red.
- Mayor seguridad con la red el exterior a interior y viceversa.

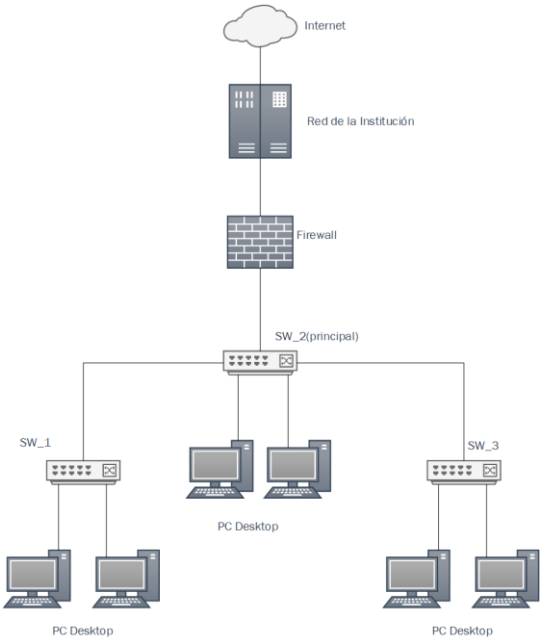


Figura 3-1 Topología propuesta (propia)

En la implementación se usará un entorno virtual para extender los servicios en diferentes máquinas virtuales (MV) y estos no estén concentrados en un solo sistema, donde una MV para un firewall y otra MV para un servidor donde se podrán instalar diferentes servicios como: servidor NAS, servidor web u otro servicio. La estructura lógica se muestra en la figura 3-2.

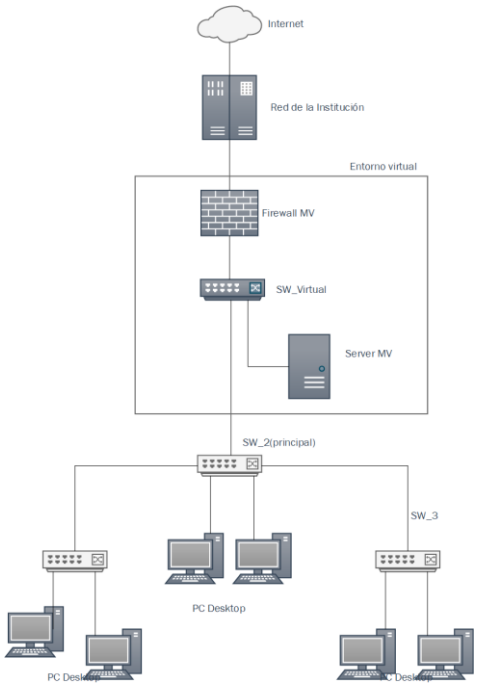


Figura 3-2 Topología completa (propia)

Direccionamiento.

El direccionamiento para los equipos externos al centro de cómputo se realizará de manera dinámica (DHCP) mientras que para los equipos pertenecientes se realizará de manera manual. La implementación de un servidor DHCP para equipos externos es porque se ofrecen:

- Fácil administración de direcciones IP.
- Tiempo en realizar conexión reducido.
- Conexiones sin necesidad de un responsable que proporcione la configuración de conexión.
- No dar la configuración de conexión a externos y esto pueda abrir una brecha en la seguridad del centro de cómputo o a la institución.

La segmentación de redes por VLAN permite crear fronteras lógicas en las distintas áreas y aumentar la seguridad. El rango de direcciones para las VLAN correspondientes a los usuarios se puede ver en la tabla 3-2.

Tabla 3-2 Direcciones VLAN

Dirección LAN	**Usuarios**	**Cantidad**	**VLAN**
192.168.199.1-120	Áreas de trabajo	120	VLAN 199
192.168.200.1-120	Equipos externos	120	VLAN 200
192.168.241-254	Administración	14	VLAN 199
192.168.201.1-253	Áreas de trabajo inalámbrica	253	VLAN 201
192.168.201.254	Administración	1	VLAN 201

Servicios.

Se proponen los siguientes servicios para solucionar problemas de seguridad y conexión, así como mejorar servicios presentes.

Firewall.

La propuesta para control de tráfico de datos que ingresan a la red será por medio de un sistema operativo orientado a Firewall pfSense basado en sistema operativo FreeBSD para sustituir al anterior con OpenBSD también basado en el sistema operativo FreeBSD. Para el uso no comercial es gratuito lo que permite reducción de costos.

La selección de pfSense radica en la facilidad de uso en comparación con el sistema anterior, el centro de cómputo carece de personal de tiempo completo para la administración de la red, por lo que al asignar a un personal temporal para la administración de la red pueda resolver los problemas con mayor rapidez.

El uso de este sistema facilita la configuración de diferentes servicios integrados como parte de sus funciones, estas funciones pueden ser habilitadas en caso de que se requieran en un futuro. Algunas de ellas son: Firewall, DHCP, VPN, NAT, State Tables, Etc.

Para la seguridad en el control de acceso radica en las políticas vigentes en el centro de cómputo que consiste en la creación de listas para el bloqueo de páginas web. Algunos ejemplos son:

- Bloqueos de redes sociales.
- Bloqueos en plataformas de video.
- Bloqueos de páginas de contenido adulto.

3.1.3 Selección de equipos.

Para la selección de equipos se toman las características empleadas para implementar la topología recomendada, los dispositivos a continuación son recomendados y compatibles para el servidor y las conexiones entre el switch y servidor para operar a las velocidades óptimas entre los equipos. Para el adaptador de red en el servidor se consideró la compatibilidad del equipo para ser compatible con módulos SFP+. Para los cables DAC SFP+ se muestran dos diferentes opciones, el uso de cables DAC SFP+ se da por la reducción de costos ya que el uso de transceiver con patch cord de fibra óptica el gasto es más elevado. Se requiere una cantidad de tres cables DAC para poder realizar las conexiones entre switch’s y servidor y como mínimo 2 y

un patch cord de fibra óptica con conectores LC/LC para hacer uso de los dos transceiver restantes (tabla 3-3).

Tabla 3-3 Precios de equipos y medios

Adaptador de Red				
Marca	ID Fab	Puertos	Velocidad	Precio
DELL - MELLANOX	WMW2G	2 SFP+	10 Gbps	290 USD
Cables DAC				
DELL	K592N	SFP+	10 Gbps	271 USD
HP	J9283B	SFP+	10 Gbps	145 USD

3.1.4 Presupuesto.

El presupuesto de los equipos es de referencia, los precios pueden variar con el tiempo al igual que la aparición de equipos más competentes y a mejores precios. En la tabla 3-4 se muestran los artículos y el costo total.

Tabla 3-4 Presupuesto

Presupuesto equipos				
ARTÍCULO	CANTIDAD	PRECIO	SUBTOTAL	TOTAL
Adaptador de red	1	290 USD	290 USD	290 USD
Cables DAC	4	271 USD	271 USD	271 USD
			TOTAL:	561 USD

3.1.5 Simulación.

La simulación del sistema propuesto es dar evidencia sobre el diseño propuesto, donde para lograrlo se realizó la construcción de la red del centro de cómputo con el hipervisor de tipo 2 VMware Workstation. Las acciones realizadas a continuación son las misma que se realizaran en la implementación física. La simulación obedece la configuración mostrada en la figura 3-3.

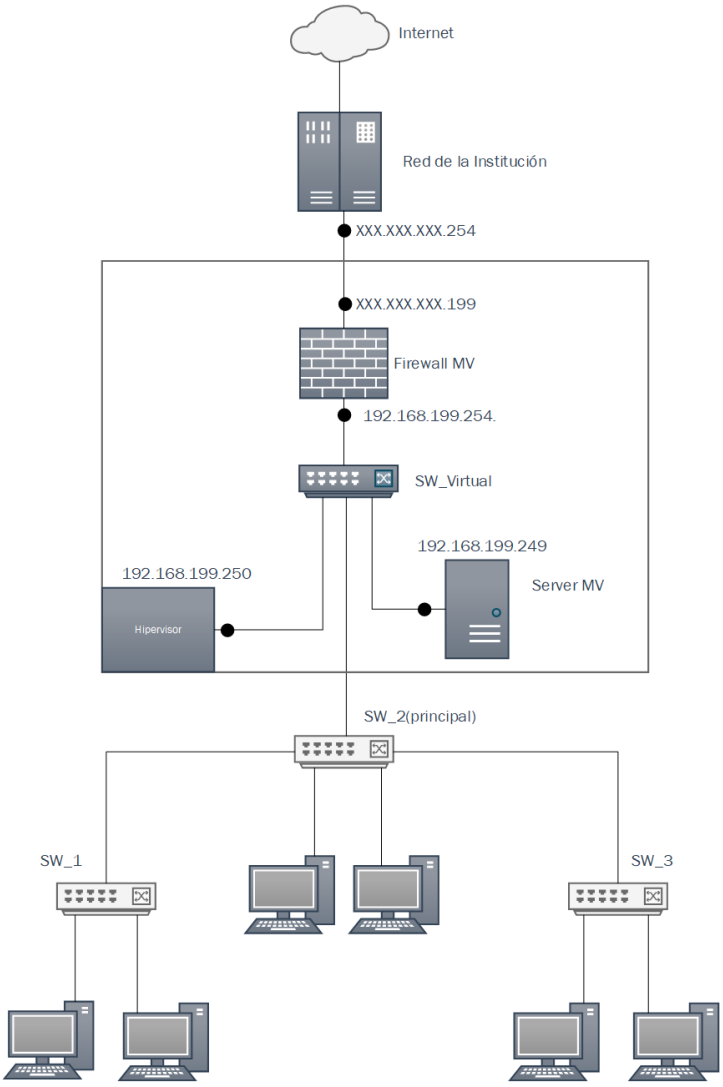


Figura 3-3 IP de las máquinas virtuales en el servidor (propia)

Máquina virtual del servidor.

Se crea una máquina virtual que será la representación del servidor del centro de cómputo. Se instala el hipervisor tipo 2 VMware ESXi versión 6.7.0 en su versión gratuita. La configuración de la instalación de VMware ESXi es la siguiente:

Nombre: VMware ESXi Guest OS family: VMware ESX Guest OS versión: VMware ESXi 6.5 and later CPU: 2 Memory: 2048 MB Hard Disk: 20 GB Network adapter 1: NAT Network adapter 2: Host CD/DVD: ISO*

**Se usará como medio de instalación una imagen de disco de VMware ESXi*
**Se simulará dos interfaces una referente a la red externa y otra para la red interna*

Usuario: root Contraseña: ******** IPv4: static IP:192.168.199.250 Subnet mask: 255.255.255.0 Puerta de enlace: 192.168.199.254 IPv6: none

Nota 1: la contraseña es representada por ******.
Nota 2: la IP 192.168.199.254 pertenece a la dirección del firewall que se instalara.
Nota 3: la IP 192.168.199.250 será la utilizada para acceder al hipervisor por un navegador web.

Se habilitarán dos interfaces que son para la conexión a la red externa y otra para la red interna.

Perfiles de usuario en VMware ESXi.

Se crea un perfil para tener privilegios de administrador con todos los privilegios a excepción de administrar usuarios y manejos de licencias. El perfil es el siguiente:

Usuario: admincc Contraseña: ********

Switch's virtuales y grupos de puertos.

Se crean switch's virtuales para asociar a las interfaces a usar para la conexión con la red WAN y la red LAN y asignar los grupos de puertos a los que pertenecen los switch como lo es la red LAN y WAN que son los que se utilizaran para las máquinas virtuales. La configuración es la siguiente:

Port group: WAN > vSwitch1 Port group: LAN > vSwitch0 Port group: MN* > vSwitch0

**MN hace referencia a Management Network se asocia con LAN para solo hacer modificaciones con la red local.*

Máquina virtual de firewall.

Dentro de VMware ESXi se crea una máquina virtual para funcionar como firewall donde se instalará pfSense versión 2.4.3. Las especificaciones principales de la máquina virtual son las siguientes:

Nombre: Firewall
Guest OS family: Other
Guest OS versión: FreeBSD 11 (64-bit)
CPU: 2
Memory: 2048 MB
Hard Disk: 20 GB
Network adapter 1: LAN
Network adapter 2: WAN
CD/DVD: ISO*

**Se usará como medio de instalación una imagen de disco de pfSense.*

Se habilita el inicio automático de la máquina virtual para que se ejecute con 10 segundos de retaso después de la carga de VMware ESXi.

Se inicia la instalación de pfSense con la configuración siguiente:

Hostname y Domain: Default
Primary DNS: 132.248.10.2
Secondary DNS: 132.248.204.1
Interfaz WAN
IPv4: Static
Address: XXX.XXX.XXX.199
Subnet mask: 255.255.255.0 => /24
Gateway: XXX.XXX.XXX.254
Asignación IPv6: none
Interfaz LAN
Asignación IPv4: Static
Address: 192.168.199.254
Subnet mask: 255.255.255.0 => /24
Asignación IPv6: none

**En la simulación para la IP en WAN se usará un servidor DHCP.*

Para realizar configuraciones se accede a la dirección perteneciente a la interfaz LAN de pfSense con los usuarios por defecto:

User: admin
Pasword: pfsense

Para más detalles configuraciones consultar el apéndice A.

Para realizar la simulación de un usuario se usa una máquina virtual con cualquier sistema operativo conectado a la interfaz virtual del servidor que corresponde a la red LAN que pertenece al firewall. Se le asigna una configuración en red con los siguientes datos.

Asignación IPv4: Static
Address: 192.168.199.1
Subnet mask: 255.255.255.0 => /24
Gateway: 192.168.199.254

Se realizan pruebas para comprobar el acceso a internet de la máquina virtual del usuario que pasa por la máquina virtual que contiene el firewall a la red del equipo donde se virtualizo la red.

2.1 Construir

La fase de construir se conforma por la implementación del diseño propuesto, así como la documentación necesaria sobre los cambios realizados junto con la elaboración de un reporte sobre los errores presentados en su elaboración para realizar las correcciones correspondientes posteriormente si éstas no se corrigieron en el momento.

3.2.1 Implementar

La implementación consiste en realizar las actividades sobre configuraciones e instalaciones físicas y de software del diseño propuesto.

Conexión entre switch's

Para realizar la conexión con la topología en árbol con los cables DAC se realizará con la siguiente configuración:

Conexión Switch1 a Switch2

Switch1 > Switch2
Port_49 > Port_49

Conexión Switch2 a Switch3

Switch2 > Switch3
Port_50 > Port_49

Para una mejor referencia ver la figura 3-3.

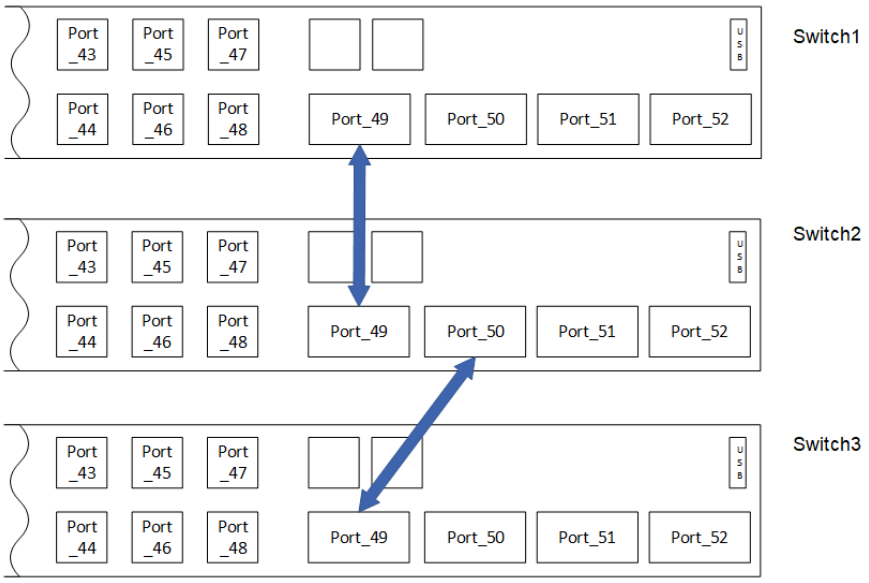


Figura 3-4 Conexiones en switch's (propia)

Configuración de servidor.

La configuración se realiza de acuerdo con el diseño propuesto con anterioridad en el presente proyecto, los pasos a seguir realizados en la simulación, tomar en consideración que los nombres de interfaces, capacidades entre otras pueden variar de acuerdo a la simulación. Con los pasos descritos se deben de obtener los mismos resultados a los obtenidos a los de la simulación.

3.2.2 Documentación de cambios.

Como una medida indispensable se requiere la entrega de la documentación con los cambios e implementación correspondiente a configuraciones físicas y lógicas, con el fin de poder realizar cambios a futuro o dar vuelta atrás para corregir problemas que se presenten.
El documento debe contener:

- Descripción del caso e incluir el por qué y cómo se implementó, no existen las obviedades.
- Usar lenguaje adecuado sobre a quién va dirigido.
- Incluir imágenes, así como descripciones de éstas.
- El documento debe de poseer una estructura coherente para proporcionar un panorama del proyecto.

3.2.3 Informe de errores.

Se realiza un informe donde se indiquen los problemas que se encontraron durante la implementación en donde se incluya:

- Descripción del problema de forma clara y concisa, señalar lo que ocurrió y lo que se esperaba.
- Si se presenta un mensaje de error adjuntar una captura de pantalla.
- Describir el entorno donde se aloja el error SO, aplicación, interfaz de conexión, etc.
- Impacto de daño que se genera.
- Propuesta de como corregir el error de forma inmediata.
- Indicar cómo es posible evitar que el error reincida.

3.3 Ejecutar

La fase final donde se realiza la puesta en marcha de la red, así como diferentes actividades para detectar problemas y solventar u optimizar el rendimiento.

3.3.1 Puesta en marcha.

Se pone a prueba el funcionamiento del diseño realizado, se establece la operatividad de la red y los equipos. Se ejecutan pruebas como la interconexión de los equipos y la conexión a la red externa que son la problemática principal que se tiene en el centro, se complementa con la prueba de aplicaciones como el funcionamiento del software de monitoreo o la transferencia de archivos en la red local. Se realiza la prueba de rendimiento con la red externa e interna, prueba del servidor DHCP si está disponible en toda la red local.

Terminadas lo anterior se realiza la prueba final con el funcionamiento del día a día y con ello obtener una evaluación sobre el diseño de la red, si este no es satisfactorio se tienen que tomar medidas.

3.3.2 Monitoreo.

Se da a la par con la puesta en marcha se realiza el monitoreo sobre el estado de la red con el fin de mejorar la calidad de servicio, así como también encontrar fallos a fin de reducir interrupciones y conservar la disponibilidad de la red. Esto da pie a futuras actualizaciones, adiciones y cambios para lograr la excelencia operativa.

Para el monitoreo de la red se utilizarán herramientas para detectar el tráfico y saturación de la red con las funciones del firewall, así como el rendimiento en los diferentes equipos de la red y las fallas que se presenten en la red sniffers.

3.2.3 Corrección de errores.

Junto al monitoreo se da seguimiento a los fallos que se presentaron en las pruebas funcionamiento u otro fallo arrastrado con anterioridad antes que éstos afecten a la red, si la acumulación de fallos impide el funcionamiento de la red y éstos están relacionados con el diseño de la red se tiene que contemplar la modificación del diseño o el rediseño de la red.

Capítulo 4. Resultados

La implementación de la solución propuesta en el presente proyecto no pudo realizarse enteramente y sin variaciones ya no se pudo adquirir el equipo solicitado a falta de presupuesto, se tomaron acciones para crear una solución a la par.

En resumen, la red instalada adolece de dos problemas principales:

1. Red segmentada por falta conexiones entre los switch's.
2. Falla en conexión con la red de la institución.

4.1 Red segmentada

El proyecto fue incompleto porque no adquirió los módulos sfp+, las tarjetas de red y los cables necesarios que evitarían que se generara el problema de la segmentación o compartición. No fue posible obtener presupuesto adicional para adquirirlos posteriormente.

Esta situación se mitigó de la siguiente forma:

1. Cambio en la topología.
2. Cambio en la configuración de los switch's (reasignación de conexiones).
3. Reconfiguración del servidor.

Con estos cambios se asegura el acceso a la red, pero tiene como desventaja compartir la red, velocidad menor a que podría funcionar, generación de brechas de seguridad, afectar otras redes, ser afectado por otras redes.

Los cambios específicos en el diseño detallado en el capítulo 3 son: el cambio en la topología, configuración en conexiones y cambios en el servidor.

4.1.1 Cambios en topología.

Se conserva la topología recomendada con los siguientes cambios debido a la falta de interfaces y medios de conexión, los cambios realizados yacen en no utilizar el firewall para hacer conexión con la red de la institución y utilizar el switch principal como un convertidor de medio óptico a eléctrico en el que se realizaran las conexiones WAN y LAN correspondientes al firewall, así como realizar la conexiones entre switch's por cable UTP en lugar del propuesto cable DAC.

Las consecuencias de esto son:

- La red interna y la red de la institución comparten conexión, por lo que las otras áreas que compartan su red con la de la institución puedan conectarse con la del centro de cómputo.
- La imposibilidad de crear diferentes VLAN ya que éstas podrían generar colisiones con otra dependencia que comparta.
- Se abren brechas de seguridad al compartir la red al no tener el cortafuegos para impedirlo.
- Para realizar las conexiones adecuadas se dará por medio de interfaces de menor velocidad, en consecuencia, podría generar cuellos de botella.
- No se aprovechará la interconexión entre los dispositivos a como están diseñados.

En la figura 4-1 se muestra la topología empleada.

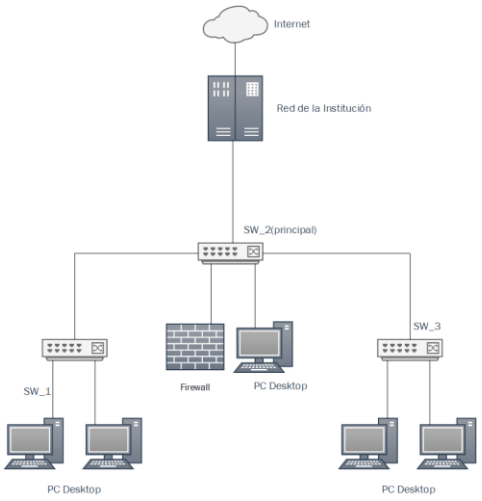


Figura 4-1 Topología implementada (propia)

4.1.2 Configuraciones.

Para poder realizar la conexión entre los switch's en ausencia de transceiver y patch cord de fibra óptica u otro medio para realizar una correcta conexión en los switch, se procedió con cable UTP Cat 6A disponibles en el centro de cómputo y la reasignación de conexiones en los puertos RJ45 para una conexión en árbol. La reasignación fue necesaria ya que todos los puertos RJ45 de dos switch's estaban en uso, las se realizaron de la siguiente forma:

Reasignación de cables para desocupar puertos Ubicación Original>Ubicación Final Switch2> Switch3 Port_47>Port_48 Port_45>Port_45 Port_48>Port_47 Switch1> Switch2 Port_47>Port_47

Puertos utilizados para la conexión en árbol Switch1 Port_47 <=> Switch2 Port_48 Switch2 Port_45 <=> Switch3 Port_29

La representación gráfica de las conexiones se puede apreciar en la figura 4-2

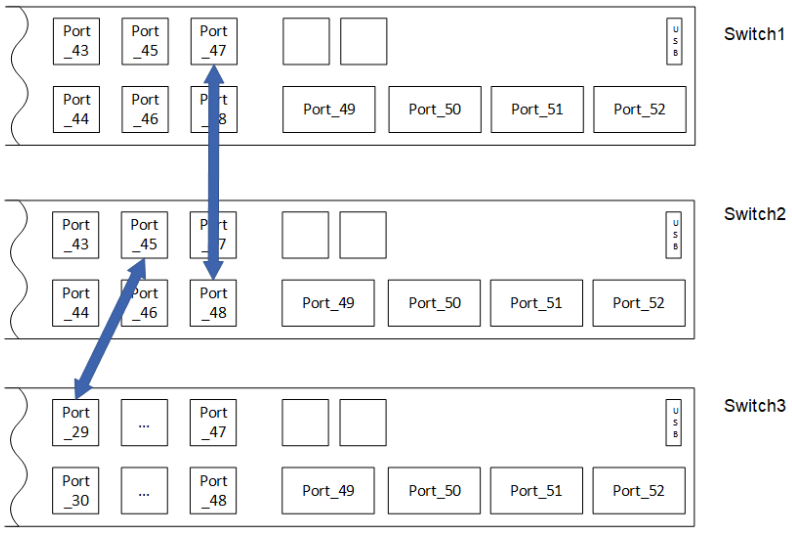


Figura 4-2 Puertos para conexión en árbol (propia)

4.1.3 Cambios en el servidor.

Los cambios implementados en el servidor funcionan aún con los cambios realizados, pero queda a aclarar los cambios en el direccionamiento y el uso del firewall.

Direccionamiento.

El direccionamiento por medio de un servidor DHCP es posible con el inconveniente que otras áreas puedan hacer uso de éste para poder conectarse a internet. Esto genera las siguientes desventajas:

- Afectar el uso de la red a otras áreas que compartan la red
- Generar tráfico de salida con equipos fuera del centro de cómputo
- Dar conexión a usuarios no autorizados
- Saturar las direcciones IP disponibles que se le asignaron al servidor DHCP

El diseño de las VLAN fue alterado ya que la configuración puede entrar en conflicto con otras áreas. Los cambios se dan con el uso de dos interfaces del servidor al separar una de la red compartida para realizar la conexión con un acces point para una conexión inalámbrica.

Tabla 4-1 Direcciones VLAN posibles

Dirección LAN	**Área**	**Cantidad**	**VLAN**
192.168.199.1-120	Áreas de trabajo	120	VLAN 199
192.168.199.121-240	Equipos externos	120	VLAN 199
192.168.199.241-254	Administración	14	VLAN 199
192.168.200.1-253	Áreas de trabajo inalámbrica	253	VLAN 200
192.168.200.254	Administración	1	VLAN 200

Servicios.

Para el Firewall**,** los servicios propuestos con ayuda de pfSense si bien son viables y no son afectados de gravedad se presentan las siguientes desventajas:

- El servicio de salida se ve limitado por la interfaz de conexión.
- Se crea una brecha de seguridad para que un usuario externo al centro de cómputo puede vulnerar el firewall.

La configuración del servidor con los servicios descritos en la simulación se realizó sin inconvenientes. Con ello se puede ver la importancia que se tiene al realizar una simulación para ver el comportamiento que se obtiene y preverse en caso de fallos. Tomar en consideración que el no obtener fallos en la simulación no descarta que al implementar el sistema en el servidor no se generen uno a causa del tipo de hardware u otros.

4.2 Conexión a la red

Para resolver la falla no fue necesario modificar la metodología.

En el transcurso de la implementación se encontró que se poseía conexión por fibra óptica, esta se encuentra conectado sobre el puerto 49 en el switch 1 ésta se trasladó al puerto 49 del switch 2 para que corresponda con la topología a implementar.

Se pidió una explicación por parte del nuestro proveedor de servicios en la institución, la respuesta fue la del puerto que da conexión al centro de cómputo se encontraba deshabilitado.

Se desconectó el cableado UTP y se utilizó la conexión por fibra óptica, la conexión se realizó sobre el mismo switch utilizándolo como conversor de medio óptico a eléctrico. La conexión de nuestro cable WAN correspondiente a la salida del servidor se colocó sobre el puerto 38 del switch 3.

El servicio de red en el laboratorio se encontró en estado activo. La velocidad máxima de descarga es de 408 MB y la velocidad máxima de subida es 673 MB (las velocidades pueden variar a causa del tráfico de red en la Institución).

4.3 Cambios complementarios o consecuencia de la adecuación

A los cambios anteriores se elaboró la documentación correspondiente a los cambios obtenidos en la presente propuesta, así como los fallos generados por la propuesta.

4.3.1 Documentación de cambios.

Se entregó la documentación con los cambios en las conexiones, así como la configuración utilizada en los diferentes dispositivos. Se entregaron dos documentos en los que destaca los siguiente:

- Descripción del proceso del por qué y cómo se implementó.
- Inclusión de imágenes y descripción gráfica de los procesos.
- División en dos documentos en los que contienen los cambios en conexiones físicas y la configuración del sistema respectivamente.

4.3.2 Informe de errores.

No se encontraron errores durante la implementación del sistema o en los cambios en las conexiones, aún con ello se entregó un informe con los errores ajenos a la implementación del presente proyecto donde se indican los fallos por los que la red no operaba con resultados satisfactorios.

4.4 Puesta en marcha, monitoreo y corrección de errores

Tras la puesta en marcha para las actividades del día a día en la red del centro de cómputo de todo los descrito con anterioridad con un monitoreo constante de una duración de 5 meses y un funcionamiento con una duración aproximada a 9 meses no se han encontrado fallas en el funcionamiento de la red, así como de los servicios. Esto no concluye el proceso de monitoreo ya que éste se debe de realizar durante toda la vida útil de proyecto.

Capítulo 5. Conclusiones

Con lo disponible, se logró cumplir con el objetivo principal de resolver las fallas en la red del centro de cómputo con los dispositivos y recursos existentes.

Se propuso una nueva metodología para obtener una solución y evitar fallos al no contemplar algún aspecto.

Se aprendió una nueva metodología, ese aprendizaje funciona para evitar lo que pasó.

La problemática es el resultado de un proyecto ejecutivo incompleto, con el que no se consultó experto en redes, con lo que se obtuvo un proyecto rígido.

La red funcionaria de forma eficiente sin los problemas generados por la solución empleada si se realizara la inversión de 561 USD.

Apéndices

Para la elaboración de la simulación del diseño de red propuesto se detallan los pasos mostrados en el capítulo 3.

A Software para la simulación

La simulación empleada en este proyecto para la fase II se realizó con el software VMware Workstation donde se realiza la instalación de los diferentes sistemas. La máquina virtual VMware ESXi 6.7.0 será la referente al servidor. Una vista al hipervisor se puede apreciar en la figura 6-1.

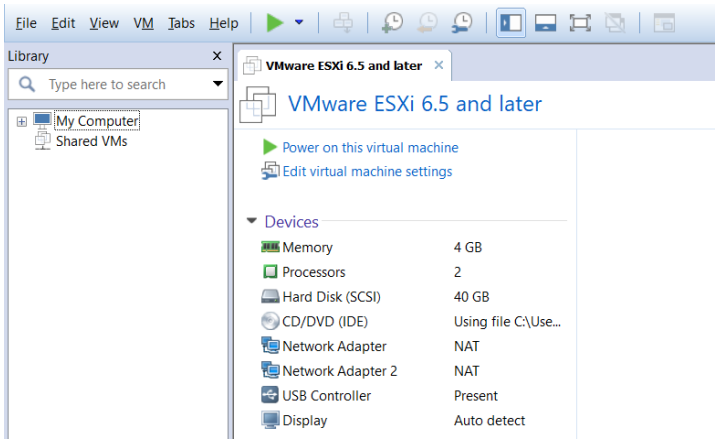


Figura 6-1 VMware Workstation (propia)

B Plataforma de virtualización

La configuración de la plataforma de virtualización se realizó con el asistente de instalación, con la configuración predeterminada y los siguientes datos.

Usuario: root Contraseña: ******** IPv4: static Ip:192.168.199.250 Subnet mask: 255.255.255.0 Puerta de enlace: 192.168.199.254 IPv6: none

Para poder acceder al hipervisor y con ello realizar configuraciones entre ellas crear, eliminar o revisar el estado de las máquinas virtuales alojadas en el servidor se requiere del uso de un navegador con soporte con HTML5. La dirección para poder entrar es la siguiente:

//192.168.199.250

Si se muestra en la pantalla un anuncio como el de la figura 6-2, descartar el mensaje de advertencia y acceder.

La conexión no es privada

Figura 6-2 Pantalla de conexión no privada (propia)

Se mostrará la pantalla para el inicio de sesión como en la figura 6-3.

Figura 6-3 Pantalla de inicio de sesión en VMware ESXi (propia)

Los datos de Acceso son los introducidos durante la instalación.

Usuario: root Contraseña: ********

Después de iniciar sesión carga la página principal como se muestra en la figura 6-4.

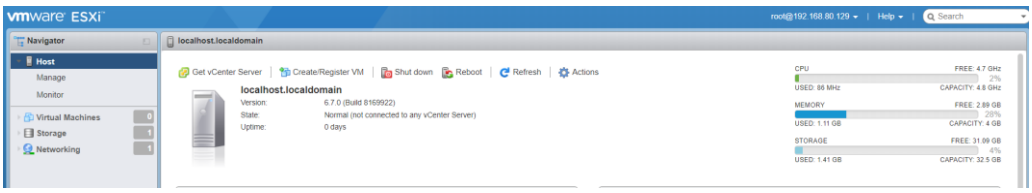


Figura 6-4 Pantalla inicial del host (propia)

Dentro se puede realizar configuraciones para la creación de MV (máquinas virtuales), supervisar el estado de las MV, conexiones con los switch's virtuales y conexiones a las salidas físicas si el usuario con el que se inició sesión tiene los permisos suficientes.

C Máquinas virtuales

En el apartado de la izquierda en la opción virtual machines nos permite acceder a las opciones de crear máquinas virtuales, modificarlas, supervisarlas entre otras. El apartado de máquinas virtuales se puede apreciar en la figura 6-5.

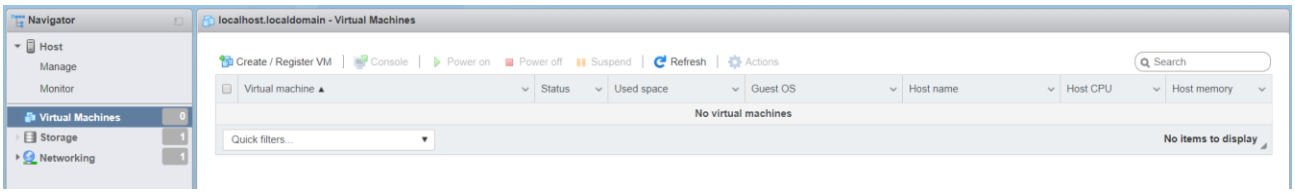


Figura 6-5 Apartado a máquinas virtuales (propia)

Creación de máquinas virtuales.

Para la creación de una máquina virtual hacer clic en Create/Register VM. Se mostrará una ventana como en la figura 6-6:

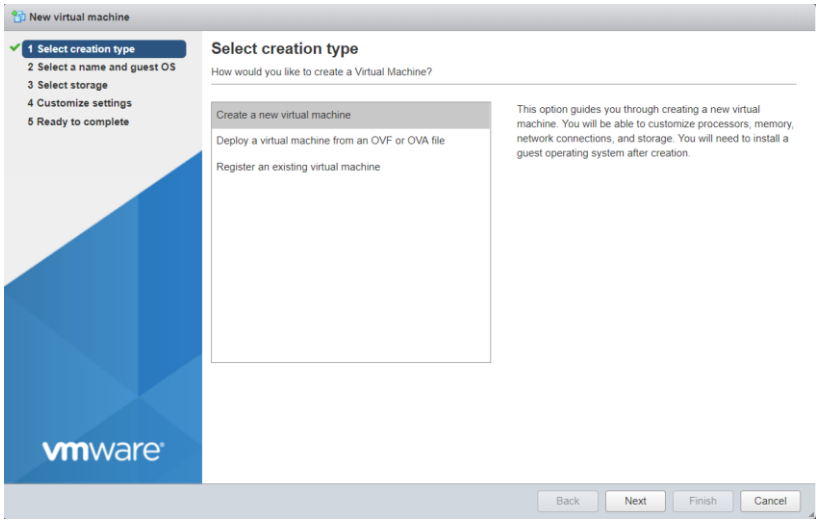


Figura 6-6 Ventana emergente de creación de máquina virtual (propia)

Seleccionar la opción deseada en el caso del firewall seleccionaremos Create a new virtual machine y hacer clic en Next.

En la ventana siguiente se introducirá la información correspondiente al sistema operativo. En el caso de pfSense 2.4 en un sistema operativo basado en FeeBSD 11 de arquitectura de 64 bits ver figura 6-7. Terminada la selección hacer clic en Next.

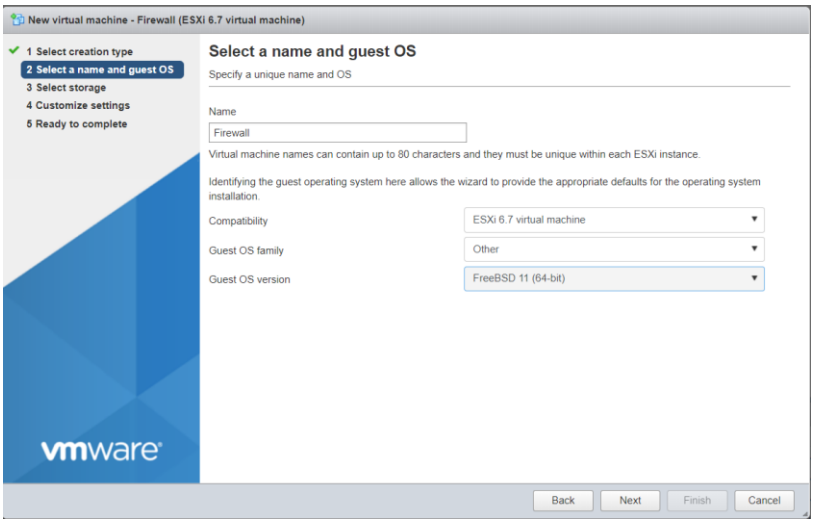


Figura 6-7 Selección de nombre y SO virtual (propia)

LA siguiente ventana trata sobre la ubicación donde se alojará la máquina virtual, si no se quiere realizar una configuración avanzada hacer clic en Next.(figura 6-8)

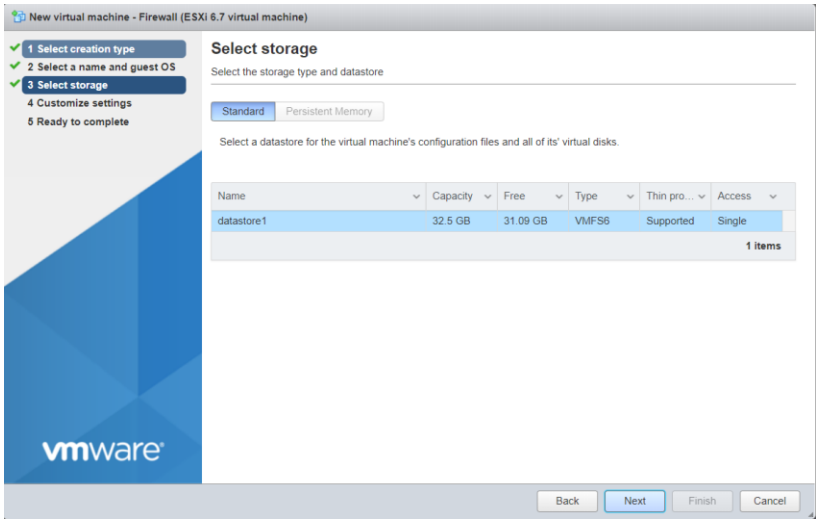


Figura 6-8 Selección de lugar de almacenamiento (propia)

En la pantalla siguiente se mostrará las especificaciones de los recursos con los que contará (RAM, HDD, CPU). pfSense no tiene requerimientos específicos ya que éstos dependen de los servicios a usar (usuarios activos, proxy, VPN, etc). Para más información sobre asignar recursos consultar (VMWare, s.f.)[1]. Para ejemplificar se tomará la siguiente configuración mostrada en la figura 6-9.

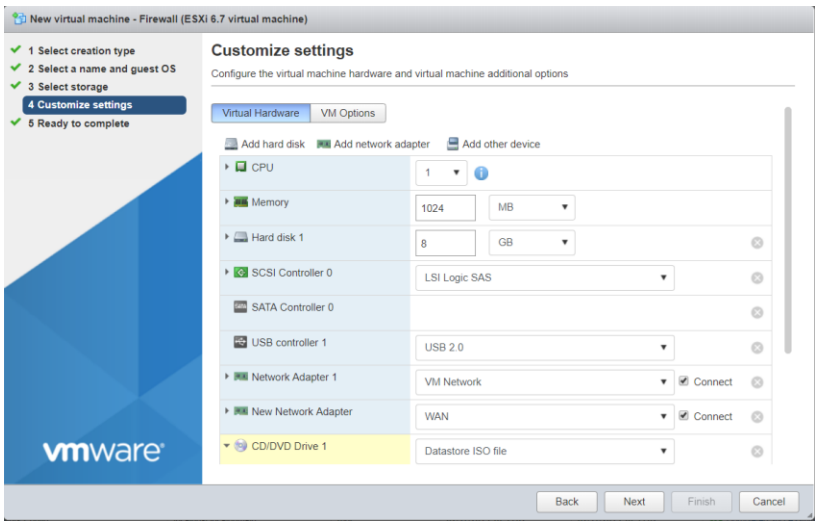


Figura 6-9 Selección de hardware virtual (propia)

Nota: El firewall requiere de dos conexiones a red una para la interfaz LAN y otra para WAN. VM Network representa a LAN.

Hacer clic en Next para revisar la configuración final ver figura 6.10. Hacer clic Finish si la configuración es la deseada o regresar con Back para realizar cambios.

[1] https://docs.vmware.com/es/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html

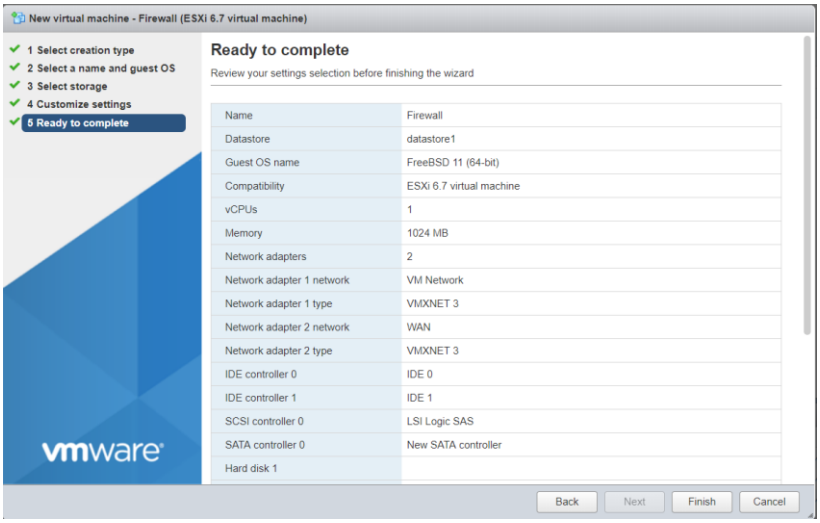


Figura 6-10 Pantalla resumen de configuración de MV (propia)

Al finalizar se mostrará la máquina virtual creada como se muestra en la figura 6-11.

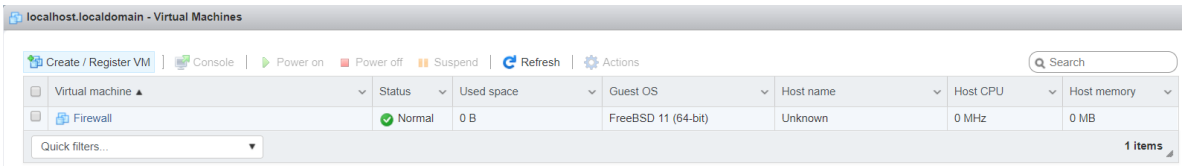


Figura 6-11 Nueva máquina virtual creada (propia)

Para que la máquina virtual inicie con el encendido del servidor, se requiere habilitar el autoinicio, se selecciona la máquina virtual y en Actions>Autostart hacer clic en Enable. (figura 6-12)

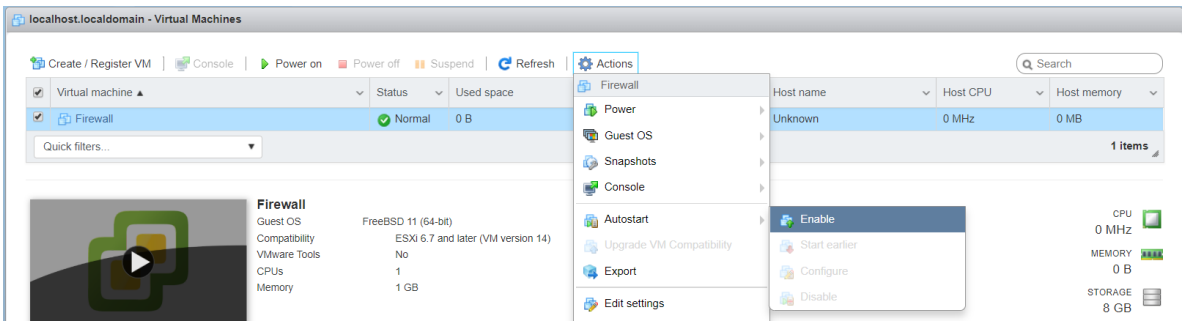


Figura 6-12 Habilitar autoinicio en MV (propia)

Se requiere habilitar la opción de autoinicio en el sistema, para ello en el menú de la izquierda seleccionar Host>Manage en el apartado de System seleccionar Autostart. (figura 6-13)

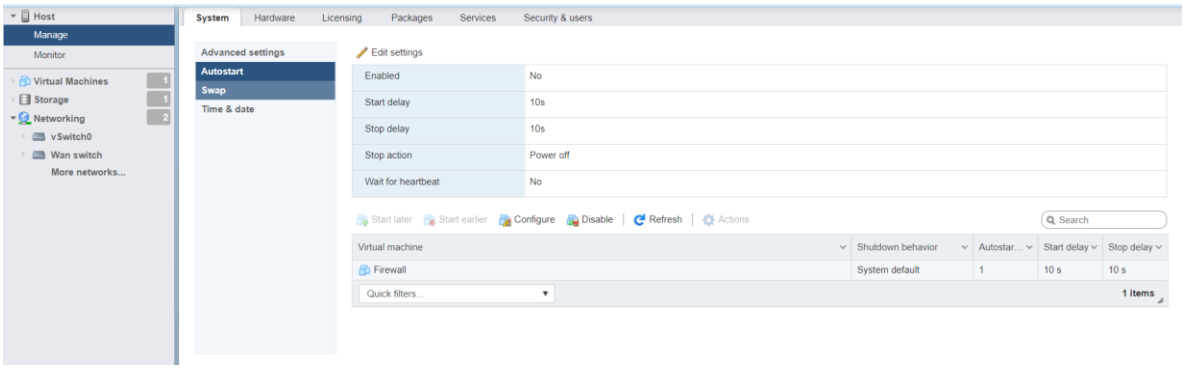


Figura 6-13 Configuración general de autoinicio (propia)

Seleccione Edit settings y seleccione la configuración como se muestra en la figura 6-14. Esto hará que el autoinicio tenga un retraso de 10 segundos y un retraso de 10 para el apagado.

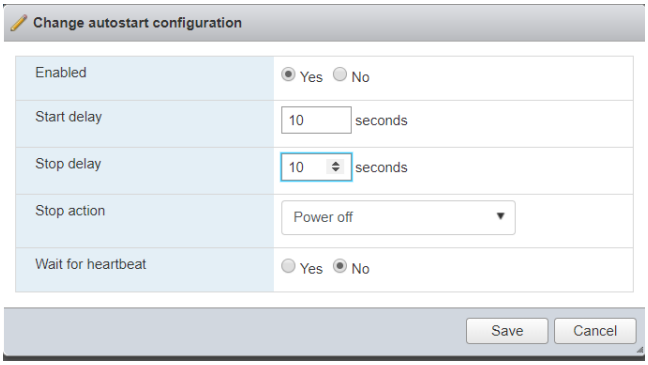


Figura 6-14 Tiempos de inicio y apagado de MV (propia)

Para hace uso de una máquina en el apartado de la izquierda seleccionar Virtual Machines y seleccionar la máquina virtual a usar. Encienda la máquina con la opción de Power on y haga clic sobre la pantalla para hacer uso de la máquina desde el navegador. (figura 6-15)

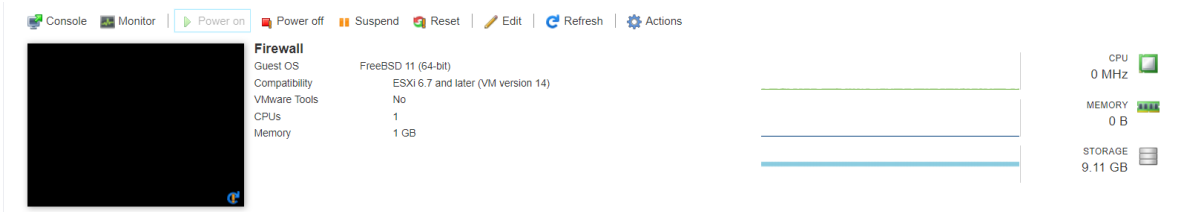


Figura 6-15 Encendido de MV (propia)

Switch virtual.

En éste se pueden realizar las configuraciones para la creación de switch's virtuales para realizar conexiones entre la MV con las interfaces de salida. Cada interfaz sólo se puede conectar a un switch virtual. El apartado de los switch's virtuales se puede ver en la figura 6-16.

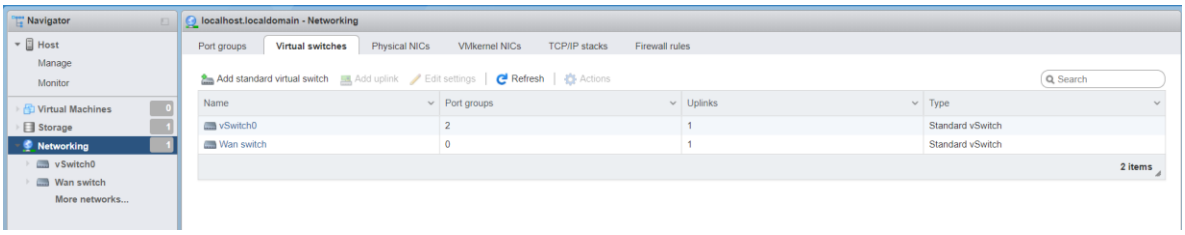


Figura 6-16 Apartado de switch's virtuales (propia)

Grupo de puertos.

Es donde se asignar la relación de los switch's, ejemplo: que switch está relacionado con la conexión Lan o Wan. Diferentes grupos se pueden asociar con un switch. El apartado de grupos se puede ver en la figura 6-17.

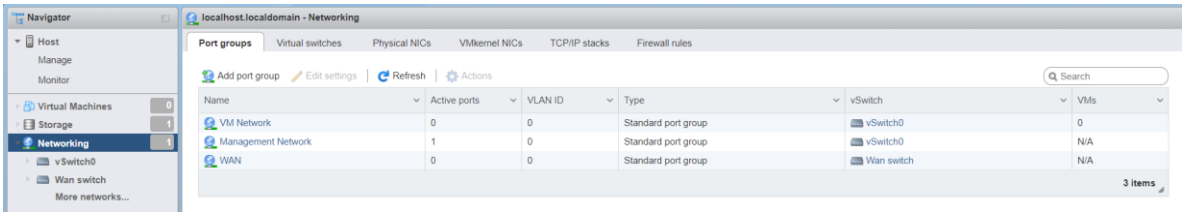


Figura 6-17 Apartado de grupos (propia)

D Firewall

El firewall tiene como núcleo pfSense que es una distribución basada en FreeBSD para el uso como Firewall. La configuración de pfSense se dio con las siguientes especificaciones.

Hostname y Domain: Default Primary DNS: 132.248.10.2 Secondary DNS: 132.248.204.1 Interfaz WAN: Puerto GB1 Etiqueta vmx1 Asignación IPv4: Static

Address: 132.248.54.199
Subnet mask: 255.255.255.0 => /24
Gateway: XXX.XXX.XXX.254
Asignación IPv6: none

Interfaz LAN: Puerto GB2
Etiqueta vmx0
Asignación IPv4: Static
Address: 192.168.199.254
Subnet mask: 255.255.255.0 => /24
Asignación IPv6: none

Interface WLAN:Puerto 1 netwok adapter card
Etiqueta vmx2
Asignación IPv4: Static
Address: 192.168.200.254
Subnet mask: 255.255.255.0 => /24
Asignación IPv6: none

Para el acceso se requiere del uso de un navegador con soporte con HTML5. La dirección para poder entrar es la siguiente:

```
//192.168.199.254
```

Si se muestra pantalla de advertencia como en la figura 6-2 descarta y acceder. Se mostrará la pantalla de inicio de sesión de pfSense como lo muestra la imagen 6-18.

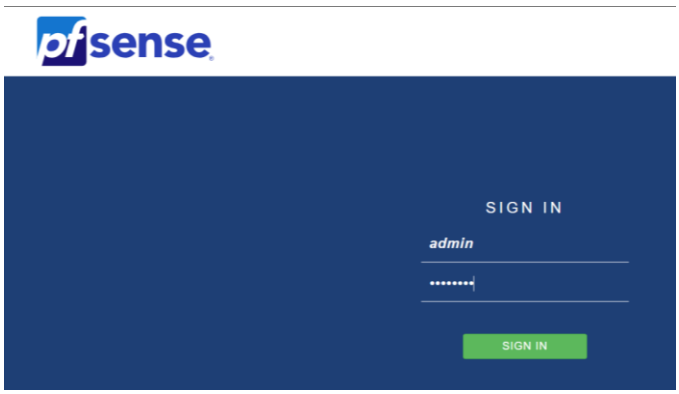


Figura 6-18 Pantalla de login pdSense (propia)

Los datos de Acceso son los siguientes:

```
Usuario: admin
Contraseña: ********
```

La contraseña por defecto es pfSense

Se mostrará el Dashboard donde se muestra principalmente la información del sistema y las interfaces. Para las configuraciones se hará uso de la barra de navegación. (figura 6-19)

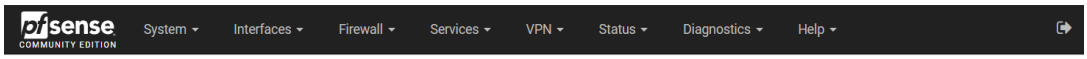


Figura 6-19 Barra de navegación (propia)

E Configuración de WAN y LAN.

Para acceder a las configuraciones de las interfaces despliegue en la barra de navegación la opción interfaces y seleccione la opción de lo que se quiera configurar o revisar. (figura 6-20)

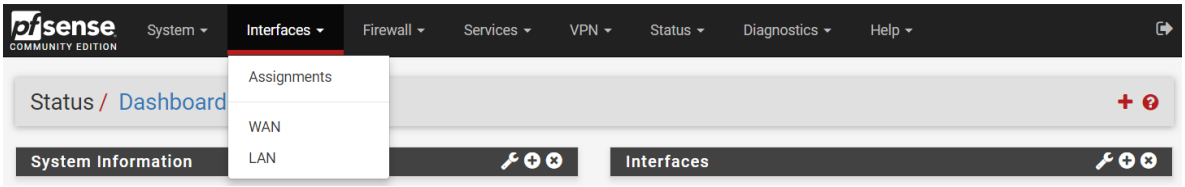


Figura 6-20 Menú de interfaces (propia)

Opción assignments.

Se puede acceder a las opciones de agregar una interfaz si se tiene una salida no habilitada o hacer uso de uno existente, también se puede eliminar una interfaz según sea el caso. (figura 6-21)

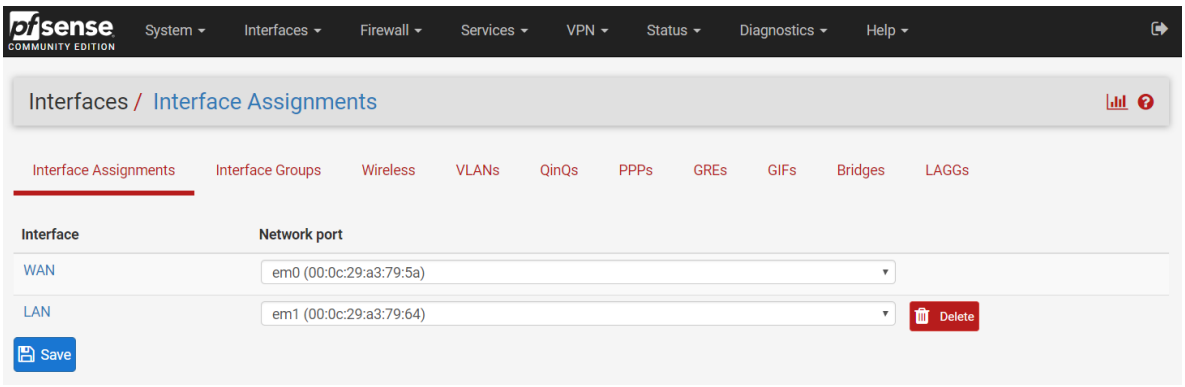


Figura 6-21 Apartado de asignación de interfaces (propia)

Opción WAN.

En este apartado se puede acceder a la configuración con la red al exterior, esta configuración es la que permite conectarse con la red troncal de la facultad. La configuración para que esto se pueda realizar es la siguiente.

IPv4 Configuration Type StaticIPv4 IPv4 Address XXX.XXX.XXX.199 /24 IPv4 Upstream Gateway > Add a new Gateway > Gateway IPv4 XXX.XXX.XXX.254

Una representación de la configuración es la mostrada en la figura 6-22.

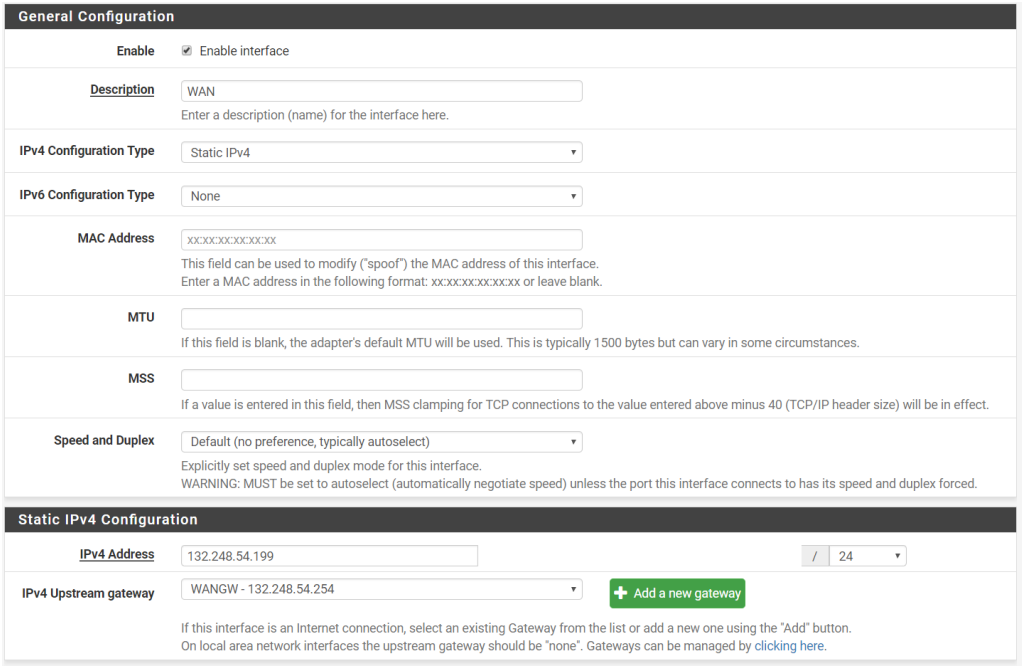


Figura 6-22 Configuración de red WAN (propia)

Opción LAN

En este apartado se puede acceder a la configuración con la IP del firewall en la LAN y es la que hace posible el acceso. La configuración es la siguiente:

IPv4 Configuration Type StaticIPv4

IPv4 Address 192.168.199.254 /24

Una representación de la configuración es la mostrada en la figura 6-23.

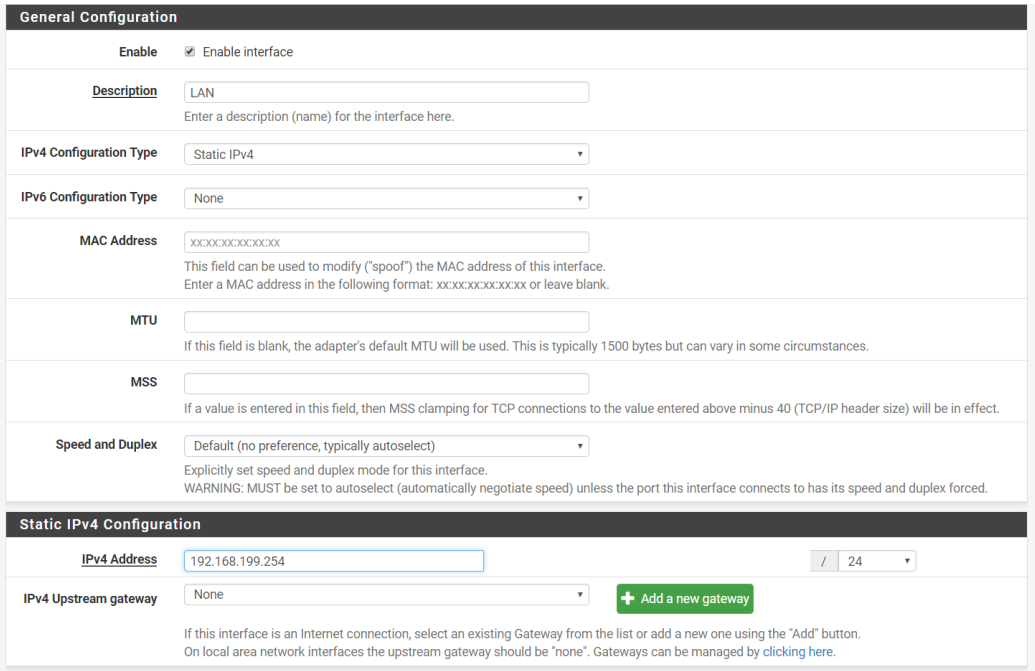


Figura 6-23 Configuración de red LAN (propia)

Las configuraciones de las interfaces se pueden realizar a través del hipervisor de VMware con el uso del terminal. PfSense posee un menú con diversas opciones como se puede ver en la figura 6-24.

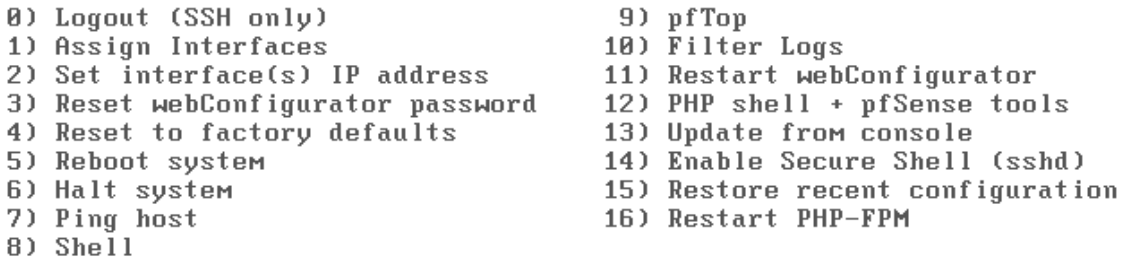


Figura 6-24 Menú de pfSense por terminal (propia)

Las opciones por usar son la numero 1 y 2 que corresponden a las anteriormente mostradas.

F Configuración de servidor DHCP.

El servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a los equipos que se encuentren configurados de forma predeterminada. Esta opción se encuentra habilitada para el uso de los alumnos que requieran conectarse a internet con un equipo propio y se les de permiso hacerlo sin necesidad que se tenga que configurar su máquina. La configuración se encuentra en el apartado de Services > DHCP Server. (figura 6-25)

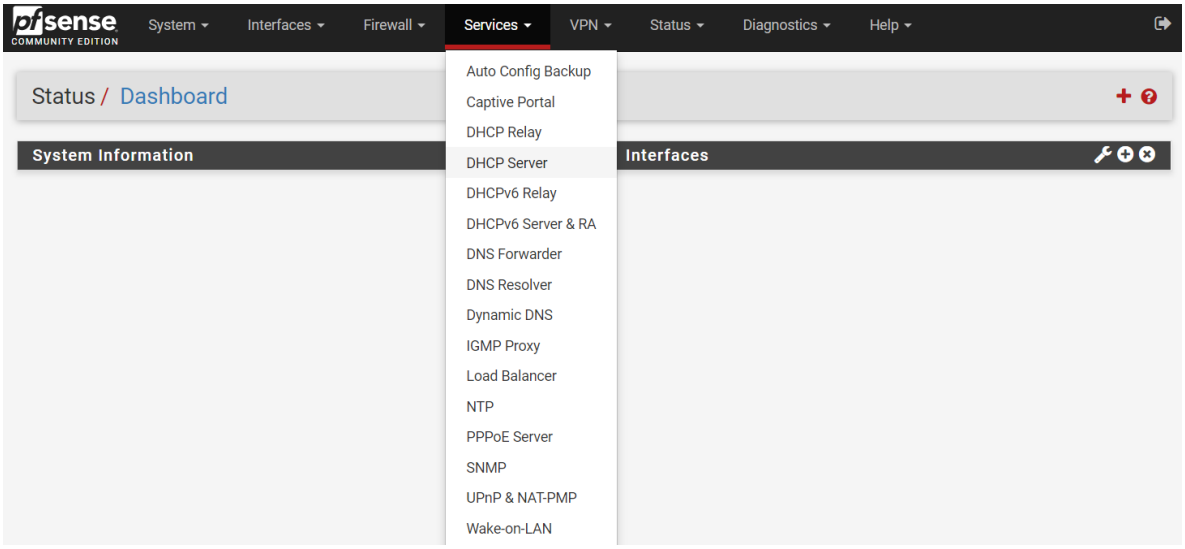


Figura 6-25 Apartado de servicios (propia)

Las opciones principales están relacionadas con el rango de direcciones, en este apartado se selecciona el rango de IP que se permite al servido DHCP asignar a los equipos, entre mayor sea el rango más equipos pueden conectarse.

El rango de direcciones es del 192.168.199.121-192.168.199.240.

NOTA: No utilizar el rango de direcciones de la 1 a 120 ya que éstas están asignadas a la configuración manual de los equipos respecto al nodo en que se conectan. No utilizar el rango 241 a 254 ya que se encuentran asignados a los diferentes servicios

La configuración de DNS en el servidor DHCP permite conectarse a internet se encuentra relacionada con los DNS, si no se tienen asignados los equipos externos al laboratorio (equipos personales) no pueden tener conexión a internet, pero si acceso a la red local. Por ejemplo:

1. Si no se le permite el uso de internet, pero requiere acceso a los archivos compartidos se borran los DNS y el alumno no podrá conectarse a internet, pero podrá hacer uso de carpetas compartidas.
2. Los alumnos requieren el uso de internet, se requiere que se tengan los DNS colocados. Si éstos no se encuentran el alumno no podrá conectarse a internet y se le mostrará una conexión limitada.

Borrar o colocar los DNS según sea el caso.

G Bloqueo de páginas web

Para bloquear el acceso a una página web en específico se realizará la siguiente configuración: Creación de un Alias: en el apartado de Firewall seleccionar Aliases seleccionar el botón Add. (figura 6-26)

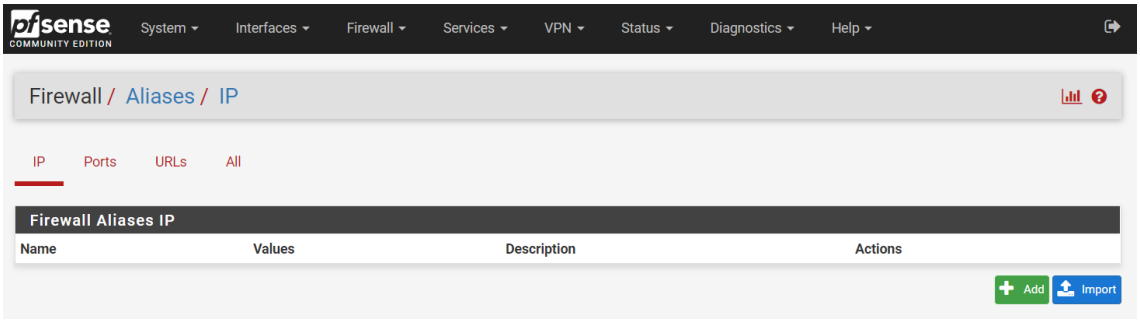


Figura 6-26 Alias creados (propia)

Se mostrará una pantalla como en la figura 6-27 en esta se muestra la configuración para Facebook.

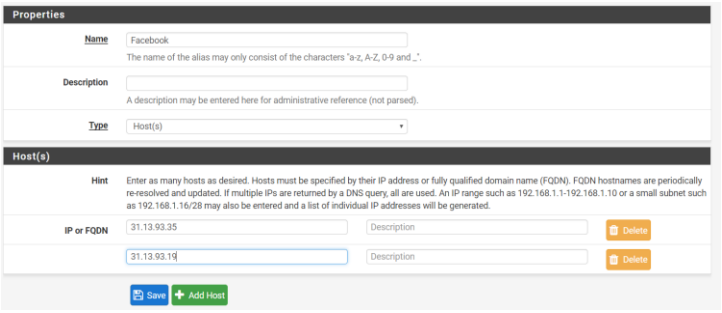


Figura 6-27 Configuración de alias Facebook (propia)

Descripción:

- En nombre es el identificador de nuestro alias ejemplo: Facebook, YouTube, etc.
- En Host se agregarán las IP a las que corresponden los sitios web.

Para obtener estas direcciones con la ayuda de la consola de Windows o un terminal en Linux usaremos la herramienta nslookup para obtener la dirección de los sitios web mencionados. Ejemplo:

```
nslookup Facebook.com
nslookup Facebook.es
```

Para que el bloqueo funcione se deben de colocar las IP para las diferentes direcciones correspondientes al sitio Web. En las figuras 6-28 y 6-29 muestran el uso de nslookup en cmd y terminal respectivamente.

Figura 6-28 nslookup en CMD de Windows (propia)

```
[2.4.4-RELEASE][root@pfSense.localdomain]/root: nslookup facebook.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.70.36
Name:   facebook.com
Address: 2a03:2880:f10d:83:face:b00c:0:25de
```

Figura 6-29 nslookup en terminal de pfSense (propia)

Para agregar las IP hacer clic en el botón Add Host y guardar los cambios con el botón Save.

Creación de reglas.

En la barra de navegación seleccionar Firewall>Rules. En el apartado de LAN seleccionar el botón Add (6-30)

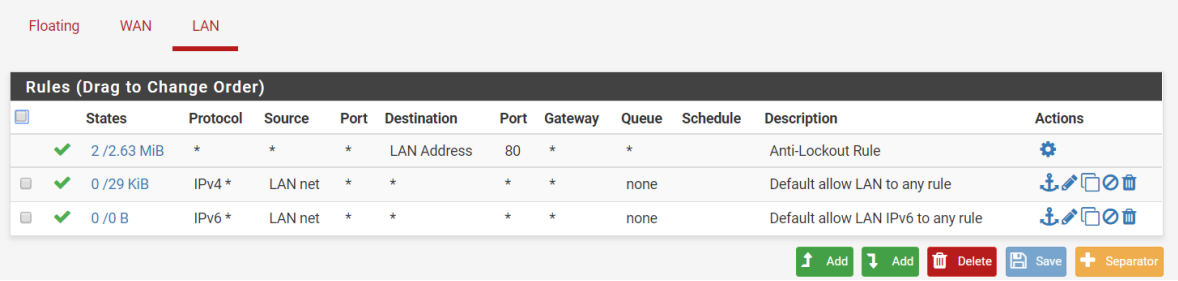


Figura 6-30 Reglas para el apartado LAN (propia)

Se mostrará la pantalla para la creación de una regla como la figura 6-31.

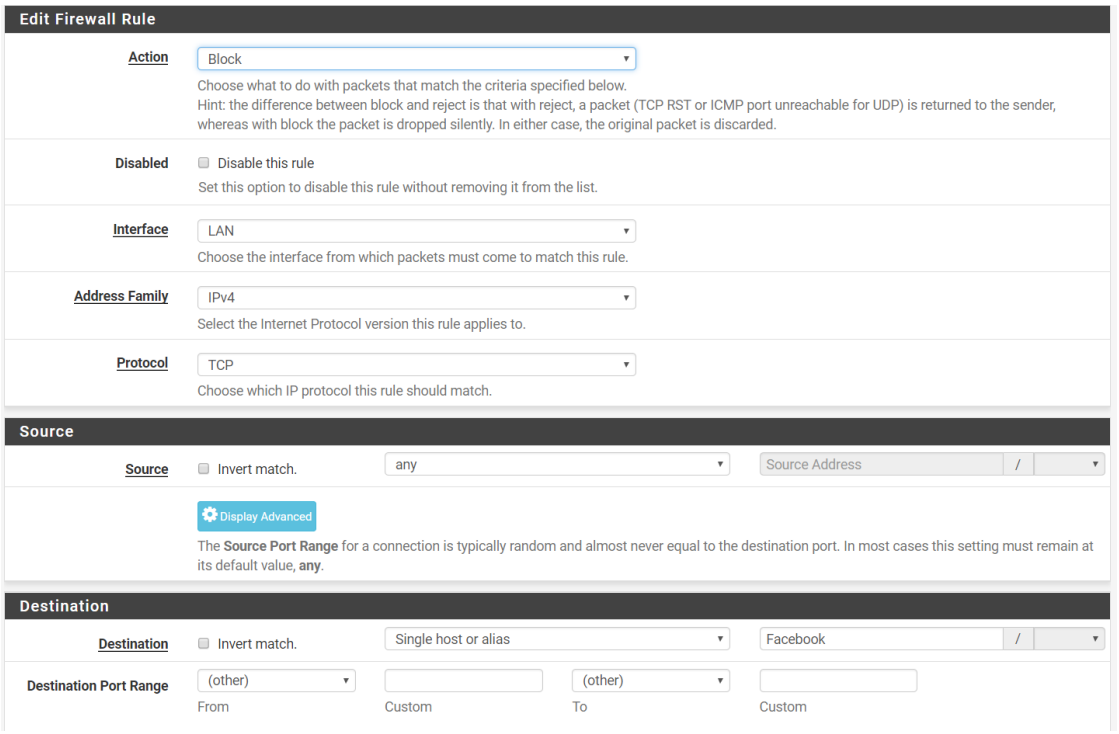


Figura 6-31 Configuración de nueva regla (propia)

En donde:

- Action: seleccionaremos *Block* para bloquear la página.
- Destination: seleccionaremos *Single host or alias* e introduciremos el alias que colocamos para la página web que queríamos bloquear nuestro ejemplo Facebook.

Guardar cambios con el botón Save y aplicar cambios para efectuar el bloqueo a la página web.

Índice de figuras

Índice de tablas

Referencias

568 A 568 B. (s.f.). Obtenido de Free png: https://dlpng.com/png/1388863

Callata Olivera, S. Y. (2016). Metodología hibrida para el diseño de enlaces de comunicación inalámbrica en los barrios Vallecito. Puno, Perú.

Delta. (1 de 3 de 2019). Obtenido de Cable de par trenzado UTP/K5/305M/MTC METACON: https://shopdelta.eu/cable-de-par-trenzado-utpk5305mmtc-metacon_l6_p8859.html

Domínguez Sanjuán, M. (2018). *Virtualización mediante entornos Open Source.* Alacant, España.

Facultad de Ingeniería. (2019). Obtenido de Facultad de Ingeniería / Misión y Visión: http://www.ingenieria.unam.mx/nuestra_facultad/organigrama.php

Fajardo Guatarasma, M. D., & Marcano, A. V. (2012). Metodología mixta para el diseño de enlaces de comunicación. Caso de estudio empresa. *10th LACCEI Latin American and Caribbean Conference (LACCEI'2012), Engineering for a Smart Planet, Innovation, Information.* Panama.

Hernández Sánchez, L. (2014). *Buenas prácticas para la implementación de la seguridad en un centro de cómputo.* Mexico D.F.

Jiménez Moreno, H., & Rojas Arteaga, I. K. (2015). *Praxis de Redes y Seguridad.* Ciudad Universitaria, México.

Joskowicz, J. (2006). Cableado Estructurado. Montevideo, Uruguay.

Joskowicz, J. (2007). Redes de datos. Montevideo, Uruguay.

Medios de Transmisión de Cobre. (s.f.). Obtenido de Unidad de Apoyo para el Aprendizaje: https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/863/mod_resource/content/1/contenido/index.html

Oppenheimer, P. (2011). *Top-Down Network Design.* Indianapolis: Cisco Press.

Portal DICyG. (2019). Obtenido de Organigrama: http://dicyg.fi-c.unam.mx:8080/Site/quienes-somos/orgnigrama

Serrano Macías, G. (2014). *Implemnetación de servicios de red en un hospital utilizando software libre.* Ciudad Universitaria.

Servicio de red. (s.f.). Obtenido de Wikipedia, la enciclopedia libre: https://es.wikipedia.org/wiki/Servicio_de_red

Topología de red. (2004). Obtenido de Wikimedia commons: https://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

VMWare. (s.f.). *Configurar hardware de la máquina virtual*. Obtenido de https://docs.vmware.com/es/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html