IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESIS COLECTIVA

Que como prueba escrita de su Examen Profesional para obtener el Título de **INGENIERO EN COMPUTACIÓN** deberán desarrollar los C.C.:

ALBERTO MARTÍNEZ NAVA
JOSÉ JAIME SALINAS HERNÁNDEZ

"FILTRADO DE CONTENIDO WEB"

Dado que la información que se genera y almacena dentro de esta red es de único interés para los usuarios de la misma, la red deberá estar aislada para evitar las intrusiones desde el exterior, pero no obstante se podrá acceder a los servicios de Internet. Es por esto que se debe definir y aplicar correctamente las políticas de red en cuestión al filtrado de contenido permitiendo a la empresa ser más productiva y efectiva en el negocio.

Capitulado:

CAPITULO I.-	INTRODUCCIÓN A LAS REDES.
CAPÍTULO II.-	SEGURIDAD EN REDES.
CAPÍTULO III.-	FIREWALLS.
CAPÍTULO IV.-	FILTRADO DE CONTENIDO WEB.
CAPÍTULO V.-	IMPLEMENTACIÓN DE FILTRADO DE CONTENIDO WEB

Ciudad de México, a 04 de abril de 2019.

M. EN C. RAYMUNDO SANTANA ALQUICIRA
PRIMER ASESOR

M. EN C. HÉCTOR BECERRIL MENDOZA
SEGUNDO ASESOR

M. EN C. JOSÉ ANTONIO LOAIZA BRITO
JEFE DE LA CARRERA DE I.C.

DR. EUSEBIO RICARDEZ VÁZQUEZ
SUBDIRECTOR ACADÉMICO INTERINO

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN
SUBDIRECCIÓN ACADÉMICA
OFICINA DE TITULACIÓN PROFESIONAL

CARTA DE AUTORIZACIÓN DE USO DE OBRA

En la Ciudad de México, a **04** de **abril** del **2019**, los que suscriben **ALBERTO MARTÍNEZ NAVA y JOSÉ JAIME SALINAS HERNÁNDEZ**, alumnos de la carrera de **Ingeniería en Computación**, con número de registro **R-019/19**, egresados de la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacan, manifestamos que somos los autores intelectuales del presente trabajo de **Tesis Colectiva,** bajo la asesoría del **M. EN C. RAYMUNDO SANTANA ALQUICIRA y del M. EN C. HÉCTOR BECERRIL MENDOZA,** y autorizamos el uso del trabajo titulado **"FILTRADO DE CONTENIDO WEB"** al Instituto Politécnico Nacional, para su difusión con fines académicos y de investigación.

Los usuarios de la información no deberán reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso de los (las) autores (as) y/ o asesor(es) del trabajo. Este puede ser obtenido escribiendo a las siguientes direcciones de correo: readiseck@gmail.com, josejaime88@hotmail.com, si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

ALBERTO MARTÍNEZ NAVA
Nombre y firma del alumno

José Jaime Salinas Hernández
Nombre y firma del alumno

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA UNIDAD "CULHUACAN"

FILTRADO DE CONTENIDO WEB.

T E S I S

PARA OBTENER EL TÍTULO DE:

INGENÍERO EN COMPUTACIÓN.

ALUMNOS:

MARTÍNEZ NAVA ALBERTO.

SALINAS HERNÁNDEZ JOSÉ JAIME.

ASESORES:

M. EN C. RAYMUNDO SANTANA ALQUICIRA.

M. EN C. HÉCTOR BECERRIL MENDOZA.

CIUDAD DE MÉXICO **JUNIO 2019**

FILTRADO DE CONTENIDO WEB

ÍNDICE

AGRADECIMIENTOS 9

INTRODUCCIÓN 10

OBJETIVO 11

ALCANCE 11

JUSTIFICACIÓN 11

PROBLEMÁTICA 11

CAPÍTULO 1 INTRODUCCIÓN A LAS REDES

1.1 ¿QUÉ ES UNA RED? 12

1.2 MODELO OSI 13

1.2.1 CAPAS DEL MODELO OSI 14

1.3 TIPOS DE REDES 17

1.3.1 RED DE COBERTURA 17

1.3.1.1 PAN 18

1.3.1.2 LAN 18

1.3.1.3 CAN 18

1.3.1.4 MAN 19

1.3.1.5 WAN 19

1.3.1.6 SAN 20

1.3.1.7 RED VIRTUAL DE AREA LOCAL (VLAN) 21

1.3.2 RED DE SERVICIO 21

1.3.2.1 PÚBLICAS 21

1.3.2.2 PRIVADAS 22

1.3.3 RED POR CONEXIÓN 23

1.3.3.1 ORIENTADAS 23

1.3.3.2 NO ORIENTADAS 25

1.3.4 RED DE SISTEMA DE PROCESAMIENTO DE LA INFORMACIÓN 27

1.3.4.1 PUNTO A PUNTO (P2P) 27

1.3.4.2 MAESTRO ESCLAVO 27

1.3.4.3 CLIENTE SERVIDOR 27
1.4 TOPOLOGIAS DE RED 29
1.4.1 FÍSICAS Y LÓGICAS 30
1.4.2 TOPOLOGÍA LINEAL O EN BUS 31
1.4.3 TOPOLOGÍA DE ESTRELLA 32
1.4.4 TOPOLOGÍA DE ANILLO 33
1.4.5 TOPOLOGÍA DE MALLA 34
1.5 TIPOS DE ENLACES 35
1.5.1 PUNTO A PUNTO 35
1.5.2 PUNTO A MULTIPUNTO 36
1.6 INTERCONECTIVIDAD 36
1.6.1 EQUIPOS DE INTERCONEXION 37
1.6.1.1 REPETIDOR 38
1.6.1.2 CONCENTRADOR (HUB) 38
1.6.1.3 PUENTE 39
1.6.1.4 CONMUTADOR DE PAQUETE (SWITCH) 39
1.6.1.5 ENRUTADOR (ROUTER) 40
1.6.1.6 GATEWAY O PROXY 40
1.6.1.7 PUNTO DE ACCESO (ACCES POINT) 41
1.6.1.8 DSU / CSU (MODEM DIGITAL) 41
1.7 PROTOCOLOS DE COMUNICACIONES 42
1.7.1 TCP IP 43
1.7.2 FTP 44
1.7.3 UDP 44
1.7.4 ICMP 45
1.7.5 SNMP 45
1.8 SERVIDORES 46
1.8.1 SERVIDOR WEB 46
1.8.2 SERVIDOR DHCP 46
1.8.3 SERVIDOR DNS 47

CAPÍTULO 2 SEGURIDAD EN REDES

2.1 ¿QUÉ ES SEGURIDAD EN REDES? 48
2.2 AMENAZAS EN INTERNET 50
2.3 ATAQUES 50
2.3.1 ATAQUES DE INTROMISIÓN 51
2.3.2 ATAQUES DE ESPIONAJE 51
2.3.3 ATAQUES DE MODIFICACIÓN 51
2.3.4 ATAQUES DE NEGACION DE SERVICIO 52
2.3.5 ATAQUES DE SUPLANTACIÓN 52
2.3.6 HACKER 53
2.3.7 CRACKER 53
2.3.8 VIRUS 54
2.3.9 SNIFFER 54
2.3.10 SPOOFING 55
2.3.10.1 TIPOS DE SPOOFING 55
2.3.10.1.1 IP SPOOFING 55
2.3.10.1.2 ARP SPOOFING 55
2.3.10.1.3 DNS SPOOFING 56
2.3.10.1.4 WEB SPOOFING 56
2.3.10.1.5 MAIL SPOOFING 56
2.4 SOLUCIONES DE SEGURIDAD EN REDES 57
2.4.1 PRIVACIDAD 57
2.4.2 CONFIDENCIALIDAD 57
2.4.3 INTEGRIDAD 57
2.4.4 DISPONIBILIDAD 57
2.4.5 AUTENTICACIÓN 57
2.4.6 AUDITORÍA 58
2.5 SPAM EN DIFERENTES MEDIOS 58
2.5.1 SPAM EN PUBLICACIONES 59
2.5.2 SPAM EN CORREO ELECTRÓNICO 59

2.5.3 SPAM EN FOROS 59
2.5.4 SPAM EN REDES SOCIALES 60
2.5.5 SPAM POR TELEFONÍA IP 60
2.5.6 SPAN EN MENSAJERIA DE JUEGOS EN LÍNEA 60
2.6 TÉCNICAS DE SPAM 61
2.6.1 OBTENCIÓN DE DIRECCIONES DE CORREO 61
2.6.2 ENTRADA ILEGAL EN SERVIDORES 61
2.6.3 ENVIO DE LOS MENSAJES 61
2.6.4 VERIFICACIÓN DE RECEPCIÓN 62
2.6.5 TROYANOS Y ORDENADORES ZOMBIS 62
2.6.6 SERVIDORES DE CORREO MAL CONFIGURADOS 62
2.6.7 PRECAUCIONES PARA EVITAR CORREO BASURA 63
2.7 ADMINISTRACIÓN DE SERVICIOS EN INTERNET 65
2.7.1 CORREO ELECTRÓNICO 65
2.7.2 LISTAS DE CORREO ELECTRONICO 65
2.7.3 WORLD WIDE WEB 66
2.7.4 FTP 66
2.7.5 NEWS 66
2.7.6 VIDEO CONFERENCIAS 66
2.7.7 TELNET 66
CAPÍTULO 3 FIREWALLS
3.1 ¿QUÉ ES UN FIREWALL? 67
3.1.1 PRIMERA GENERACIÓN FIREWALLS DE FILTRADO 67
3.1.2 SEGUNDA GENERACIÓN FIREWALLS DE ESTADO 68
3.1.3 TERCERA GENERACIÓN FIREWALLS DE APLICACIÓN 69
3.2 ¿QUÉ OFRECE UN FIREWALL? 69
3.2.1 ¿QUÉ PUEDE HACER UN FIREWALL PARA PROTEGER LA RED? 70
3.2.2 ¿QUÉ NO PUEDE HACER UN FIREWALL PARA PROTEGER LA RED? 70

3.3 OBJETIVO DE UN FIREWALL 72
3.4 COMO FUNCIONA UN FIREWALL 73
3.4.1 ¿CÓMO ES EL ACCESO DESDE EL EXTERIOR? 74
3.4.2 ¿CÓMO ES EL ACCESO DESDE EL INTERIOR 74
3.5 COMPONENTES DE LOS FIREWALLS 74
3.5.1 POLÍTICAS DE SEGURIDAD 75
3.5.2 REGISTRO DE OPERACIONES 75
3.5.3 INTERFACES 75
3.5.4 AUTENTICACIÓN DE USUARIOS 76
3.5.5 CORRELACIÓN DE DIRECCIONES 77
3.5.6 RESTRICCIONES DE DÍA Y HORA 78
3.5.7 CONTROL DE CARGA 78
3.5.8 CANALIZACIÓN 78
3.6 VENTAJAS DE LOS FIREWALLS 79
3.7 TIPOS DE FIREWALLS 80
3.7.1 FILTRADOR DE PAQUETES (PACKET FILTER) 80
3.7.2 SERVIDOR PROXY A NIVEL DE APLICACIÓN 81
3.7.3 PASARELAS A NIVEL DE RED 82
3.7.4 FIREWALLS CON ZONA DESMILITARIZADA (DMZ) 82
3.8 ALGUNAS HERRAMIENTAS DEL HACKER EN CONTRA DEL FIREWALL 83
3.9 IMPLEMENTACIÓN Y CONFIGURACION DE FIREWALLS 83
CAPÍTULO 4 FILTRADO DE CONTENIDO WEB
4.1 ¿QUÉ ES FILTRADO DE CONTENIDO WEB? 84
4.2 ¿COMO FUNCIONAN? 85
4.3 HERRAMIENTAS DE CONTROL DE ACCESOS Y MONITOREO 85
4.3.1 LISTAS POSITIVAS Y NEGATIVAS 86
4.3.2 RECONOCIMIENTO DE PALABRAS CLAVE 86
4.3.3 ANALISIS SEMANTICO 87
4.3.4 MONITOREO 87

4.3.5 HERRAMIENTAS DE CONTROL DE ACCESO EN EL POVEEDOR DE INTERNET 87
4.3.6 CLASIFICACIÓN MEDIANTE ETIQUETAS PICS 87
4.4 LOS FIREWALLS Y LOS METODOS DE FILTRADO 88
CAPÍTULO 5 IMPLEMENTACION DE FILTRADO DE CONTENIDO WEB 89
5.1 ESTADO ACTUAL 89
5.2 PROBLEMATICA 90
5.3 SOLUCIÓN 91
5.4 PROCEDIMIENTO DE CONFIGURACIONES 95
5.5 PRUEBAS DE FILTRADO DE CONTENIDO POR GRUPOS (VLAN) 98
5.5.1 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE DIRECCIÓN. 98
5.5.2 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE GERENTES. 101
5.5.3 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE OPERADORES. 104
5.5.3 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE VISITAS. 107
CONLUSIONES 110
ANEXOS 111
GLOSARIO 121

Tabla de contenido

Ilustración 1.1 Topología de bus	31
Ilustración 1.2 Topología de estrella	32
Ilustración 1.3 Topología en anillo	33
Ilustración 1.4 Topología en malla completa	34
Ilustración 1.5 Punto a punto	35
Ilustración 1.6 Punto a multipunto	36
Ilustración 5.1 Direccionamiento IP	92
Ilustración 5.2 Políticas de permisos	93
Ilustración 5.3 Expresiones regulars	94
Ilustración 5.4 Restricción media	98
Ilustración 5.5 Restricción pornografía	98
Ilustración 5.6 Restricción descargas	99
Ilustración 5.7 Restricción juegos	99
Ilustración 5.8 Restricción redes sociales	100
Ilustración 5.9 Restricción media	101
Ilustración 5.10 Restricción pornografía	101
Ilustración 5.11 Restricción descargas	102
Ilustración 5.12 Restricción juegos	102
Ilustración 5.13 Restricción redes sociales	103
Ilustración 5.14 Restricción media	104

Ilustración 5.15 Restricción pornografía 104

Ilustración 5.16 Restricción descargas 105

Ilustración 5.17 Restricción juegos 105

Ilustración 5.18 Restricción redes sociales 106

Ilustración 5.19 Restricción media 107

Ilustración 5.20 Restricción pornografía 107

Ilustración 5.21 Restricción descargas 108

Ilustración 5.22 Restricción juegos 108

Ilustración 5.23 Restricción redes sociales 109

AGRADECIMIENTOS:

Le agradezco a mis padres Jaime Salinas López y María del Carmen Hernández Delgado por la paciencia y apoyo brindado durante todos estos años. Por su ayuda durante toda mi etapa escolar, por el esfuerzo que realizaron para que esto concluyera de manera satisfactoria.

Agradezco a mis hermanas (Norma, Ana y Tere) por siempre estar pendientes y apoyándome incondicionalmente.

A mis asesores que me apoyaron durante esta parte final y más importante de mi carrera para poder obtener mi título profesional

José Jaime Salinas Hernández.

Dedico esta tesis, primero que nada, a mis padres Alberto Martínez Serrano y María Guadalupe Nava Ramírez quienes siempre han estado para mí en todo momento, por apoyarme, aconsejarme y sobre todo a nunca rendirme y luchar por ser una gran persona y un gran profesionista.

También quiero dedicar y agradecer a mi esposa Sara Isabel, quien siempre me ha dado su apoyo incondicional en todo momento, a mi hijo Sael quien es el motor principal de mi vida y quien me hace luchar y seguir adelante siempre.

Quiero agradecer a Dios por darme a los mejores padres, a la mejor esposa y al mejor hijo, gracias a todos ustedes por apoyarme, amarme y sobre todo siempre estar conmigo.

Alberto Martínez Nava.

INTRODUCCIÓN:

En la actualidad todos tenemos acceso a internet, es una herramienta de bastante ayuda en todos los sentidos, nos apoya a realizar tareas, ayuda a encontrar muchas maneras de resolver un problema, nos conecta con cualquier persona en cualquier parte del mundo, nos ayuda a investigar de cualquier tema que nos interese.

Cualquier persona con acceso a internet es capaz de subir cualquier información sea o no verídica la información que está subiendo.
Nos mantiene actualizados en tiempo real de los acontecimientos locales y alrededor del mundo.

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este magnífico mundo.

En la sociedad de hoy en día, el acceso a cualquier clase de información se ve facilitado por diferentes tecnologías de conexión, con costos muy accesibles, que permiten interactuar local o remotamente con diferentes centros de cómputos. Sin embargo, este acceso instantáneo a la información trae consigo muchas dificultades en cuanto a la seguridad y privacidad de la información de una organización.

Por otro lado el uso indebido de esta herramienta (internet) puede llegar a provocar problemas en muchos sentidos, por este motivo, los administradores de red han tenido la necesidad de crear políticas de seguridad las cuales consisten en realizar conexiones seguras, enviar y recibir información, así mismo de mantener un control en la red así como filtrar accesos e información, pensando en un ámbito laboral, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red y protegerse contra la exportación privada de información.

Una herramienta para poder tener mayor rendimiento de los trabajadores dentro de una red, es limitarle el contenido de internet, para evitar distracciones y se pueda obtener un mayor aprovechamiento del tiempo laboral, es precisamente en este punto donde se basa esta investigación ya que se pretende dar a conocer una de las herramientas para la restricción de algunos sitios web de los equipos de cómputo cuando se conectan a Internet, a esto se le conoce como filtrado de contenido.

OBJETIVO.

Implementar mediante un firewall políticas de filtrado de contenido en la red para restringir acceso a sitios no deseados que impiden que los trabajadores sean más productivos.

ALCANCE.

Este trabajo pretende aplicar las configuraciones de las políticas de filtrado de contenido en un firewall elegido.

JUSTIFICACIÓN.

Dado que la información que se genera, maneja y almacena dentro de esta red es de único interés para los usuarios de la misma, la red deberá estar aislada para evitar las intrusiones desde el exterior, pero no obstante se podrá acceder a los servicios de Internet. Es por esto se deben definir y aplicar correctamente las políticas de red en cuestión al filtrado de contenido permitiendo a la empresa ser más productiva y efectiva en el negocio.

PROBLEMÁTICA.

Se ha encontrado que los usuarios en horas laborables están en páginas que no corresponden a su función como: Facebook, juegos, pornografía, por lo cual tiene impacto en la entrega de resultados en proyectos se están retrasando, se genera más trabajo, los costos aumentan.

CAPÍTULO 1. INTRODUCCIÓN A REDES.

1.1 ¿QUÉ ES UNA RED?.

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.

La estructura y el modo de funcionamiento de las redes informáticas están definidos en varios estándares, siendo el más extendido de todos, el modelo TCP/IP, basado en el modelo de referencia o teórico OSI.

DISPOSITIVOS.

Los dispositivos conectados a una red informática pueden clasificarse en dos tipos: los que gestionan el acceso y las comunicaciones en una red (dispositivos de red), como módem, router, switch, access point, bridge, etc.; y los que se conectan para utilizarla (dispositivos de usuario final), como computadora, notebook, Tablet, teléfono celular, impresora, televisor inteligente, consola de videojuegos, etc.

Los que utilizan una red, a su vez, pueden cumplir dos roles (clasificación de redes por relación funcional): servidor, en donde el dispositivo brinda un servicio para todo aquel que quiera consumirlo; o cliente, en donde el dispositivo consume uno o varios servicios de uno o varios servidores. Este tipo de arquitectura de red se denomina cliente/ servidor.

MEDIO.

El medio es la conexión que hace posible que los dispositivos se relacionen entre sí. Los medios de comunicación pueden clasificarse por tipo de conexión como guiados o dirigidos, en donde se encuentran: el cable coaxial, el cable de par trenzado (UTP/STP) y la fibra óptica; y no guiados, en donde se encuentran las ondas de radio (Wi-Fi y Bluetooth), las infrarrojas y las microondas. Los medios guiados son aquellos conformados por cables, en tanto que los no guiados son inalámbricos.

INFORMACIÓN.

Comprende todo elemento intercambiado entre dispositivos, tanto de gestión de acceso y comunicación, como de usuario final (texto, hipertexto, imágenes, música, video, etc.).

RECURSOS.

Un recurso es todo aquello que un dispositivo le solicita a la red, y que puede ser identificado y accedido directamente. Puede tratarse de un archivo compartido en otra computadora dentro de la red, un servicio que se desea consumir, una impresora a través de la cual se quiere imprimir un documento, información, espacio en disco duro, tiempo de procesamiento, etc.

Si nos conectamos a una red, por ejemplo, para solicitar un archivo que no podemos identificar y acceder directamente, tendremos que consumir un servicio que identifique y acceda a él por nosotros. Existen servicios de streaming de video (webs en donde podemos ver videos online, como YouTube), de streaming de audio (alguna radio en Internet), servicios de aplicación (como Google Docs.), y otros. En general, los dispositivos que brindan servicios se denominan servidores.

1.2 MODELO OSI.

El modelo de interconexión de sistemas abiertos más conocido como “modelo OSI”, (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization.

Es un estándar desarrollado en 1980 por la ISO, una federación global de organizaciones que representa aproximadamente a 130 países. El núcleo de este estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan desmarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo, se usa en la enseñanza como una manera de mostrar cómo puede estructurarse una «pila» de protocolos de comunicaciones.

El modelo especifica el protocolo que debe usarse en cada capa, y suele hablarse de modelo de referencia ya que se usa como una gran herramienta para la enseñanza de comunicación de redes.

Se trata de una normativa estandarizada útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. De este modo, no importa la localización geográfica o el lenguaje utilizado. Todo el mundo debe atenerse a unas normas mínimas para poder comunicarse entre sí. Esto es sobre todo importante cuando hablamos de la red de redes, es decir, Internet.

1.2.1 CAPAS DEL MODELO OSI.

Actualmente todos los desarrollos se basan en este modelo de 7 niveles que son los siguientes:

- **Físico.**
- **Enlace de datos.**
- **Red.**
- **Transporte.**
- **Sesión.**
- **Presentación.**
- **Aplicación.**

Nivel Físico: Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

- Definir conexiones físicas entre computadoras.
- Describir el aspecto eléctrico de la interface física.
- Describir el aspecto funcional de la interface física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.
- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

Nivel Enlace de Datos: Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red.

Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

- Detectar errores en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.
- En general controla el nivel y es la interface con el nivel de red, al comunicarle a este una transmisión libre de errores.

Nivel de Red: Este nivel define el enrutamiento y el envío de paquetes entre redes.

- Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
- Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
- Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
- Define el estado de los mensajes que se envían a nodos de la red.

Nivel de Transporte: Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información.

Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).

- Este nivel define cómo direccionar la localidad física de los dispositivos de la red.
- Asigna una dirección única de transporte a cada usuario.

- Define una posible multicanalización.
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío del mensaje.
- Establece la transparencia de datos, así como la confiabilidad en la transferencia de información entre dos sistemas.

Nivel Sesión: proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.
- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

Nivel Presentación: Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.

- Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
- Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
- Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Opera la visualización.

Nivel Aplicación: Proporciona servicios al usuario del Modelo OSI.

- Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
- Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (FTP), etc.

1.3 TIPOS DE REDES.

Al margen de que puedan hacerse por cable estructurado, o por vía inalámbrica, las redes pueden dividirse por su alcance o cobertura. Lógicamente, cuanto mayor sea el espacio que se quiere abarcar, más difícil y costosa puede resultar la instalación de cables.

1.3.1 RED DE COBERTURA.

Las redes de cobertura se clasifican de maneras esenciales y estas se caracterizan por el área geográfica que llegan a alcanzar o cubrir y son las siguientes:

- **Redes de área personal (PAN).**
- **Redes de área local (LAN).**
- **Redes de área de campus (CAN).**
- **Redes de área metropolitana (MAN).**
- **Redes de área amplia (WAN).**
- **Redes de área de almacenamiento (SAN).**
- **Redes de área local virtual (VLAN).**

1.3.1.1 RED DE AREA PERSONAL (PAN).

Hablamos de una red informática de pocos metros, algo parecido a la distancia que necesita el Bluetooth del móvil para intercambiar datos. Son las más básicas y sirven para espacios reducidos, por ejemplo, si trabajas en un local de una sola planta con un par de ordenadores.

Las redes PAN pueden serte útiles si vas a conectar pocos dispositivos que no estén muy lejos entre sí. La opción más habitual, sin embargo, para aumentar el

radio de cobertura y para evitar la instalación de cablea estructurado, suele ser la compra de un router y la instalación de una red de área local inalámbrica.

1.3.1.2 RED DE AREA LOCAL (LAN).

Es la que todos conocemos y la que suele instalarse en la mayoría de las empresas, tanto si se trata de un edificio completo como de un local. Permite conectar ordenadores, impresoras, escáneres, fotocopiadoras y otros muchos periféricos entre sí para que puedas intercambiar datos y órdenes desde los diferentes nodos de la oficina.

Las redes LAN pueden abarcar desde los 200 metros hasta 1 kilómetro de cobertura.

1.3.1.3 RED DE AREA DE CAMPUS (CAN).

Una CAN es una colección de LAN´s dispersadas geográficamente dentro de un Campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en un área delimitada en kilómetros.

Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro disperso.

En tal caso, tenemos las redes CAN. Habría varias redes de área local instaladas en áreas específicas, pero a su vez todas ellas estarían interconectadas, para que se puedan intercambiar datos entre sí de manera rápida, o pueda haber conexión a Internet en todo el campus.

1.3.1.4 RED DE AREA METROPOLITANA (MAN).

Mucho más amplias que las anteriores, abarcan espacios metropolitanos mucho más grandes. Son las que suelen utilizarse cuando las administraciones públicas

deciden crear zonas Wifi en grandes espacios. También es toda la infraestructura de cables de un operador de telecomunicaciones para el despliegue de redes de fibra óptica. Una red MAN suele conectar las diversas LAN que hay en un espacio de unos 50 kilómetros.

Otro tipo de red que se aplica en las organizaciones es la red de área metropolitana o MAN, una versión más grande que la LAN y que normalmente se basa en una tecnología similar a ésta.

La red MAN abarca desde un grupo de oficinas corporativas cercanas a una ciudad y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales.

La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione (se llama DQDB), que equivale a la norma IEEE. EL DQDB consiste en dos buses (cables) unidireccionales, los cuales se conectan a todas las computadoras.

1.3.1.5 RED DE AREA AMPLIA (WAN).

Son las que suelen desplegar las empresas proveedoras de Internet para cubrir las necesidades de conexión de redes de una zona muy amplia, como una ciudad o país.

Son redes punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica, como, por ejemplo: una ciudad o un continente. Está formada por una vasta cantidad de computadoras interconectadas (llamadas hosts), por medio

de subredes de comunicación o subredes pequeñas, con el fin de ejecutar aplicaciones, programas, etc.

Una red de área extensa WAN es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos. Las

líneas utilizadas para realizar esta interconexión suelen ser parte de las redes Las redes LAN comúnmente, se conectan a redes WAN, con el objetivo de tener acceso a mejores servicios, como por ejemplo a Internet.

Las redes WAN son mucho más complejas, porque deben enrutar correctamente toda la información proveniente de las redes conectadas a ésta.

1.3.1.6 RED DE AREA DE ALMACENAMIENTO (SAN).

Es una red propia para las empresas que trabajan con servidores y no quieren perder rendimiento en el tráfico de usuario, ya que manejan una enorme cantidad de datos. Suelen utilizarlo mucho las empresas tecnológicas para el almacenamiento de sus datos.

Una red de área de almacenamiento, en inglés Storage Area Network (SAN), es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad de canal de fibra o ISCSI.
- Un equipo de interconexión dedicado (conmutadores, puentes, etc.).
- Elementos de almacenamiento de red (discos duros).

Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Además de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red específica que se conecta a la SAN. El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza.

1.3.1.7 RED DE AREA DE AREA LOCAL VIRTUAL (VLAN).

Las redes de las que hablamos normalmente se conectan de forma física.

Las redes VLAN se encadenan de forma lógica (mediante protocolos, puertos, etc.), reduciendo el tráfico de red y mejorando la seguridad. Si una empresa tiene varios departamentos y quieres que funcionen con una red separada, la red VLAN.

1.3.2 REDES DE SERVICIO.

Las redes también se clasifican por el tipo de servicio que ofrece a los usuarios y se dividen en dos formas diferentes:

- Redes Públicas
- Redes Privadas

1.3.2.1 REDES PÚBLICAS.

Este tipo de redes son usualmente a las que todo usuario tiene acceso a ella y de la misma manera a su información, un ejemplo bastante claro lo podemos encontrar en la Internet ya que podemos tener acceso a ella desde cualquier parte del mundo sin restricción alguna.

Las redes públicas brindan servicios de telecomunicaciones a cualquier usuario que pague una cuota. El usuario o suscriptor puede ser un individuo, una empresa, una organización, una universidad, un país, etcétera.

El término público se refiere a la disponibilidad del servicio para todos en general, no se refiere a la privacidad de la información. Cabe mencionar que los PST se rigen por regulaciones que varían de país a país para proteger la privacidad de los datos de los usuarios.

Ejemplos de compañías operadoras que ofrecen su red pública de telecomunicaciones son: telefonía fija, telefonía celular, televisión por cable, televisión por satélite, radio por satélite, etcétera.

Ejemplos de redes públicas, de acceso abierto que no cobran cuota alguna al usuario, son las radiodifusoras de radio AM y FM, así como las televisoras en UHF y VHF. Este tipo de empresas también tienen una concesión del estado para operar y difundir señales, y se mantienen por el cobro de tiempo a sus anunciantes.

1.3.2.2 REDES PRIVADAS.

Con este tipo de redes no tan fácilmente cualquier usuario puede tener acceso a la red y a la información que se maneja, comúnmente estos tipos de redes las podemos encontrar en empresas, universidades o edificios gubernamentales y son conocidas también como Intranet.

Una red privada es administrada y operada por una organización en particular. Generalmente, los usuarios son empleados o miembros de esa organización, aunque, el propietario de la red podrá dar acceso a otro tipo de usuarios que no pertenecen a la institución pero que tienen ciertos privilegios. Una universidad, por ejemplo, puede constituir una red privada, sus usuarios son estudiantes, maestros, investigadores, administrativos, etc. Personas ajenas a estas organizaciones no tendrán acceso a los servicios. Una red privada también podrá ser usuaria de los servicios de una red pública, pero seguirá siendo una red restringida a usuarios autorizados.

Una red privada pura es aquella que no utiliza los servicios de terceros para interconectarse, sino sus propios medios. En cuestiones de seguridad, podría decirse que una red privada es más segura debido a que la información no está tan expuesta más que en sus propias premisas, pero cuando esta red privada hace uso de una red pública para algunos servicios, la seguridad está comprometida. Muchas veces se hace uso de esquemas de encriptación para hacer que los datos se transporten de una manera segura. Un ejemplo de esto,

son las redes privadas virtuales VPN (Virtual Private Network), las cuales usan redes públicas bajo ciertos mecanismos de seguridad para el manejo de su información.

Una red pública (PST) puede suministrar a una compañía servicios para establecer una red privada que interconecte mediante enlaces a una o más entidades o sucursales de esa misma empresa; en otras palabras, los PST están autorizados para brindar a sus usuarios opciones de servicios de telecomunicaciones para establecer redes privadas.

No hay que confundir las redes privadas y públicas respecto a las direcciones de Internet IP (Internet Protocol), las cuales explicaremos más adelante. Una red privada puede tener en sus nodos direcciones IP públicas o privadas. El concepto de red pública o privada se refiere a quienes (usuarios) tienen acceso a sus servicios en particular.

1.3.3 REDES POR CONEXIÓN.

Las aplicaciones de las redes de paquetes pueden ser de 2 tipos**:**

- Redes por medios Guiados**.**
- Redes por medios No Guiados**.**

1.3.3.1 REDES POR MEDIOS GUIADOS.

Una red por medios guiados está formada por la conexión de cables entre los distintos dispositivos que la conforman. Estos medios de transmisión de datos pueden estar compuestos por:

- Cable coaxial.
- Cables de par trenzado.
- Fibra óptica.

CABLE COAXIAL.

Este cordón permite conducir electricidad y está recubierto por una envoltura compuesta por varias capas, está fabricado con conductores eléctricos como el aluminio o el cobre**.**
El cable coaxial es un tipo de cable que se utiliza para transmitir señales de electricidad de alta frecuencia. Estos cables cuentan con un par de conductores concéntricos: el conductor vivo o central que está destinado a transportar los datos, y el conductor exterior**,** blindaje o malla, el cual actúa como retorno de la

corriente y referencia de tierra. Entre ambos se sitúa el dieléctrico, una capa aisladora.

CABLE DE PAR TRENZADO.

Un par trenzado consiste en 2 cables de cobre aislado, los cuales están unidos entre sí de forma similar a una estructura de ADN; esta forma trenzada se utiliza para reducir la interferencia eléctrica entre dos o más pares de cobre o bien interferencias del exterior. Debido a su fácil instalación, velocidad de transmisión de hasta varios Mbps y bajo coste, los pares trenzados se utilizan ampliamente.
Dependiendo de la forma en que se agrupen los pares, encontramos:

- Pares trenzados no apantallados (UTP): son los más simples. El par trenzado UTP categoría 5 está recubierto de una malla de teflón que no es conductora.
- Pares trenzados apantallados individualmente (STP): iguales a los anteriores, pero cada par rodeado de una malla conductora, que se conecta a las diferentes tomas de tierra de los equipos. Poseen mayor inmunidad al ruido.
- Pares trenzados apantallados (FTP): Cables pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a interferencias.

Así mismo, dependiendo del número de pares que tenga un cable, el número de vueltas por metro que posee su trenzado y los materiales utilizados, los estándares de cableado clasifican a los pares trenzados por categorías: categoría 2, categoría 3, categoría 4, categoría 5, categoría 5e, categoría 6 y categoría 7.

FIBRA ÓPTICA.

La Fibra Óptica consiste un conducto generalmente de fibra de vidrio o silicio que transmite impulsos luminosos normalmente emitidos por un láser o LED. Las fibras utilizadas en telecomunicación a largas distancias son siempre de vidrio; las de plásticos sólo son usadas en redes locales.

En el interior de la fibra óptica, el haz de luz se refleja contra las paredes en ángulos muy abiertos, así que prácticamente avanza por su centro. Esto permite transmitir las señales casi sin pérdida por largas distancias. La fibra óptica ha reemplazado a los cables de cobre por su costo/beneficio.

Este tipo de cable cuenta con una gran velocidad de transmisión de datos, no se ve afectada por ruido ni interferencias, además cuenta con mayor seguridad en la transmisión de datos.

1.3.3.2 REDES POR MEDIOS NO GUIADOS.

Los medios no guiados transportan ondas electromagnéticas sin usar un conductor físico. Este tipo de comunicación se denomina Comunicación Inalámbrica. Las transmisiones no guiadas se pueden clasificar en tres**:** radio frecuencia, microondas y luz tales como infrarrojos o láser… Es en este tipo de red donde clasificamos las tecnologías tales como Wifi, bluetooth, telefonía móvil, TV, Radio, etc… es decir, todas las señales que recibes sin necesidad de un cable.

- **Microondas terrestres.**
- **Satélites.**
- **Ondas de radio.**

MICROONDAS TERRESTRES.

Las microondas están definidas como un tipo de onda electromagnética situada en el intervalo del milímetro al metro y cuya propagación puede efectuarse por el interior de tubos metálicos. Es en si una onda de corta longitud. Tiene como características que su ancho de banda varía entre 300 a 3.000 MHz, aunque con algunos canales de banda superior, entre 3´5 GHz y 26 GHz. Es usado como enlace entre una empresa y un centro que funcione como centro de conmutación del operador, o como un enlace entre redes LAN.

Para la comunicación de microondas terrestres se deben usar antenas parabólicas, las cuales deben estar alineadas o tener visión directa entre ellas, además entre mayor sea la altura mayor el alcance, sus problemas se dan perdidas de datos por atenuación e interferencias, y es muy sensible a las malas condiciones atmosféricas.

SATÉLITES.

Conocidas como microondas por satélite, está basado en la comunicación llevada a cabo a través de estos dispositivos, los cuales después de ser lanzados de la tierra y ubicarse en la órbita terrestre siguiendo las leyes descubiertas por Kepler, realizan la transmisión de todo tipo de datos, imágenes, etc., según el fin con que se han creado. Las microondas por satélite manejan un ancho de banda entre los 3 y los 30 GHz, y son usados para sistemas de televisión, transmisión telefónica a larga distancia y punto a punto y redes privadas punto a punto. Las microondas por satélite, o mejor, el satélite en si no procesan información, sino que actúa como un repetidor-amplificador y puede cubrir un amplio espacio de espectro terrestre

ONDAS DE RADIO.

Son las más usadas, pero tienen apenas un rango de ancho de banda entre 3 KHz y los 300 GHz. Son poco precisas y solo son usados por determinadas redes de datos o los infrarrojos.

Las señales no guiadas pueden viajar del origen al destino de formas diferentes: En superficie, por el cielo y en línea de visión.

- Propagación por Superficie: Las ondas de radio viajan a través de la porción más baja de la atmósfera, abrazando a la tierra. Las señales emanan en todas las direcciones desde la antena de transmisión. La distancia depende de la cantidad de potencia en la señal. Cuanto más grande es la potencia, más grande es la distancia.

- Propagación por el cielo: Las ondas de radio con una frecuencia mayor se irradian hacia arriba en la ionosfera y permite distancias mayores con una potencia de salida menor.

- Propagación por Línea de Vista: Se transmiten señales de muy alta frecuencia directamente de antena. La propagación por línea de vista es truculenta porque las transmisiones de radio no se pueden enfocar completamente y deben ser direccionales.

1.3.4 REDES DE SISTEMA DE PROCESAMIENTO DE LA INFORMACIÓN.

1.3.4.1 PUNTO A PUNTO (P2P).

La mayor parte de la infraestructura de redes de área extensa está construida a partir de líneas alquiladas punto a punto.

Constituye este tipo de red las conexiones exclusivas entre terminales y computadoras con una línea directa. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión que soporta y la seguridad que presenta al no existir conexión con otros usuarios. Un inconveniente es su costo.

1.3.4.2 MAESTRO - ESCLAVO.

En este tipo de sistema un ordenador controla a uno o varios ordenadores, repartiéndoles las tareas y los recursos necesarios para la solución de las mismas.

1.3.4.3 CLIENTE - SERVIDOR.

En las redes basadas en estructuras cliente-servidor, los servidores ponen a disposición de sus clientes recursos, servicios y aplicaciones.

Dependiendo de que recursos ofrezca el servidor y cuales se mantienen en los clientes se pueden hacer distinciones entre distintas estructuras cliente-servidor.
En estas estructuras se diferencia:

- Donde se encuentran los datos.
- Donde se encuentran los programas de aplicación.
- Donde se presentan los datos.

A continuación, se presentarán brevemente los distintos conceptos.

1. **Sistema centralizado basado en el host (anfitrión).**

   Aquí, los datos, los programas de aplicación y la presentación se encuentran en el servidor. La imagen final se transmite a los terminales de los usuarios. Desde los terminales, las cadenas de caracteres de las entradas de los usuarios se reenvían al host. Este concepto es el que sirve de base para los mainframes.

2. **PC cliente y servidor host.**

   Los datos de aplicación se conservan de forma centralizada en el servidor. Con programas clientes de las aplicaciones, éstas se presentan en cada estación de trabajo. El lugar de trabajo suele ser una PC ejecutando, por ejemplo, Windows.

3. **Estación de trabajo cliente y servidor de archivo.**

   Los datos se encuentran en el servidor (generalmente en una base de datos). Con una base de datos cliente se accede a esos datos desde cualquier computadora. En el cliente se procesan los datos utilizando la inteligencia del cliente. Cada computadora contiene aplicaciones con las que se puede procesar los datos.

4. **PC cliente y servidor de aplicaciones.**

   En esta red se dispone al menos de dos servidores distintos. Uno de ellos actúa meramente como servidor de base de datos y el resto como servidor de aplicaciones. Los servidores de aplicaciones de esta red también son los responsables de acceso a las bases de datos. En las estaciones de trabajo funcionan los clientes de los programas de aplicación correspondientes.

5. **Sistema cliente-servidor cooperativo descentralizado.**

   Las bases de datos están repartidas en distintos servidores o incluso clientes. Las aplicaciones funcionan igualmente en distintos servidores o en parte también en clientes.

1.4 TOPOLOGÍA DE REDES.

La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como conjunto de nodos interconectados. Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

Los componentes fundamentales de una red son el servidor, los terminales, los dispositivos de red y el medio de comunicación.

En algunos casos, se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de cómo el protocolo considera dicho cableado.

La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Hay varias maneras de conectar dos o más computadoras en red. Para ellos se utilizan cuatro elementos fundamentales: servidores de archivos, estaciones de trabajo, tarjetas de red y cables.

A ellos se les suman los elementos propios de cada cableado, así como los manuales y el software de red, a efectos de la instalación y mantenimiento.

Los cables son generalmente de 3 tipos: UTP par trenzado, coaxial y fibra óptica.

La manera en que están conectadas no es arbitraria, sino que siguen estándares físicos llamados topologías.

Dependiendo de la topología será la distribución física de la red y dispositivos conectados a la misma, así como también las características de ciertos aspectos de la red como: velocidad de transmisión de datos y confiabilidad del conexionado.

Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman.

Los Criterios a la hora de elegir una topología, en general, buscan que eviten el coste del encaminamiento (necesidad de elegir los caminos más simples entre el nodo y los demás), dejando en segundo plano factores como la renta mínima, el coste mínimo, etc.
Otro criterio determinante es la tolerancia a fallos o facilidad de localización de éstos. También tenemos que tener en cuenta la facilidad de instalación y reconfiguración de la Red.

1.4.1 TOPOLOGÍAS FÍSICAS Y LÓGICAS.

TOPOLOGÍA FÍSICA: Es la forma que adopta un plano esquemático del cableado o estructura física de la red, también hablamos de métodos de control.

TOPOLOGÍA LÓGICA. Es la forma de cómo la red reconoce a cada conexión de estación de trabajo

1.4.2 TOPOLOGÍA DE RED DE BUS LINEAL.

PUNTO DE VISTA MATEMÁTICO.

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos.

PUNTO DE VISTA FÍSICO.

Cada host está conectado a un cable común. En esta topología, los dispositivos clave son aquellos que permiten que el host se "una" o se "conecte" al único medio compartido. Una de las ventajas de esta topología es que todos los hosts están conectados entre sí y, de ese modo, se pueden comunicar directamente.

Una desventaja de esta topología es que la ruptura del cable hace que los hosts queden desconectados.

PUNTO DE VISTA LÓGICO.

Una topología de bus hace posible que todos los dispositivos de la red vean todas las señales de todos los demás dispositivos. Esto representa una ventaja si desea que toda la información se dirija a todos los dispositivos. Sin embargo, puede representar una desventaja ya que es común que se produzcan problemas de tráfico y colisiones.

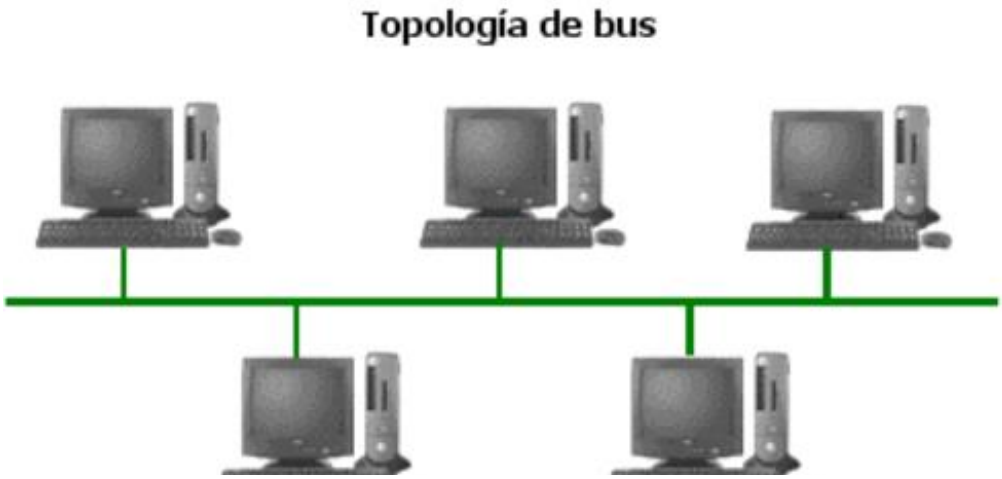


Ilustración 1.1 Topología de bus

1.4.3 TOPOLOGÍA DE RED ESTRELLA.

Es la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en la topología estrella este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar ccon los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. El tipo de concentrador hub se utiliza en esta topología, aunque ya es muy obsoleto; se suele usar comúnmente un switch.

La desventaja radica en la carga que recae sobre el nodo central. La cantidad de tráfico que deberá soportar es grande y aumentará conforme vayamos agregando más nodos periféricos, lo que la hace poco recomendable para redes de gran tamaño. Además, un fallo en el nodo central puede dejar inoperante a toda la red. Esto último conlleva también una mayor vulnerabilidad de la red, en su conjunto, ante ataques.

Si el nodo central es pasivo, el nodo origen debe ser capaz de tolerar un eco de su transmisión. Una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Ilustración 1.2 Topología de estrella

1.4.4 TOPOLOGÍA DE RED ANILLO.

Topología de red en la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos).
Simplifica la arquitectura y facilita la fluidez de datos, una desventaja es la longitud de canales y el canal usualmente se degrada a medida que la red crece.

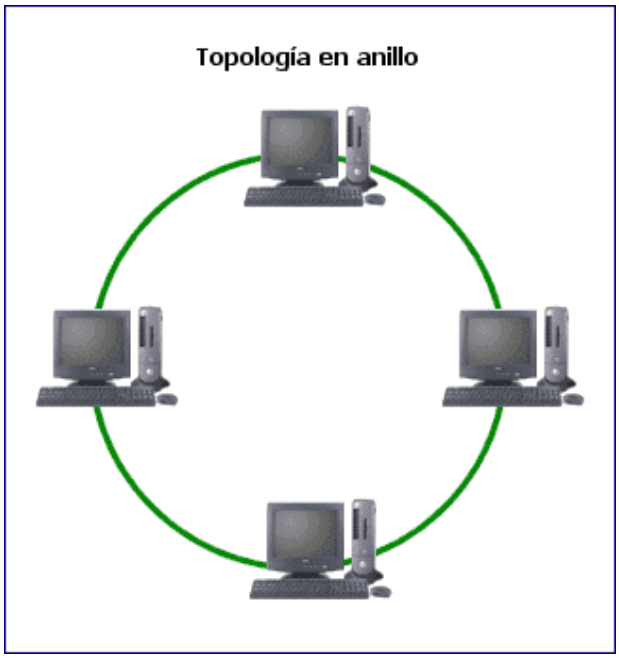


Ilustración 1.3 Topología en anillo

1.4.5 TOPOLOGÍA DE RED EN MALLA.

La topología en malla es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos.

Cada servidor tiene sus propias conexiones con todos los demás servidores. Una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar n dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S).

Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).

Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado.

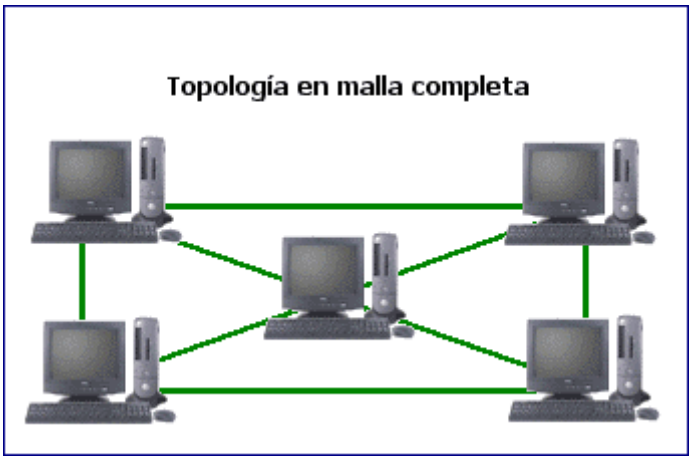


Ilustración 1.4 Topología en malla completa

1.5 TIPOS DE ENLACES.

En las conexiones de Computador a Computador existen diferencias de Sistemas y Fabricantes, para lograr la Sincronización del transmisor y el Receptor se logra a través de un protocolo de Enlace que es un conjunto de instrucciones predefinido que asegura la correcta secuencia e integridad de los datos transmitidos y reciba cuando se le instruya y notifique a la Terminal que envía cuando reciben datos erróneos.

Un protocolo debe ser capaz para distinguir entre los datos transmitidos y los caracteres de control.

Enlace de datos es el conjunto de módems u otro equipo de interfaces y circuitos de comunicaciones que conectan dos o más terminales que desean comunicarse.

1.5.1 PUNTO A PUNTO.

Es aquel que conecta únicamente dos estaciones en un instante dado. Se puede establecer enlaces punto a punto en circuitos dedicados o conmutados, que a su vez pueden ser dúplex o semidúplex.

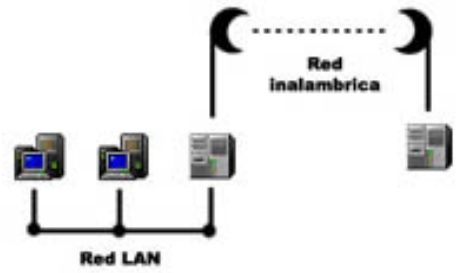


Ilustración 1.5 Punto a punto

1.5.2 PUNTO A MULTIPUNTO.

Estos conectan más de dos estaciones a la vez o se conectan múltiples dispositivos al enlace que se ramifican desde un único punto. Generalmente, el dispositivo que proporciona la conexión es un controlador inteligente, que manejan el flujo de información de los múltiples dispositivos unidos a ella.

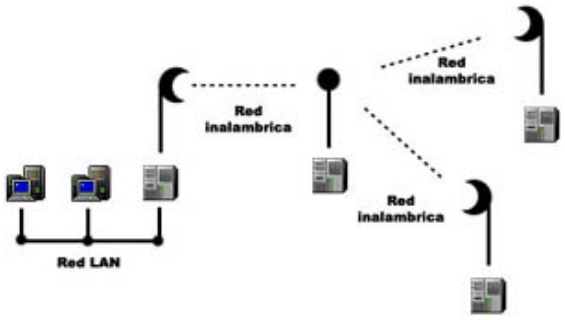


Ilustración 1.6 Punto a multipunto

1.6 INTERCONECTIVIDAD.

La plataforma que conforma las redes de datos, y de la cual hoy en día dependen nuestras relaciones sociales y de negocios, se basa en un conjunto de tecnologías y servicios en donde se diseñan, desarrollan y mantienen redes modernas, en su mayoría completamente heterogéneas.

Las primeras redes de datos estaban limitadas a intercambiar información basada en caracteres, pero las actuales redes han evolucionado tanto que hoy en día se transmite voz, flujos de video, texto y gráficos en una amplia gama de dispositivos, lo que proporciona acceso a una amplia variedad de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

Una primera aproximación a la definición, involucra desglosar los términos. Inter significa entre, y conectividad es la medida de qué tan bien los dispositivos se comunican entre sí y comparten información sin intervención humana. Así pues, la "Interconectividad" es el nivel de conexión que ocurre entre dos o más elementos. Y, por otro lado, "Red" hace referencia a un conjunto de equipos informáticos que se conectan usando un medio para poder transmitir información. Estas dos palabras pueden llevar a una definición no formal que hace alusión a la unión de diversas redes para conformar un solo elemento.

El Internet es la red de redes, la red de mayor extensión pues abarca todo el planeta (e incluso fuera de éste) conectando una gran cantidad de redes heterogéneas. Se sabe que todo sistema se compone de elementos de menor tamaño, por lo que la Interconectividad de Redes (Internet-working) viene a ser una estructura de comunicación entre dos o más redes que están conectadas entre sí para intercambiar datos o recursos, donde cada red conserva su propia identidad.

Realizar dicha interconexión requiere de diversos dispositivos, los cuales están diseñados para solventar las dificultades en transmisión de datos y lograr un funcionamiento ininterrumpido. A estos dispositivos se les llama “equipos de interconexión”, y son sobre los que recae la tarea de envío y recepción de datos en la red, por lo que pasan a ser el tema de estudio principal de la materia.

1.6.1 EQUIPOS DE INTERCONEXIÓN.

Dos o más redes separadas están conectadas para intercambiar datos o recursos forman una interred (internetwork). Enlazar LAN’s en una interred requiere de equipos que realicen ese propósito. Estos dispositivos están diseñados para sobrellevar los obstáculos para la interconexión sin interrumpir el funcionamiento de las redes. A estos dispositivos que realizan esa tarea se les llama equipos de Interconexión.

Existen equipos de Interconexión a nivel de:

- **LAN**:
  - Hub.
  - Switch.
  - Repetidor.
  - Gateway.
  - Puente.
  - Access point.

- **MAN**:
  - Repetidor.
  - Switch capa 3.
  - Enrutador.
  - Multicanalizador.
  - Wireless bridges.

  - Puente.
  - Modem analógico.
  - Modem ADSL.
  - Modem CABLE.
  - DSU/CSU.

- **WAN**:
  - Enrutador.
  - Multicanalizador.
  - Modem analógico.
  - DSU/CSU.
  - Modem satelital.

1.6.1.1 REPETIDOR.

Un repetidor (o generador) es un dispositivo electrónico ú que opera sólo en la Capa Física del modelo OSI (capa 1). Un repetidor permite sólo extender la cobertura física de una red, pero no cambia la funcionalidad de la misma. Un repetidor regenera una señal a niveles más óptimos. Es decir, cuando un repetidor recibe una señal muy débil o corrompida, crea una copia bit por bit de la señal original. La posición de un repetidor es vital, éste debe poner antes de que la señal se debilite. En el caso de una red local (LAN) la cobertura máxima del cable UTP es 100 metros; pues el repetidor debe ponerse unos metros antes de esta distancia y poner extender la distancia otros 100 metros o más.

1.6.1.2 CONCENTRADOR (HUB).

El concentrador o hub es un dispositivo de capa física que interconecta físicamente otros dispositivos (computadoras, impresoras, en topología estrella o ducto. Existen hubs pasivos o hubs activos. Los pasivos sólo interconectan dispositivos, mientras que los hubs activos además regeneran las señales recibidas, como si fuera un repetidor. Un hub activo entonces, puede ser llamado como un repetidor multipuertos.

1.6.1.3 PUENTE.

Los puentes operan tanto en la Capa Física como en la de Enlace de Datos del modelo de referencia OSI.

Los puentes pueden dividir una red muy grande en pequeños segmentos. Pero también pueden unir dos redes separadas. Los puentes pueden hacer filtraje para controlar el tráfico en una red.

Como un puente opera en la capa de enlace de datos, da acceso a todas las direcciones físicas a todas las estaciones conectadas a él. Cuando una trama entra a un puente, el puente no sólo regenera la señal, sino también verifica la dirección del nodo destino y la reenvía la nueva copia sólo al segmento al cual la dirección pertenece. En cuanto un puente encuentra un paquete, lee las direcciones contenidas en la trama y compara esa dirección con una tabla de todas las direcciones de todas las estaciones en ambos segmentos. Cuando encuentra una correspondencia, descubre a que segmento la estación pertenece y envía el paquete sólo a ese segmento.

1.6.1.4 CONMUTADOR DE PAQUETE (SWITCH).

Los switches son otro dispositivo de interconexión de capa 2 que puede ser usado para preservar el ancho de banda en la red al utilizar la segmentación.

Los switches son usados para reenviar paquetes a un segmento particular utilizando el direccionamiento de hardware MAC (como los puentes). Debido a que los switches son basados en hardware, estos pueden conmutar paquetes más rápido que un puente.

Los conmutadores que emplean la técnica store-and-forward completamente procesan el paquete incluyendo el campo del algoritmo CRC y la determinación del direccionamiento del paquete. Esto requiere que el paquete sea almacenado temporalmente antes de que sea enviado al apropiado segmento. Este tipo de técnica elimina el número de paquetes dañados que son enviados a la red.

Los conmutadores que usan la técnica cut-through son más rápidos debido a que estos envían los paquetes tan pronto la dirección MAC es leída. Por otra parte, también existe en el mercado conmutadores de paquetes de capa 3 y 4.

1.6.1.5 ENRUTADOR (ROUTER).

Los enrutadores operan en la capa de red (así como Enlace de Datos y capa física) del modelo OSI. Los enrutadores organizan una red grande en términos de segmentos lógicos. Cada segmento de red es asignado a una dirección así que cada paquete tiene tanto dirección destino como dirección fuente.

Los enrutadores son más inteligentes que los puentes, no sólo construyen tablas de enrutamiento, sino que además utilizan algoritmos para determinar la mejor ruta posible para una transmisión en particular.

Los protocolos usados para enviar datos a través de un enrutador deben ser específicamente diseñados para soportar funciones de enrutamiento. IP (Arpanet), IPX (Novell) y DDP (AppleTalk Network Layer Protocol) son protocolos de transporte enrutables.

Los enrutadores pueden ser de dos tipos:

- **Enrutadores estáticos:** estos enrutadores no determinan rutas. En vez de eso, se debe de configurar la tabla de enrutamiento, especificando las rutas potenciales para los paquetes.
- **Enrutadores dinámicos:** Estos enrutadores tienen la capacidad determinar rutas (y encontrar la ruta más óptima) basados en la información de los paquetes y en la información obtenida de los otros enrutadores.

1.6.1.6 GATEWAY O PROXY.

Los gateways, pasarelas o proxy servers son computadoras que están corriendo una aplicación o software. Los gateways trabajan en las capas superiores del modelo OSI (transporte, sesión, presentación y aplicación).

Este software es capaz de realizar una infinidad de tareas: conversión de protocolos para proveer la comunicación de dos plataformas distintas (SNA de IBM con una LAN de PC). También los gateways suelen ser servidores que corren software de seguridad como firewall; correo electrónico (SNMP, POP3); servidores de web (HTTP/1.1); servidores de dominios de nombre (DNS), etc.

Un Proxy permite a otros equipos conectarse a una red de forma indirecta a través de él.

Cuando un equipo de la red desea acceder a una información o recurso, es realmente el Proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial.

En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el Proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (una página Web) en una cache que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de Proxy se agrupan diversas técnicas.

1.6.1.7 PUNTO DE ACCESO (ACCES POINT).

Un punto de acceso es un dispositivo inalámbrico que funciona en la capa de enlace de datos del modelo OSI. Es parecido a un switch (pero inalámbrico) que les da acceso a todos los nodos conectados a él. El medio de comunicación es el aire en las bandas de frecuencia del espectro disperso (2.4 GHz y 5 GHz).

Existen varias tecnologías, pero las más importantes son las IEEE 802.11, IEEE 802.11b (Wi-Fi) y la IEEE 802.11a.

1.6.1.8 DSU/CSU (MODEM DIGITAL).

El DSU/CSU (Data Service Unit / Channel Service Unit) o mejor conocido como DTU (Data Terminal Unit) es un equipo de interconexión que opera en la capa de Enlace de Datos.

Un DSU/CSU es básicamente un modem digital que enlaza dos o más redes que tengan servicios digitales tales como E0s, E1/T1s, Frame Relay, etc.

Un CSU provee además acondicionamiento y ecualización de la línea, así como pruebas de loopback.

Un DSU (el cual puede contener las características de un CSU) convierte las señales de datos de un equipo DTE [Data Terminal Equipment] (una computadora) en señales digitales bipolares requeridas en la red digital, realiza la sincronización de relojes y regenera la señal.

1.7 PROTOCOLOS DE COMUNICACIONES.

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

También se define como un conjunto de normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse.

Los sistemas de comunicación utilizan formatos bien definidos (protocolo) para intercambiar mensajes. Cada mensaje tiene un significado exacto destinado a obtener una respuesta de un rango de posibles respuestas predeterminadas para esa situación en particular. Normalmente, el comportamiento especificado es independiente de cómo se va a implementar. Los protocolos de comunicación tienen que estar acordados por las partes involucradas. Para llegar a dicho acuerdo, un protocolo puede ser desarrollado dentro de estándar técnico.

Un lenguaje de programación describe el mismo para los cálculos, por lo que existe una estrecha analogía entre los protocolos y los lenguajes de programación:

Los protocolos son a las comunicaciones como los lenguajes de programación son a los cómputos. Un protocolo de comunicación, también llamado en este caso protocolo de red, define la forma en la que los distintos mensajes o tramas de bit circulan en una red de computadoras.

1.7.1 TCP.

(Protocolo de control de transmisión). Está basado en IP que es no fiable y no orientado a conexión, y sin embargo es:

- Orientado a conexión. Es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

- Fiable. La información que envía el emisor llega de forma correcta al destino.

El protocolo TCP permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un circuito virtual.

Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los encaminadores intermedios, para llegar a un mismo sitio.

Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes, aunque el protocolo TCP logré la ilusión de que existe un único

Circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino).

Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión.

Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el byte, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes.

Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-dúplex.

1.7.2 FTP.

(Protocolo de Transferencia de Ficheros). Es uno de los diversos protocolos de la red Internet y es el ideal para transferir grandes bloques de datos por la red.

Se precisa de un Servidor FTP y un cliente FTP, puede darse el caso de que los servidores sean de libre acceso para todo el mundo y entonces estamos hablando de login anónimo o FTP anónimo. La mayoría de las páginas Web a nivel mundial son subidas a los respectivos servidores mediante este protocolo.

Por defecto utiliza los puertos 20 y 21. El puerto 20 es el utilizado para el flujo de datos entre el cliente y el servidor y el puerto 21 para el flujo de control, es decir, para enviar las órdenes del cliente al servidor.

Mientras se transfieren datos a través del flujo de datos, el flujo de control permanece en espera. Esto puede causar problemas en el caso de transferencias de datos muy grandes realizadas a través de cortafuegos que interrumpan sesiones después de periodos largos en espera.
El archivo puede que se haya transferido con éxito, pero el cortafuegos puede desconectar la sesión de control, por lo que se genera un error.

1.7.3 UDP.

Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Tampoco tiene asentimiento, ni control de flujo, por lo que los paquetes pueden pisarse unos a otros; y tampoco sabemos si ha llegado correctamente, ya que no hay asentimiento. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión / desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

1.7.4 ICMP.

(Protocolo de Control de Mensajes de Internet). Es uno de los protocolos centrales de la suite de protocolos de Internet.

Es usado principalmente por los Sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red.

La única excepción es la herramienta ping, que envía mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible y el tiempo que le toma a los paquetes en ir y regresar a ese host.

1.7.5 SNMP.

(Protocolo simple de gestión de redes). Es el protocolo de gestión de red más importante y usado en la actualidad.

Forma parte del conjunto de protocolos TCP/IP y está definido en la capa de aplicación del mismo. SNMP busca la sencillez y es por ello que en la capa de transporte está soportado por el protocolo UDP (caracterizado por su rapidez y su falta de fiabilidad) a través del puerto 170.

La información que proporciona un dispositivo y los comandos que se pueden efectuar sobre él se definen en un lenguaje llamado SMI (Structure of Management Information, un subconjunto de ASN.1). Al árbol completo de la información estándar definida en SMI se le denomina MIB (Management Information Base), aunque coloquialmente se usa este nombre para referirse a los archivos definidos en SMI. SNMP permite a las aplicaciones de administración (managers) hacer consultas e incluso actualizaciones de los objetos definidos en el MIB. Estas peticiones son atendidas por los agentes SNMP que se ejecutan en los dispositivos de red. Este proceso permite la administración y monitorización remota de los dispositivos.

Existen programas gestores (managers) que periódicamente obtienen datos por SNMP de algún parámetro en especial, esto permite hacer gráficas de uso del sistema.

Los agentes también pueden notificar algún evento detectado en el sistema a los managers mediante mensajes llamados traps.

1.8 SERVIDORES.

Un servidor Web es un programa que implementa el protocolo HTTP. Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas Web o páginas HTML, textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

1.8.1 SERVIDOR WEB.

Se encarga de mantenerse a la espera de peticiones HTTP llevada a cabo por un cliente HTTP que solemos conocer como navegador.

El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita.

Sobre el servicio Web clásico podemos disponer de aplicaciones Web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas http.

1.8.2 DHCP.

(Protocolo de configuración dinámica de servidores). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras

conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP.

1.8.3 DNS.

(Servidor de nombre de dominios). Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. Alojaba un archivo llamado HOSTS.TXT que contenía todos los nombres de dominio conocidos (técnicamente, este archivo aún existe - la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts).

CAPÍTULO 2. SEGURIDAD EN REDES.

2.1 ¿QUÉ ES LA SEGURIDAD EN REDES?

La Seguridad en redes tiene el objetivo de mantener el intercambio de información libre de riesgo y proteger los recursos informáticos de los usuarios y las Organizaciones. Generalmente, se encuentra amenazada por riesgos que van de la mano con el aumento del uso de Internet en las Instituciones de todos los ámbitos. De esta forma, la Seguridad en redes es la clave para conseguir la confianza de los visitantes web

Se estima que 57 millones de usuarios de Internet recibieron correos electrónicos malintencionados en los que, haciéndose pasar por entidades y sitios web de prestigio y solvencia, se les solicitaban sus contraseñas. Y alrededor de 1,8 millones de personas divulgaron este tipo de información personal.

Ante estos escenarios, las empresas pretenden evitar la proliferación de prácticas fraudulentas con rigurosas medidas preventivas y de comprobación. Y aplicando estas medidas han conseguido una media de pérdidas por fraude del uno por ciento de sus ventas.

Estos datos reflejan que los volúmenes de compras y transacciones que registran las Organizaciones son directamente proporcionales a la disminución de los riesgos en las redes y el aumento de la confianza en las Organizaciones.

En este sentido, preservar la Seguridad en redes también debe considerar riesgos como ataques de virus, códigos maliciosos, gusanos, caballos de Troya y hackers. Asimismo, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y las Organizaciones deben enfrentar ataques de negación de servicio y amenazas combinadas. Es decir, la integración de herramientas automáticas de hackeo, accesos no autorizados a los sistemas, capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

En otras palabras, las amenazas informáticas no solamente incluyen troyanos en los sistemas o software espías que utilizan las plataformas convencionales de ataque. Además, existen intervenciones que manipulan el significado del

contenido virtual, provocando confusión del usuario y permitiendo la intrusión en los sistemas.

Por otro lado, es importante considerar que la Seguridad en redes también puede ser vulnerable desde el interior de las Organizaciones. Es decir, existen dos tipos de amenazas: internas y externas.

Las amenazas internas pueden ser más serias que las externas porque los IPS y Firewalls son mecanismos no efectivos en amenazas internas, los usuarios conocen la red, saben cómo es su funcionamiento y tienen algún nivel de acceso a ella.

Esta situación se presenta debido a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

En cuanto a las amenazas externas, que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

Ante los riesgos y amenazas, el empleo de tecnología Secure Sockets Layer (SSL), son piezas fundamentales para establecer confianza y confidencialidad en la red e internet.

Los Certificados de Seguridad SSL funcionan autentificando a las Organizaciones y la propiedad de sus sitios y con procesos de cifrado o encriptación que protegen la información sensible, a los usuarios y sus equipos de amenazas y riesgos.

Además, cuentan con opciones de recursos en sus Certificados de Seguridad como Validación Extendida (EV, Extended Validation) que ofrece el grado más alto de validación y lo constata mediante la barra de direcciones del navegador en color verde.

2.2 AMENAZAS EN INTERNET.

En todo momento es vital para las empresas evaluar sus prácticas de seguridad hacia los sistemas de información que estas dependen, con el fin de estar preparados y pensar en planes de acción para mitigar las amenazas que puedan surgir en cualquier momento.

Cada día las amenazas de seguridad son cada vez más graves, sofisticadas y difíciles de detectar, he aquí la importancia para las empresas de comprender y entender cuáles son las posibles amenazas que toda organización está hoy en día expuesta.

2.3 ATAQUES.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una contraseña válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de los mismos. Ante la diversificación de clasificaciones de amenazas y la inminente aparición de nuevas técnicas.

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

Los Administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Los "advisories" (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.

2.3.1 ATAQUES DE INTROMISIÓN.

Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

2.3.2 ATAQUE DE ESPIONAJE EN LÍNEAS.

Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.
Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una red.

2.3.3 ATAQUE DE MODIFICACIÓN.

Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos, utilizando la vulnerabilidad de los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.).

2.3.4 ATAQUE DE DENEGACIÓN DE SERVICIO.

Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

2.3.5 ATAQUE DE SUPLANTACIÓN.

Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Es importante mencionar, que así como se llevan estos tipos de ataques en medios electrónicos, muchas veces se llevan a cabo en archivos físicos (expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días (como teléfonos convencionales, celulares, cajeros automáticos, etc.); inclusive los ataques a computadoras, muchas veces, comienzan precisamente con información obtenida de una fuente física (papeles, basura, intervención de correo, cartas, estados de cuenta que llegan a los domicilios; o simplemente de alguien que vigila lo que hacemos).

Se hace mención de estos últimos puntos, porque muchas veces pensamos que la intrusión, pérdida, alteración, inserción, bloqueo de información en sistemas, bloqueo de sistemas operativos y de dispositivos, suceden por casualidad o simplemente porque existen los Hackers.
Lo que motiva a un pirata informático y/o Hacker a realizar los ataques son: los retos, ya que ellos trabajan en generar códigos que pueden burlar la seguridad, infiltrarse en redes y sistemas para extraer o alterar la información sintiéndose así superiores; codicia, unos de los motivos más antiguos por lo que las personas

delinquen, tratado de hacer "dinero fácil" y un propósito mal intencionado o también definido como vandalismo o terrorismo.
Los métodos tradicionales de los Hackers son: buscar comparticiones abiertas, contraseñas deficientes, fallas y vulnerabilidades en programación, desbordamiento de buffer y denegaciones de servicios. Los Métodos más avanzados son: Rastreo de redes conmutadas (transmisión de paquetes entre nodos o redes); métodos de falseamiento y enmascaramientos de IP; códigos malintencionados y virus.

2.3.6 HACKER.

Hacker (del inglés hack, recortar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.
Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo hardware o software. Se suele llamar hackeo y hackear a las obras propias de un hacker.
El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. En palabras de Richard Stallman, "Hacker, usando la palabra inglesa, quiere decir divertirse con el ingenio, usar la inteligencia para hacer algo difícil.

2.3.7 CRACKER.

El término cracker (del inglés crack, romper) tiene varias acepciones. Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de estos últimos por el uso incorrecto del término.

Se considera que la actividad de esta clase de cracker es dañina e ilegal. También se denomina cracker a quien diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario

del mismo. Esta acepción está más cercana al concepto de hacker en cuanto al interés por entender el funcionamiento del programa o hardware, y la adecuación a sus necesidades particulares, generalmente desarrolladas mediante ingeniería inversa.

Por ello los crackers son temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos (Haffner y Markoff, 1995). Pueden considerarse un subgrupo marginal de la comunidad de hackers. Hay muy distintos tipos de crackers, pero no consideramos entre ellos a aquellos que penetran en ordenadores o redes de forma ilegal para robar: éstos son ladrones de guante blanco, una vieja tradición criminal.

2.3.8 VIRUS.

Existe cierta controversia sobre la definición de virus informático. Quizás la más aceptada pertenece a Fred B. Cohen, quien en 1984 escribió su tesis doctoral acerca de los virus, definiéndolos como «un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo».
Los virus informáticos tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.
El funcionamiento de un virus informático es conceptualmente simple: ejecutando un programa infectado (normalmente por desconocimiento del usuario) el código del virus queda almacenado (residente) en la memoria RAM del ordenador, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando los posteriores ficheros ejecutables que sean abiertos o ejecutados, añadiendo su propio código al del programa infectado y grabándolo en disco, con lo cual el proceso de replicado se completa.

2.3.9 SNIFFER.

Un Sniffer, según el glosario de la Comisión de archivos y bibliotecas del estado de Texas, es un programa que captura datos dentro de una red de cómputo; es utilizado por los hackers para obtener nombres de usuarios y contraseñas, y es una herramienta que permite auditar e identificar paquetes de datos en una red, misma que, puede ser usado legítimamente por los administradores de redes y personal de mantenimiento para identificar problemas de la misma red.

2.3.10 SPOOFING.

En términos de seguridad informática hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.
Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

2.3.10.1 TIPOS DE SPOOFING.

2.3.10.1.1 IP SPOOFING.

Suplantación de IP. Consiste básicamente en sustituir la IP origen de un paquete TCP/IP por otra IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo, si enviamos un ping (paquete ICMP "echo request") spoofeado, la respuesta será recibida por el host al que pertenece la IP legalmente.

2.3.10.1.2 ARP SPOOFING.

Suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP falseadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Explicándolo de una manera más sencilla: El protocolo Ethernet trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando un host quiere comunicarse con una IP emite una trama ARP-Request a la dirección de Broadcast pidiendo la MAC del host poseedor la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC. Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP".

2.3.10.1.3 DNS SPOOFING.

Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables.

2.3.10.1.4 WEB SPOOFING.

Suplantación de una página Web real (no confundir con phising). Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB visitas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de Proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página Web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. El WEB SPOOFING es difícilmente detectable, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

2.3.10.1.5 MAIL SPOOFING.

Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails hoax como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales.

2.4 SOLUCIÓNES DE SEGURIDAD EN REDES.

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental.
El saber donde identificar los riesgos de la información es de vital importancia.

2.4.1 PRIVACIDAD.

La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial.

2.4.2 CONFIDENCIALIDAD.

Debe garantizarse que la información enviada sólo puede ser leída por personas debidamente autorizadas

2.4.3 INTEGRIDAD.

La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

2.4.4 DISPONIBILIDAD.

La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (Denial of Service ó DoS) o “tirar” el servidor.

2.4.5 AUTENTICACIÓN.

Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

2.4.6 AUDITORÍA.

Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este rubro el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Para poder entender mejor las tareas de administración de seguridad, tomaremos el ejemplo de una compañía ficticia a la que llamaremos "Servicios de Cómputo". Esta compañía dispone de un servidor donde corre el software a través del cual se lleva a cabo el procesamiento de las nóminas y el control de recursos humanos.

Autenticación se refiere a que sólo las personas de esos departamentos tengan cuentas de acceso a dichos equipos, puesto que sería peligroso que algún otro departamento lo tuviera.

El responsable de los equipos de cómputo llevaría a cabo la labor de Autorización, al no permitir que todas las personas responsables de recursos humanos tuvieran acceso a las Bases de Datos de Nóminas, si no lo necesitan.

La Auditoria se lleva a cabo al establecer políticas de uso y acceso a los recursos, así como reglamentos que rijan la no-divulgación de información confidencial. También aquí se debe llevar un registro de los recursos utilizados para prevenir, por ejemplo, que un uso del 100% en un disco provoque que el sistema deje de funcionar. Debe vigilarse también los intentos de acceso legal e ilegal al mismo.

2.5 SPAM EN DIFERENTES MEDIOS.

Spam, o información basura, hace referencia a aquellos mensajes, con remitente desconocido, que no son solicitados ni deseados por el usuario y que, además, por norma general, son enviados en grandes cantidades. Por consiguiente, el spam se caracteriza por ser anónimo, masivo y no demandado.

Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, redes sociales, páginas web, wiki, foros, blogs, a través de ventanas emergentes y todo tipo de imágenes y textos en la web.

También se llama correo no deseado a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios como viajes, drogas, software y pornografía), se activa

mediante el ingreso a páginas de comunidades o grupos o acceder a enlaces en diversas páginas o inclusive sin antes acceder a ningún tipo de páginas de publicidad.

2.5.1 SPAM EN PUBLICACIONES.

Es una técnica de correo basura relativamente nueva, que surge en lugares como publicaciones de los blogs. Consiste en dejar un comentario en una entrada, que por lo general no tiene nada que ver con la misma, sino que tiene enlaces a sitios comerciales, o promociona algún producto.

2.5.2 SPAM EN CORREO ELECTRONICO.

El correo masivo supone actualmente la mayor parte de los mensajes electrónicos intercambiados en Internet, siendo utilizado para anunciar productos y servicios de dudosa calidad.

Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, no sirve de nada contestar a los mensajes de spam: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos.

2.5.3 SPAM EN FOROS.

El spam, dentro del contexto de foros, es cuando un usuario publica algo que desvirtúa o no tiene nada que ver con el tema de conversación. También, en algunos casos, un mensaje que no contribuye de ninguna forma al tema es considerado spam. Una tercera forma de spamming en foros es cuando una persona publica repetidamente mensajes acerca de un tema en particular en una forma indeseable (y probablemente molesta) para la mayor parte del foro. Finalmente, también existe el caso en que una persona publique mensajes únicamente con el fin de incrementar su rango, nivel o número de mensajes en el foro.

2.5.4 SPAM EN REDES SOCIALES.

Es una nueva forma de correo basura que consiste en enviar publicidad, ofertas de empleo, publicidad directamente a los usuarios de redes sociales profesionales sin que estos lo hayan solicitado o en los foros de la red social.

Dos ejemplos de correo no deseado corporativo en este sector son el envío de invitaciones no solicitadas a los contactos de usuarios de Facebook, y la "respuesta automática" con publicidad que aleatoriamente se hace desde MSN Hotmail cuando alguien envía un mensaje a un buzón de dicha corporación.

2.5.5 SPAM POR TELEFONÍA IP.

Se ha predicho que las comunicaciones de Voz sobre IP (VoIP) serán vulnerables a ser spammeadas por mensajes pregrabados. A pesar de que se han reportado muy pocos incidentes, muchas compañías ya han comenzado a intentar vender defensas contra ello.

2.5.6 SPAM EN MENSAJERÍA DE JUEGOS EN LÍNEA.

Muchos juegos en línea permiten a los jugadores contactarse entre ellos vía mensajería peer-to-peer o salas de Chat. Estos servicios de mensajería también están siendo utilizados por jugadores inescrupulosos para promover ciertos sitios Web y tiendas en línea, sin preocuparse por violar directamente el acuerdo de usuario final del juego, el cual prohíbe utilizar las comunicaciones dentro del juego para tales propósitos.

2.6 TÉCNICAS DE SPAM.

2.6.1 OBTENCIÓN DE DIRECCIONES DE CORREO.

Los spammers (individuos o empresas que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren Internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam son:

Las propias páginas Web, que con frecuencia contienen la dirección de su creador, o de sus visitantes (en foros, weblogs, etc.).Los grupos de noticias de usenet, cuyos mensajes suelen incluir la dirección del remitente,. Listas: les basta con apuntarse e ir anotando las direcciones de sus usuarios.

Correos electrónicos con chistes, cadenas, etc. que los usuarios de Internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje, o, más raramente, por un usuario malicioso.

Páginas en las que se solicita tu dirección de correo (o la de "tus amigos" para enviarles la página en un correo) para acceder a un determinado servicio o descarga.

Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).

2.6.2 ENTRADA ILEGAL EN SERVIDORES.

Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales.

2.6.3 ENVÍO DE LOS MENSAJES.

Una vez que tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los *spammers* utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en

general a Internet, por consumirse gran parte del ancho de banda en mensajes basura.

2.6.4 VERIFICACIÓN DE RECEPCIÓN.

Además, es frecuente que el spammer controle qué direcciones funcionan y cuáles no por medio de Web bugs o pequeñas imágenes o similares contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del spammer, que registra automáticamente el hecho. Son una forma más de spyware. Otro sistema es el de prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído. Si recibe un correo no solicitado debe borrarlo sin leerlo.

2.6.5 TROYANOS Y ORDENADORES ZOMBIS.

Recientemente, han empezado a utilizar una técnica mucho más perniciosa: la creación de virus troyanos que se expanden masivamente por ordenadores no protegidos (sin cortafuegos). Así, los ordenadores infectados son utilizados por el spammer como "ordenadores zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos (sobre todo cadenas) en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora haber sido infectado (que no tiene por qué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios.

2.6.6 SERVIDORES DE CORREO MAL CONFIGURADOS.

Los servidores de correo mal configurados son aprovechados también por los spammer. En concreto los que están configurados como Open Relay. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos. Existen diferentes bases de datos públicas que almacenan los ordenadores que conectados directamente a Internet permiten su utilización por los spammers. El más conocido es la Open Relay Data Base.

2.6.7 PRECAUCIONES PARA EVITAR EL CORREO BASURA.

En lugar de poner la dirección como texto, muéstrala en una imagen con la dirección de correo. Actualmente no se pueden rastrear automáticamente.

En lugar de poner el enlace a tu cuenta, usa una redirección (puede ser temporal o por un número de usos), y bórrala cuando recibas excesivo spam.

Modificar la dirección para evitar el rastreo automático. Por ejemplo, cambiar "nombre@dominio.com" por "nombre (ARROBA) dominio (PUNTO) com", "nombre@dominioNOSPAM.com, quita NOSPAM" o "n0mbre@d0mini0.c0m (sustituir los ceros por oes)". Ayuda, pero no es 100% efectivo.

Una combinación de las anteriores.

Algunos servicios de correo gratuito como Mailinator ofrecen cuentas temporales sin tener que usar contraseñas. Los mensajes se borran automáticamente al cabo de unas horas. Puede ser útil si sólo quieres que contacten contigo una vez, por ejemplo, para confirmar un pedido.

En los grupos de noticias y listas de correo:

No poner el remitente verdadero en los post enviados.

Si el archivo de mensajes a la lista es visible desde Web, cambiar las direcciones de remite por una imagen, ocultarlas, o escribirlas de forma que sea difícil reconocerla como tal para un programa.

Para evitar spam en una lista:

El foro puede estar moderado, para evitar mensajes inadecuados.

Rechazar correos de usuarios no suscritos a la lista.

No reenviar mensajes parte de una cadena de correo electrónico.

No hacer envíos a amigos o colaboradores en los que aparezcan muchas direcciones y, si se hace, usar Bcc (o CCO) para que no sean visibles las demás direcciones.

Igualmente, si reenvías un correo electrónico que ya contiene alguna dirección en el mensaje, asegúrate de borrarla.

Al rellenar una inscripción no dar el correo. Si es necesario dar una dirección correcta (envío de contraseñas, confirmación de la suscripción, etc.) utiliza una redirección temporal, o una cuenta gratuita "extra" prescindible de las que se ofrecen en la mayoría de los portales de Internet. No se debe hacer caso de las recomendaciones del tipo "preferiblemente cuenta no Hotmail".

Leer los correos de remitentes sospechosos como texto, y no como HTML.

No enviar nunca mensajes al spammer, aunque prometan dejar de enviar spam si se les pide. A menudo ofrecen una forma de anular la suscripción a su boletín de mensajes (lo que en inglés llaman "opt-out", u optar por salir) que suele consistir en mandar un mensaje a una dirección de tipo unsubscribe@dominio.com. Si mandas un mensaje a dicha dirección con la esperanza de dejar de recibir correo no solicitado, sólo estás confirmando que tu cuenta existe y está activa, por lo que acabarás recibiendo más spam que antes.

Tener siempre al día las actualizaciones de seguridad del sistema operativo.

Instalar un buen cortafuegos (firewall) y un buen antivirus, y tenerlos siempre activados.

Hay formas de bloquear mensajes que tengan ciertas características, por ejemplo, si en el asunto aparece la palabra "porno". Sin embargo, muchos spammers escriben algunas palabras con faltas intencionadas de ortografía o introducen algún espacio o signo de puntuación en la palabra más propensa a ser bloqueada (por ejemplo, escribirían "p0rn0" o "p o r n o"). Por lo que bloquear mensajes no suele ser muy útil.

2.7 ADMINISTRACIÓN DE SERVICIOS EN INTERNET.

Para hablar acerca de la administración de servicios en Internet, primero hablaremos de algunos servicios de Internet, estos, principalmente tienen como función brindar un servicio o necesidad a un usuario de la Internet, entre ellos talvez el más usado es el correo electrónico.

El término ‘servicio de información’ hace referencia a cada uno de los diferentes sistemas de distribución de información que se pueden plantear en una red de transmisión de datos como Internet. Desde el punto de vista de un usuario, la parte visible de un servicio de información es la aplicación cliente que da acceso al mismo, que dispone de unas reglas de uso propias para recoger y presentar la información. Unido a la aplicación cliente siempre hay un servidor, que proporciona los datos requeridos tras el oportuno diálogo.

Las redes de comunicaciones, tal y como se conciben en la actualidad, proporcionan numerosos servicios de información considerados como básicos.

2.7.1 CORREO ELECTRÓNICO.

Es tal vez el principal servicio de Internet, y sin duda el de mayor importancia histórica. Cada persona que está conectada cuenta con un "buzón electrónico" personal, simbolizado en una dirección de correo.
El correo electrónico sirve para enviar y recibir mensajes a otros usuarios, y por eso no hay nunca dos nombres iguales. La primera parte de una dirección identifica habitualmente a la persona y la segunda a la empresa u organización para la que trabaja, o al proveedor de Internet a través del que recibe la información. Así el correo usuario@hotmail.com identifica al usuario llamado usuario, la @ significa "at" y hotmail.com es la compañía que proporciona el servicio de correo. Por este medio se pueden enviar texto, gráficos, hojas de cálculo, algunos programas ejecutables (dependiendo de la política del proveedor y del espacio que este le dé para su correo), etc.

2.7.2 LISTAS DE CORREO.

Están íntimamente relacionadas con el correo electrónico. Son listas de direcciones electrónicas de personas con intereses comunes. Cada vez que se envía un e-mail a una lista, todas las personas que pertenecen al grupo lo reciben, y a su vez, cada

vez que alguien envíe un mensaje a la lista de correo nosotros recibiremos una copia.

2.7.3 WORLD WIDE WEB.

Permite consultar información almacenada en cualquier computadora de la red. Es el servicio más flexible, porque además de consultar información permite también enviar datos. De esta manera, se puede rellenar formularios oficiales para entregarlos a través de Internet, comprar a distancia, etc.

2.7.4 FTP.

Permite el intercambio de archivos de una computadora a otra. Gracias a este servicio se puede acceder a enormes bibliotecas de programas y documentos disponibles en la red. También es posible poner a disposición de terceras personas información que nos pertenece, colocándola en archivos en una máquina de acceso público en Internet.

2.7.5 NEWS.

Son foros de discusión que permiten intercambiar opiniones entre todos los usuarios de Internet.

2.7.6 VIDEOCONFERENCIAS.

Para hablar con otra persona de viva voz y viendo además su imagen, a un costo mucho más barato que una llamada telefónica internacional.

2.7.7 TELNET.

Acceso remoto a un servidor de la red, no es frecuente que el usuario medio lo necesite.

CAPÍTULO 3. FIREWALLS.

3.1 ¿QUÉ ES UN FIREWALL?

Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

3.1.1 PRIMERA GENERACIÓN CORTAFUEGOS DE RED: FILTRADO DE PAQUETES.

El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.

El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto).[5] Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico (ya sean navegación web, impresión remota, envío y recepción de correo electrónico, transferencia de archivos…); a menos que las máquinas a cada lado del filtro de paquetes estén a la vez utilizando los mismos puertos no estándar.

El filtrado de paquetes llevado a cabo por un cortafuegos actúa en las tres primeras capas del modelo de referencia OSI, lo que significa que todo el trabajo lo realiza entre la red y las capas físicas.[7] Cuando el emisor origina un paquete y es filtrado por el cortafuegos, este último comprueba las reglas de filtrado de paquetes que lleva configuradas, aceptando o rechazando el paquete en consecuencia. Cuando el paquete pasa a través de cortafuegos, éste filtra el paquete mediante un protocolo y un número de puerto base (GSS). Por ejemplo, si existe una norma en el cortafuegos para bloquear el acceso telnet, bloqueará el protocolo TCP para el número de puerto 23.

3.1.2 SEGUNDA GENERACIÓN CORTAFUEGOS DE ESTADO.

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo.

3.1.3 TERCERA GENERACIÓN CORTAFUEGOS DE APLICACIÓN.

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI.

Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los cortafuegos de aplicación resultan más lentos que los de estado.

3.2 ¿QUÉ OFRECE UN FIREWALL?

El firewall proporciona un único check point que preserva la intranet del ataque de intrusos que pudieran accederla. Nos permite monitorear la seguridad a través de sus alarmas, logs y sistema de antivirus, los cuales deben ser revisados periódicamente, pues debemos poder determinar hipotéticos intentos de acceso ya que el mismo firewall puede ser violado y una vez que esto sucede estamos sin protección.

Un firewall también determina el tipo de información que se puede acceder en la Internet, también determina cual de los servicios de red pueden ser accesados dentro de ésta por los que están fuera de la red interna, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización. También define el contenido que puede ser accesado y descargado desde la Web y de los diferentes servicios de correo.

3.2.1 ¿QUÉ PUEDE HACER UN FIREWALL PARA PROTEGER LA RED?

Se instala un firewall entre la red y el punto de conexión con Internet (u otra red no de confianza). El firewall le permite entonces limitar los puntos de entrada a la red. Un firewall proporciona un único punto de contacto (denominado punto de concentración) entre la red e Internet. Dado que tiene un único punto de contacto, tendrá más control sobre qué tráfico permitirá entrar y salir de la red.

El firewall aparece como una única dirección para el público. El firewall proporciona acceso a la red no de confianza a través de servidores Proxy o SOCKS o de la conversión de direcciones de red (NAT) a la vez que oculta las direcciones de la red interna. Por consiguiente, el firewall mantiene la confidencialidad de la red interna. Conservar la información sobre la red en privado es una de las formas en que el firewall puede evitar que se produzcan ataques en los que el intruso se haga pasar por otra persona (suplantación (spoofing)).

Un firewall le permite controlar el tráfico de entrada y salida de la red para reducir al mínimo el riesgo de ataque a la red. El firewall filtra todo el tráfico que entra en la red de forma que sólo puedan entrar tipos específicos de tráfico para destinos específicos. Esto minimiza el riesgo de que alguien utilice TELNET o el protocolo de transferencia de archivos (FTP) para obtener acceso a los sistemas internos.

3.2.2 ¿QUÉ NO PUEDE HACER UN FIREWALL PARA PROTEGER LA RED?

Un firewall proporciona gran protección ante ciertos tipos de ataque, pero es solamente una parte de la solución de seguridad total. Por ejemplo, un firewall no puede proteger necesariamente datos que se envíen por Internet mediante aplicaciones como correo SMTP, FTP y TELNET. A menos que decida cifrar estos datos, cualquier persona podrá acceder a ellos en Internet mientras se dirigen a su destino.

Los Firewalls ofrecen excelente protección a posibles amenazas, pero no son una solución completamente segura. Ciertas amenazas están fuera del control del Firewall.

Un Firewall no puede proteger acciones ilegales de los usuarios internos:

Un firewall puede tener un sistema de usuarios capaz de enviar información privada fuera de la organización sobre una conexión de red; pero podría simplemente no tener una conexión de red.
Pero el mismo usuario puede copiar datos en disco, tape, papel y enviarlo fuera de su compañía en su portafolio.

Si el ataque es realmente dentro de firewall, un firewall puede virtualmente notarlo. Los usuarios internos pueden robar datos, dañar hardware y software y modificar programas cerca del firewall. Las amenazas internas requieren una seguridad interna, tal como un host de seguridad y educación a los usuarios.

Un Firewall no puede proteger las conexiones que no pasan por él:
Un firewall puede efectivamente controlar el tráfico que pasa a través de él, pero no el que no pasa. Un firewall no tiene forma de prevenir intrusos que se comunican a través de un módem.

Un Firewall no puede enfrentar completamente nuevas amenazas:
Un firewall está diseñado para proteger amenazas conocidas. Solo un buen diseñador puede también protegerse de nuevas amenazas. Por lo tanto, un firewall no puede automáticamente defenderse cuando sucede un nuevo ataque.

Periódicamente la gente descubre nuevas formas de ataque. No se puede resetear un firewall y creer que se está protegido para siempre.

Un Firewall no puede protegerse de los virus:
Los firewalls no pueden mantener virus de una PC fuera de la red. Algunos firewalls escanean todo el tráfico que pasa a través de él a la red interna; el escaneo es al menos de la dirección de origen y del destino.
Con sofisticados filtrados de paquetes o Proxy, la protección de virus en firewalls no es muy práctico. Existen simplemente algunos tipos de virus y algunas formas de virus que pueden ocultarse en los datos.

Detectar virus en un paquete al azar de un dato pasando a través del firewall es muy dificultoso, esto requiere:

- Reconocer que el paquete es parte de un programa
- Determinar a qué programa se parece
- Determinar que el cambio es debido a un virus

La forma más práctica de atacar el problema de los virus, es a través de la protección del software y de la educación de usuarios.

3.3 OBJETIVO DE UN FIREWALL.

El objetivo principal de un firewall es proteger a una red de otra. Por lo general, la red que se está protegiendo le pertenece a usted (o está bajo su responsabilidad), y la red contra la que se protege es una red externa en la que no puede confiarse y desde la que se pueden originar intrusiones de seguridad. Para proteger su red debe evitar que usuarios no autorizados tengan acceso a datos delicados, mientras que se permite que usuarios legítimos tengan acceso irrestricto a los recursos de la red.

Aunque el modelo OSI es una manera tradicional de diferenciar entre arquitecturas y capacidades de comunicación, no todos están conscientes de él o lo aplican. Muchos utilizan firewall corno término genérico que describe un amplio rango de funciones, además de la arquitectura de los dispositivos que protegen a la red. Algunos, en realidad, utilizan el término firewall para describir casi cualquier dispositivo de seguridad de red, como un dispositivo de encriptación de hardware, un router de selección o Gateway a nivel de aplicación.

En general, un firewall se coloca entre la red interna confiable y la red externa no confiable. El firewall actúa como un punto de cierre que monitorea y rechaza el tráfico de red a nivel de aplicación. Los firewalls también pueden operar en las capas de red y transporte en cuyo caso examinan los encabezados de IP y de TCP de paquetes entrantes y salientes, Y rechazan o pasan paquetes con base en las reglas de filtración de paquetes programadas.

El firewall es el principal instrumento utilizado para la implementación de una política de seguridad de la red de una organización. En muchos casos se necesitan técnicas de mejoramiento de la autentificación, la seguridad y la primacía para aumentar la seguridad de la red o implementar otros aspectos de la política de seguridad.

Un firewall, debido a su funcionalidad, debe ser capaz de ofrecernos una serie de características mínimas, como puede ser el empleo de una adecuada política de seguridad, esto solo no basta, sino que el firewall además debe ser capaz de poder ofrecer otros servicios como pueden ser el registro de las operaciones que vaya realizando y el poseer una interfaz fácil e intuitiva que reduzca al mínimo la posibilidad de que el operario se equivoque al momento de configurarlo y darle mantenimiento.

3.4 ¿CÓMO FUNCIONA UN FIREWALL?

Un firewall actúa bloqueando el tráfico no autorizado y cada diseño de implementación se enfocará a las características y necesidades de cada tipo de empresa.

El Firewall bloquea todos los puertos y protocolos y solo deja abiertos aquellos que realmente se van a emplear, esto evita que los puertos abiertos sean empleados para causar problemas en los servidores o tomar control de los mismos.

Para comprender cómo funciona un firewall, imagine que la red es un edificio en el que quiere controlar el acceso. El edificio tiene un vestíbulo como único punto de entrada. En este vestíbulo tiene recepcionistas para recibir a los visitantes, guardias de seguridad para controlarlos, cámaras de vídeo para grabar sus acciones y lectores de tarjetas identificadoras para comprobar la identidad de los visitantes que entran en el edificio.

Estas medidas pueden funcionar bien para controlar el acceso al edificio. Pero si una persona no autorizada consigue entrar en el edificio, no hay forma de proteger el edificio ante las acciones del intruso. Sin embargo, si supervisa los movimientos del intruso, tiene la oportunidad de detectar las actividades sospechosas que pueda llevar a cabo.

Al definir la estrategia de los cortafuegos, es posible que piense que hay suficiente con prohibir todo lo que represente un riesgo para la organización y permitir todo lo demás. Sin embargo, dado que los piratas informáticos crean nuevos métodos de ataque constantemente, debe anticiparse con métodos para evitar dichos ataques. Como en el ejemplo del edificio, debe buscar señales de que alguien ha roto las defensas de alguna manera. Generalmente ocasiona muchos más daños y gastos recuperarse de una intrusión que impedirla.

En el caso de un firewall, la mejor estrategia es permitir solamente las aplicaciones que haya probado y que le merezcan toda confianza. Si sigue esta estrategia, debe definir la lista de servicios a ejecutar en el firewall de forma exhaustiva. Puede caracterizar cada servicio por la dirección de la conexión (de interna a externa o de externa a interna). También deberá listar los usuarios a los que autorizará el uso de cada servicio y las máquinas que pueden emitir una conexión para el mismo.

3.4.1 ¿CÓMO ES EL ACCESO DESDE EL EXTERIOR?

Si el Firewall no valida nuestra IP no podremos conectarlo con la LAN, aunque como la IP podemos falsificarla hoy en día se implementan también Servidores Proxys, ante los cuales deberemos identificarnos antes, protegiendo así también al Firewall.

3.4.2 ¿CÓMO ES EL ACCESO DESDE EL INTERIOR?

Para el usuario la LAN es transparente, es decir, si desde cualquier estación enviamos un paquete a una IP y el Firewall nos valida el tamaño, IP de destino, puerto, etc. (Estos parámetros varían según las necesidades de seguridad cada red, y por tanto del nivel de configuración del Firewall), no veremos proceso alguno, sería como si no hubiera nada vigilando por nuestra seguridad, aunque si lo hay.

3.5 COMPONENTES DE LOS FIREWALLS.

Un firewall se compone de hardware y software que, utilizado conjuntamente, impide el acceso no autorizado a parte de una red. Un firewall consta de los siguientes componentes:

- El hardware del firewall consta normalmente de un sistema aparte dedicado a ejecutar las funciones del software del firewall.
- El software del firewall puede constar de todas estas aplicaciones o algunas de ellas:
  - Filtros de paquetes
  - Servidores Proxy
  - Servidores SOCKS
  - Servicios de Conversión de direcciones de red (NAT)
  - Software de anotaciones y supervisión
  - Servicios de Red privada virtual (VPN)

3.5.1 POLÍTICAS DE SEGURIDAD.

Consiste en determinar los principios generales en los que debe basarse el diseño de un sistema de seguridad, en nuestro caso un firewall:

- Política Principal: Todo aquello que no está expresamente permitido está prohibido
- Política de Diseño: Encaminada a la minimización y la simplicidad.
- Política de Escepticismo: Tras dotar al firewall de todas las protecciones disponibles se toma en consideración que se pueden desarrollar nuevas técnicas y que ningún grado de seguridad es absoluto.

Depende más que todo de los servicios que esta presta y del contexto en el cual esta. No es lo mismo diseñar un firewall para una ISP o una universidad que para proteger subdivisiones dentro de una empresa.

3.5.2 REGISTRO DE OPERACIONES.

Como ya dijimos anteriormente, el firewall podía ser utilizado para obtener datos estadísticos acerca de la afluencia entre ambas redes. Pues bien, para poder realizar esta estadística deberá recoger, como mínimo, la siguiente información y almacenarla en algún fichero:

- Service Information - fecha, y hora.
- Remote Information - dirección IP del presunto intruso, así como el puerto
- y el protocolo utilizado.
- Local Information - dirección IP de destino y puerto.
- Filter Information - actuación del filtro y qué adaptador de red lo hizo.
- Packet Information - encabezamiento e información del paquete.

3.5.3 INTERFACES.

Con una política de seguridad lo suficientemente hermética y un firewall eficaz, el mayor riesgo provendrá de un error humano del administrador del firewall. Estos pueden incorporar un gran número de funciones que complican su trabajo de administración.

Los firewalls que cuentan con una buena interfaz reducen la posibilidad de errores humanos y simplifican el trabajo del administrador del firewall. Una interfaz fácil de

utilizar y con un número mínimo de opciones de configuración reduce la posibilidad de que se produzcan errores de administración. Naturalmente, un número menor de opciones de configuración puede significar también menor flexibilidad de configuración.

Existen tres clases de interfaz del administrador de firewalls:

- Administración basada en ficheros de texto.
- Administración basada en menús de texto.
- Administración basada en GUI.

La interfaz basada en ficheros de texto es la de uso más extendido en lo que respecta a los firewalls de elaboración propia. Este tipo de interfaces permiten
Al administrador editar un archivo específico donde puede introducir parámetros de configuración específicos. Se trata de la interfaz de elección para los administradores de sistemas UNIX tradicionales, dado que ofrece una interfaz de control a bajo nivel con los mecanismos del firewall. La desventaja de dicho control a bajo nivel es que resulta mucho más fácil cometer errores, ya que, al editar un fichero, pueden producirse errores de escritura u otros errores técnicos que, en un sistema basado en menús, es menos probable que ocurran.

La interfaz de administrador basada en menús de texto presenta un menú basado en texto que reduce la probabilidad de producirse errores pero que proporciona menor capacidad de control para el administrador. Sin embargo, la posibilidad de error no queda totalmente excluida, dado que el administrador no siempre puede ver el efecto de algunos cambios.

La interfaz gráfica de usuario, o GUI, para administradores incorpora ventanas, botones, menús desplegables y pantallas de ayuda que facilitan el trabajo de configuración. La mayoría de proveedores ha optado por incluir esta interfaz en sus productos, puesto que tiende a ser más fácil de utilizar y no es susceptible a muchos de los errores que pueden producirse en los otros dos tipos de interfaz.

3.5.4 AUTENTICACIÓN DE USUARIOS.

La dirección IP del host origen se emplea para efectuar el control básico de acceso. Sin embargo, esta dirección puede ser suplantada fácilmente, especialmente por hosts que forman parte de la misma red. Además, en el caso de conexiones procedentes de hosts multiusuario, la dirección de éstos no permite distinguir un usuario de otro. La mayoría de firewalls a nivel de aplicación soportan la

autenticación de usuarios para algunos servicios de red. Para ello, el firewall interrumpe la conexión y solicita a los usuarios que se identifiquen antes de continuar la conexión hacia el destino deseado.

Sin embargo, la mayoría de protocolos de servicio de red no toleran dicha interrupción y, por lo tanto, no pueden soportar los métodos de autenticación, como contraseñas y tarjetas inteligentes. Otros protocolos como el correo electrónico o los grupos de noticias no establecen una conexión directa con el usuario, por lo que no es posible solicitar información para la identificación.

Los servicios de red estándar que contemplan la posibilidad de que un firewall pueda realizar funciones de autenticación son Telnet y FTP. Algunos firewalls soportan también la autenticación para los servicios X11 y HTTP.

Los mecanismos estándar de autenticación que ofrecen los firewalls en la actualidad son contraseñas convencionales, tarjetas inteligentes y servicios S/Key.
El mecanismo de contraseñas convencional emplea contraseñas multiuso y no es recomendable utilizarlo en Internet porque las contraseñas pueden ser interceptadas y empleadas más adelante por un intruso. Las tarjetas inteligentes verifican la identidad de un usuario devolviendo una respuesta única basada en un número aleatorio, que proporciona el firewall. Los usuarios responden introduciendo el número en un dispositivo autentificador, que calcula la respuesta apropiada.

3.5.5 CORRELACIÓN DE DIRECCIONES.

Antes de producirse el auge de Internet, muchas organizaciones poseían redes privadas desprovistas de conexión con otras redes también privadas. Como estaban aisladas entre sí, no tenían que solicitar a las autoridades de Internet direcciones de red no utilizadas. En lugar de ello, escogían cualquier clase de dirección IP que les apetecía.

Con el advenimiento de la Internet como parte de la infraestructura global, estas organizaciones han comenzado a conectarse a Internet y no pueden utilizar las mismas direcciones porque probablemente ya han sido asignadas a otro usuario. Naturalmente, las organizaciones podrían solicitar una clase de dirección única, pero resultaría muy costoso cambiar todas sus computadoras y es difícil obtener las direcciones IP.

Otra solución consistiría en que el firewall correlacionara direcciones orígenes legales con direcciones de Internet legales en el momento que abandonan la

intranet interna. En esta situación, es necesario des correlacionar la dirección de destino de los paquetes de retorno o restaurarla a la dirección original.

Una razón plausible para tener o mantener direcciones ilegales en la red es que puede poner trabas a los intrusos que hayan podido entrar en la misma evitando el firewall. En este caso, los paquetes del intruso pueden encontrar dificultades para llegar a la red, ya que los protocolos de direccionamiento estándar los dirigirán

hacia el propietario de la dirección real. Ésta es una protección adicional mínima y, probablemente, no compensa la reducción de la velocidad y el aumento de la complejidad al tener que correlacionar todas las direcciones.

3.5.6 RESTRICCIONES DE DÍA Y HORA.

La política de seguridad puede variar en función de del día de la semana y la hora del día. Por ejemplo, es posible permitir transferir archivos a Internet durante las horas laborales normales, aunque no durante los fines de semana o después de las 6 de la tarde. Algunos firewalls permiten basar las reglas de acceso o listas de acceso en la hora del día y el día de la semana.

3.5.7 CONTROL DE LA CARGA.

El control de la carga es una característica que ofrecen muy pocos firewalls. Para la mayoría de estos, cuando se permite el acceso, el host o la red pueden efectuar un número ilimitado de conexiones. Es útil poder establecer limitaciones al número de conexiones simultáneas con un host o una red de hosts que puede haber activas. Esta característica puede ayudar a impedir ataques por inundación, mediante los cuales un pirata informático inunda la red con conexiones a fin de ocultar el ataque real.

3.5.8 CANALIZACIÓN.

La canalización es la capacidad de combinar múltiples servicios de aplicación en una única conexión. Los intrusos emplean en ocasiones esta técnica para disfrazar un servicio no autorizado (por ejemplo, FTP) como servicio autorizado (como el correo electrónico).
Un firewall puede proporcionar también la característica de canalización para permitir a dos sitios de una compañía compartir servicios en Internet que no serían autorizados normalmente a través del mismo.

3.6 VENTAJAS DE LOS FIREWALLS.

Mantiene alejados a los piratas informáticos de la intranet al mismo tiempo que permite acceder a todo el personal de la oficina. (PROTECCION DE LA RED).

Al encargarse de filtrar, en primer nivel antes de que lleguen los paquetes al destino interno en nuestra red, el firewall es idóneo para implementar en los controles de acceso. (CONTROL DE ACCESO A LOS RECURSOS DE LA RED)

Permite bloquear el material no adecuado, determinar los sitios que puede visitar el usuario de la red interna y llevar un registro. (CONTROL DE USO DE INTERNET)

Facilita la labor a los responsables de seguridad, dado que su máxima preocupación es encarar los ataques externos, vigilar y mantener un monitoreo del trafico tanto del interior hacia el exterior y viceversa. (CONCENTRA LA SEGURIDAD).

Permite controlar el uso de Internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas. (CONTROL Y ESTADISTICAS)

Permite al administrador de la red definir un embudo manteniendo al margen a los usuarios no autorizados fuera de la red, prohibiendo potencialmente la entrada o salida de trafico prohibido de la red. (CHECK-POINT)

3.7 TIPOS DE FIREWALLS.

Existen tres tipos fundamentales de firewalls, pudiendo catalogarse en función al nivel en el que se encuentren. Esto no siempre es cierto ya que un firewall, para ser completo, deberá estar presente en todos los niveles.

3.7.1 FILTRADOR DE PAQUETES (PACKET FILTER).

Cada computadora de una red tiene una dirección comúnmente llamada dirección IP. Un firewall de filtración de paquetes verifica la dirección de donde proviene el tráfico entrante y rechaza cualquier tráfico que no coincida con la lista de las direcciones confiables. El firewall de filtración de paquetes utiliza reglas para negar el acceso, según la información contenida en el paquete, como, por ejemplo: el número del puerto TCP/IP, la dirección IP de la fuente/origen o el tipo de datos. Las restricciones pueden ser tan estrictas o tan flexibles como se requiera.

Un router común de una red puede filtrar el tráfico por dirección, pero los hackers tienen un pequeño truco llamado spoofing de IP, con el cual los datos parecen prevenir de una fuente confiable o incluso de una dirección de su propia red. Desafortunadamente el firewall de filtración es propenso al spoofing de IP y son muy difíciles de configurar. Cualquier error en su configuración puede dejarlo vulnerable a los ataques.

El filtrador de paquetes va a analizar la información contenida dentro de los paquetes IP antes de permitirles el acceso o no al ordenador. Para ello va a coger los paquetes IP y les va a aplicar unas reglas de filtrado.
Algunos firewalls de este estilo permiten establecer también filtros a nivel de puertos, con lo que podremos determinar qué servicios dejamos pasar y cuáles no. Además, algunos routers utilizan el BIT de ACK del protocolo IP para el reconocimiento de la conexión. Cuando este BIT está activo, quiere decir que el paquete está esperando la respuesta de otro paquete anterior que hemos lanzado nosotros. Usando esta técnica algunos firewalls permiten pasar cualquier tipo de información, pero “si y solo si” la comunicación ha sido iniciada por una máquina interna.

El firewall va a contener en su interior una lista de filtros a aplicar. Estos filtros se aplican a los paquetes secuencialmente, de forma que si el paquete es aceptado por uno de ellos pasará al sistema, mientras que si no es así se le aplicará el siguiente filtro. Como es obvio, el último filtro no va a permitir el acceso a nada.

3.7.2 SERVIDOR PROXY A NIVEL DE APLICACIÓN.

Es el extremo opuesto a los filtradores de paquetes. En lugar de filtrar el flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado en cada uno de ellos. Es probablemente el sistema más seguro, ya que no necesita utilizar complicadas listas de acceso y centraliza en un solo punto la gestión del servicio, además de que nos permitirá controlar y conocer información de cada uno de los servicios por separado.

Un servidor Proxy a nivel de aplicación examina la aplicación usada por cada paquete IP, con el fin de verificar su autenticidad. El tráfico de cada aplicación, tales como Http para la Web, FTP para la transferencia de archivos y SMTP/POP3 para el E-mail, por lo general, requieren de la instalación y configuración de un Proxy de aplicaciones diferente. Con frecuencia, los servidores requieren que los administradores reconfiguren su red y aplicaciones para soportar el Proxy lo cual puede resultar en un proceso muy trabajoso.

Este tipo de firewalls es la única solución efectiva para el tratamiento de servicios cuya conexión debe ser iniciada desde el exterior. Servicios como FTP, Telnet o E-Mail deberán tratarse con esta categoría de firewall.

En realidad, lo que suele hacerse a la hora de trabajar con este sistema de protección es establecer una puerta de acceso para cada servicio. Como esta puerta es de uso obligatorio, podemos establecer sobre ella los criterios de control que mejor nos convengan. Una vez sobrepasada la puerta, puede ocurrir que la propia pasarela ofrezca el servicio de forma segura o que se establezca una conexión con un ordenador interno que realmente ofrezca el servicio, teniendo a éste último configurado para aceptar conexiones tan solo de dentro a afuera.

El nivel de aplicación constituye la última generación en la tecnología de firewall. Los expertos en Internet que SPI es la tecnología más avanzada y segura, gracias a que examina todos los componentes de un paquete IP para decidir si acepta o rechaza la comunicación.

El firewall mantiene un registro de todas las solicitudes de información que se originan de su red. Luego, inspecciona toda comunicación entrante para verificar si realmente fue solicitada y rechaza cualquiera que no lo haya sido.

Los datos solicitados aprobados proceden al siguiente nivel de inspección y de termina el estado de cada paquete de datos.

3.7.3 PASARELAS A NIVEL DE RED.

Se basan en el control de las conexiones TCP y su manera de actuar es la que sigue: por un lado, reciben las peticiones de conexión a un puerto TCP y por el otro se establecen las conexiones con el destinatario deseado si se han cumplido las restricciones de acceso establecidas.
Normalmente, este tipo de firewalls trabajan junto a los servidores Proxy. Si la acreditación es positiva se entabla la conexión. Por su forma de trabajar son muy adecuados para la recogida de información.
Este tipo de firewalls suele ser el más adecuado para el tratamiento de conexiones salientes, y con él no será nada complicado establecer restricciones sobre los ordenadores a los que se puede acceder o limitar el máximo de accesos permitidos.

3.7.4 FIREWALLS CON ZONA DESMILITARIZADA (DMZ).

Un firewall que provee protección DMZ es una solución efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red a partir de cualquier medio externo, ya sea a través de Internet o cualquier otra ruta, como, por ejemplo, una compañía de hosting de Web o que vende sus productos o servicios por Internet.

La decisión de optar por un firewall con DMZ debe basarse con la cantidad de usuarios externos que accedan a la red y la frecuencia con la que lo hacen. Un firewall con DMZ crea un área de información protegida (desmilitarizada) en la red, los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red.
Esto permite a los usuarios externos acceder a la información que usted quiere que vean, pero previene que obtengan información no autorizada.

3.8 ALGUNAS HERRAMIENTAS DEL HACKER EN CONTRA DEL FIREWALL.

El protocolo SNMP (Simple Network Manager Protocol) que puede ser usado para examinar la tabla de ruteo que usa la intranet, y conocer de esta manera la topología de la red.

El programa TraceRoute que puede revelar detalles de la red y de los enrutadores.

El protocolo Who is, que es un servicio de información que provee datos acerca del servidor de nombres de la intranet.

El acceso al servidor DNS que podría listar los IP's de los diferentes hosts de la intranet y sus correspondientes nombres.

El protocolo Finger, que puede revelar información sobre los usuarios (como su login, sus números telefónicos, la fecha y hora de la última logueada, etc.…)

El programa ping, que puede ser empleado para localizar un host particular, y al correrlo a menudo en diferentes IP's construir una lista de los host residentes actualmente en la red.

3.9 IMPLEMENTACIÓN Y CONFIGURACIÓN DE FIREWALLS.

Formas de implementación de Firewall hay muchas, dependiendo de gustos y necesidades, como lo es un Proxy, siendo posiblemente la fórmula más utilizada.
Los Firewalls son la primera línea de defensa frente a los atacantes, estos componentes deben estar óptimamente configurados para ser efectivos, de lo contrario es posible que un atacante aproveche las vulnerabilidades para lograr entrar a la red interna.
El diseño de un firewall, tiene que ser el producto de una organización consciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por MODEM (dial-in MODEM calling).

CAPÍTULO 4. FILTRADO DE CONTENIDO WEB.

Poco a poco, Internet se está convirtiendo en un elemento imprescindible para las empresas, las escuelas y los hogares. Sin embargo, la incorporación de este medio a nuestra realidad diaria nos hace plantear nuevas necesidades y nuevas situaciones ya que son cada vez más las noticias que surgen sobre la exposición de los niños a contenidos nocivos, mucho más que antes, los empleados de oficinas evolucionan de los tradicionales juegos del solitario, hacia otros juegos electrónicos tales como Quake, EverQuest y Snood durante sus horas laborales. De hecho, más de la mitad de los administradores de sistemas reportan que sus empleados acceden desde sus oficinas a portales de juegos en la Internet.

En el mercado existen sistemas de filtrado de accesos a Internet, para asegurar una navegación segura de los menores y empleados. Se pueden instalar tanto en el hogar en la empresa, así como en los centros educativos.

4.1 ¿QUÉ ES EL FILTRADO DE CONTENIDO WEB?

En informática, un filtro de contenido, se refiere a un software o hardware diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.

El filtro de contenido determina qué contenido estará disponible en una máquina o red particular. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable. Cuando se impone sin el consentimiento del usuario, puede constituir censura.

Los usos comunes de estos programas incluyen padres que desean limitar los sitios que sus hijos ven en sus computadoras domésticas, escuelas con el mismo objetivo, empleadores para restringir qué contenidos pueden ver los empleados en el trabajo, etc.

Esta función permite el filtrado de paquetes, examina los paquetes de comunicación que intentan pasar a través del firewall, comparándolos con las reglas. Las reglas determinan cómo se maneja la comunicación. Estas reglas están basadas en la dirección IP de origen de los datos y el puerto a que se destina.

El filtrado de contenidos permite a los administradores bloquear fácilmente algunos tipos de contenido web sin tener que hacerlo manualmente con cada URL individual.

Un filtro es un programa de ordenador que causa una separación efectiva entre los contenidos nocivos que están en Internet (como puede ser la pornografía, contenidos de violencia, sectas, racismo, etc.) y las personas que navegan por Internet.

El programa se pone en marcha para que la persona no llegue a tener acceso a dicho material. Si el contenido de la página pertenece a una de las categorías consideradas no aptas por el sistema (pornografía, violencia, y racismo son las más comunes, pero eso dependerá de cada programa) dicha página no aparece en la pantalla de la computadora. De este modo, los contenidos nocivos no pueden llegar a las personas.

4.2 ¿CÓMO FUNCIONAN?

Existen hoy en día en el mercado diversas técnicas de selección y filtrado de contenidos capaces de evitar que los materiales nocivos que están en Internet, como es la pornografía, lleguen al ordenador de una casa o de una oficina:

- Herramientas de control de acceso y monitoreo para la PC.
- Herramientas de control y de acceso en el proveedor de Internet.
- Clasificación y filtrado de contenidos

4.3 HERRAMIENTAS DE CONTROL DE ACCESOS Y MONITOREO.

Existe en la actualidad una extensa gama de herramientas de control de accesos y monitoreo capaces de bloquear el acceso a contenidos no apropiados para las personas. Estas herramientas pueden variar mucho según los métodos empleados y la facilidad de configuración por parte de los usuarios.

Estas herramientas funcionan de distintas maneras para evitar que los contenidos nocivos que están en Internet lleguen a las personas:

- Bloqueando direcciones de páginas web que contengan dichos contenidos controlando horas de acceso.

- Aceptando listas de direcciones predeterminadas.
- Permitiendo establecer una lista propia de direcciones aceptadas o negadas.
- Asignando diferentes perfiles en diferentes días y horas (trabajo, tiempo libre, etc.).
- Permitiendo regular qué servicios se pueden utilizar en cada momento y por cada usuario (correo, chat, etc.), etc.

Los precios de estos productos varían de acuerdo con sus funciones y configuraciones y casi todos ellos pueden ser adquiridos a través de la Red.

4.3.1 LISTAS POSITIVAS Y NEGATIVAS.

Tales herramientas pueden partir de una lista predeterminada de páginas prohibidas, el programa no permite el acceso a las páginas que están incluidas en esta lista, o de una lista de páginas permitidas, a través del cual sólo se permite el acceso a páginas que estén incluidas en esta lista.

Las listas deben actualizarse periódicamente para que el programa pueda funcionar eficazmente, ya que a cada día miles y miles de páginas nuevas son creadas. Algunas empresas permiten que las actualizaciones se hagan de forma gratuita desde la Red y otras cobran por cada actualización.

4.3.2 RECONOCIMIENTO DE PALABRAS CLAVE.

Hay programas que utilizan ciertas palabras para realizar el bloqueo, no permitiendo el acceso a páginas que contengan dichas palabras. Sin embargo, en estos casos el software bloquea palabras aisladas y que no están en un contexto determinado, por ejemplo, algunas palabras clásicamente incluidas en estas listas son marihuana, sexo, etc. Un programa puede llegar a bloquear una página de educación sexual solamente porque incluya la palabra "sexo.

4.3.3 EL ANÁLISIS SEMÁNTICO.

El análisis semántico es una técnica distinta al bloqueo de palabras clave. El análisis semántico no está basado en el reconocimiento de palabras sino en tecnologías de inteligencia artificial. Utilizando esta tecnología se realiza un verdadero análisis semántico con resultados completamente distintos a los obtenidos con el reconocimiento de palabras.

Hay hoy en día en el mercado, productos como Puresight, un producto israelí, que utilizan este tipo de tecnología.

4.3.4 MONITOREO.

Hay algunos programas que permiten hacer un rastreo del tiempo que pasan las personas navegando y las páginas que visitan.

Además, hay aplicaciones que permiten bloquear la información que entra en la computadora, tal como emails, y otros que permiten el bloqueo a la información de salida a Internet, como puede ser el caso de datos personales, impidiendo que las personas respondan encuestas.

4.3.4 HERRAMIENTAS DE CONTROL DE ACCESO EN EL PROVEEDOR DE INTERNET.

En este método, el usuario utiliza el sistema de filtrado que tenga instalado el ISP (Proveedor de Servicios de Internet), sin necesidad de instalar un programa en la computadora que se utiliza.

4.3.5 CLASIFICACIÓN DE PÁGINAS MEDIANTE ETIQUETAS PICS.

Este sistema se basa en que los proveedores de contenidos de Internet, o sea, las personas que tienen páginas web en Internet, pongan unas etiquetas a las páginas que crean especificando el tipo de contenido de dichas páginas.

Posteriormente los administradores de red, padres y educadores pueden configurar el navegador para que se permita el acceso únicamente a aquellas páginas con etiquetas que identifiquen que el tipo de contenido no es nocivo para las personas. El sistema funciona más o menos como el utilizado por los productores de alimentos enlatados. En el rótulo de cada lata de alimento se dice exactamente los ingredientes que fueron utilizados para la elaboración de dicho alimento.

4.4 LOS FIREWALLS Y LOS METODOS DE FILTRADO.

El filtrado de paquetes juega un papel fundamental dentro de la operación de cada uno de los cortafuegos de hardware. Para ello, el firewall se configura manualmente de acuerdo a unas normas para saber qué paquetes debe dejar pasar y cuáles no. El filtrado tiene lugar en las capas OSI 3 y 4, es decir, la capa de red y la capa de transporte, donde comprueba las propiedades de los paquetes al tomar el encabezado de cada protocolo. Dependiendo de las normas, las direcciones IP o los puertos exactos, por ejemplo, serán permitidos o bloqueados.

Con el modelo de puente anteriormente mencionado o con un conmutador, que representa una extensión del primero, el filtrado de paquetes se puede realizar en la capa de enlace de datos, es decir, la segunda capa del modelo OSI. Con este, el filtrado de paquetes no se basa en direcciones IP, sino en direcciones MAC**,** que se utilizan para el direccionamiento del hardware.

Por extensión, los cortafuegos también pueden realizar filtrado de paquetes con métodos de verificación basados en seguimiento de estado (Stateful Packet Inspection, SPI). Para ello, el proceso de filtrado tiene lugar en la capa 3 y 4, así como en la capa de aplicación (capa 7), incluyendo los datos intercambiados. A diferencia de los proxy firewall, que también tienen acceso a la séptima capa de aplicación, la técnica SPI no permite modificar estos datos.

CAPÍTULO 5. IMPLEMENTACIÓN DE FILTRADO DE CONTENIDO.

5.1 ESTADO ACTUAL.

Actualmente se tienen 2 conexiones de internet una para la red de operación y otra para los clientes.

Se cuenta con una conexión de 1000 Mb/s para la red de operación y 10 Mb/s para la red de clientes.

El proveedor de internet entrega el servicio en un pequeño site con un router que está conectado al switch que alimenta a los puntos en donde se requiere la red operativa

Aproximadamente existen 15 puntos de conexión para las maquinas operativas mediante cable, además de tener aproximadamente 25 puntos más de conexión mediante Wifi. (3 access point), el direccionamiento ip de la red es 172.10.2.0/24

De los puntos de acceso existen grupos (VLAN), los cuales debido a su nivel de jerarquía de la empresa se dividen como

- VLAN 2 Dirección general
- VLAN 3 Gerentes
- VLAN 4 Operadores
- VLAN 5 Visitas

Actualmente todos los niveles de jerarquía tienen los mismos permisos y accesos para internet, no existe ninguna herramienta que les permita o les impida visitar ciertas paginas o descargar cualquier cosa de internet. Por favor referirse al **anexo 1** diagrama de red

5.2 PROBLEMÁTICA.

Se ha detectado que un gran número de usuarios ocupan el recurso de Internet para fines no laborales, como lo son: las redes sociales, el servicio de audio y video por suscripción (Netflix, Blim, Amazon, Claro video, Spotify, Apple music etc.), video en YouTube, la pornografía, sistemas de descarga de archivos y otros más, esto limita las actividades y la eficiencia de cada usuario y afecta de manera directa al resto de la intranet al verse reducida la capacidad de ancho de banda.

Mediante un sondeo con un aplicativo de escucha (sniffer) se ha obtenido una lista de porcentajes por cada usuario de las actividades realizadas en Internet evidenciando el mal uso del mismo.

Tomando una muestra de las páginas visitadas obtenemos lo siguiente:

- Servicios de audio y video por suscripción 95%
- Pornografía 80%
- Redes sociales 95%
- Descarga de archivos 70%
- YouTube 90%
- Videos en streaming 70%

Al observar estos porcentajes notamos que el servicio de Internet no está siendo utilizado de la forma más adecuada y el ancho de banda se ve limitado para el resto de las actividades que se deben realizar, como descarga de material con el cual se realizan procesos de trabajo.

Esto afecta directamente en el desempeño de los trabajadores, así como en el uso del ancho de banda real para cuestiones operativas.

5.3 SOLUCIÓN.

De acuerdo a la problemática ya planteada en conjunto con el departamento de sistemas, se dio a la tarea de evaluar el estado actual de la red y se acordó el implementar un firewall en el SITE entre el router que entrega la compañía de servicios de internet y el switch encargado de proveer distribuir el internet en la compañía.

Se realizó el diseño y evaluación de las políticas de red que más favorecieran el adecuado uso del ancho de banda, también las que limitaran el uso de los recursos web como los mencionados en la problemática y las que prohibieran el manejo de aplicaciones dañinas, ociosas y del rango no laboral.

Las políticas diseñadas se aplicarán a todos los usuarios por igual sin excepción alguna.

Se evaluaron las marcas y modelos de firewalls de acuerdo con características, prestaciones y precios y se llegó a la conclusión de adquirir un firewall marca mikrotik. Por favor refiérase al **anexo 3**

Este firewall fue el indicado para que mediante él pudiéramos aplicar adecuadamente las políticas diseñadas y así poder realizar un filtrado de contenido web eficiente.

Ya instalado físicamente el firewall se conectó por medio de un cable UTP proveniente del router a la Interface WAN que es la llegada del enlace de internet y una conexión de cable UTP de la Interface LAN hacia el switch de la LAN de la compañía, refiérase por favor al anexo diagrama 2 modificación de la red.

Después se procede a la configuración interna de las interfaces físicas y lógicas, la configuración de permisos para administrar dicho firewall creando cuentas administrativas con diferentes perfiles etc. Para esto se crea un plan de network en el cual se recolecta cierta información como lo es el direccionamiento IP de las interfaces WAN Internal, este plan también contiene las direcciones del Gateway a ocupar, el direccionamiento del servidor de nombres de dominio y sus direcciones primarias y secundarias, lo anterior se representa en la tabla 1.

Tabla 1. Direccionamiento IP.

Direccionamiento IP		
Internet		
WAN	10.10.10.1	255.255.255.0
LAN	172.10.2.1	255.255.255.0
Roles		
Admin	xxxxxxxxxx	RW
Soporte	yyyyyyyyyy	R
Red	172.10.2.0	255.255.255.0
DNS	primario	8.8.8.8
	secundario	8.8.2.2
DHCP	172.10.2.1	
VLAN_DIRECCION	172.10.2.2 - 172.10.2.5	3
VLAN_GERENTES	172.10.2.6 - 172.10.2.10	5
VLAN_OPERADORES	172.10.2.11 - 172.10.2.35	25
VLAN_VISITAS	172.10.2.36 - 172.10.2.50	15

Ilustración 5.1 Direccionamiento IP

Políticas de filtrado de contenido.

Estas son implementadas bajo 5 vertientes; Media, pornografía, redes sociales, juegos descargas. La siguiente tabla 2 nos refiere la política de filtrado

Se están utilizando la técnica de filtrado de contenido de expresiones regulares.

Media: YouTube, Netflix, Blim, Amazon, Claro video, Spotify, Apple music
Pornografía: Paginas de pornografía en general
Redes Sociales: WhatsApp, Facebook, Instagram, Messenger, twitter, snapchat.
Juegos: Juegos.com, freegames, mini juegos, gamers.com,kizzi.com
Descargas: MediaFire, Rappidshare, freakshare, Mega,4shared.

Tabla 2. Políticas de Permisos.

Políticas de Permisos					
Área	**Media**	**Pornografía**	**Redes sociales**	**Juegos**	**Descargas**
Dirección general	✔	✔	✔	✔	✔
Gerentes	✔	✘	✔	✘	✔
Operadores	✘	✘	✘	✘	✘
Visitas	✘	✘	✘	✘	✘

Ilustración 5.2 Políticas de permisos

Tabla 3. Expresiones regulares.

Media	Pornografía	Redes sociales	Juegos	Descargas
^.+(youtube.com).*$	^.+(pornhub.com).*$	^.+(facebook.com).*$	^.+(ubisoft.com).*$	^.+(4share.com).*$|
^.+(spotify).*$	^.+(youporn.com).*$	^.+(instagram.com).*$	^.+(ea.com).*$	^.+(media.com).*$
^.+(vimeo.com).*$	^.+(redtube.com).*$	^.+(snapchat.com).*$	^.+(nintendo.com).*$	^.+(rapidshare.com).*$
^.+(netflix.com).*$	^.+(xhamster.com).*$	^.+(twitter.com).*$	^.+(playstation.com).*$	^.+(softonic.com).*$
^.+(prime.com).*$	^.+(aztecaporno.com).*$	^.+(tinder.com).*$	^.+(xbox.com).*$	^.+(cnetdownload.com).*$
^.+(blim.com).*$	^.+(elephanttube.com).*$	^.+(tumblr.com).*$	^.+(blizzard.com).*$	^.+(sourceforge.net.com).*$
^.+(clarovideo.com).*$	^.+(muyzorras.com).*$	^.+(wechat.com).*$	^.+(riotgames.com).*$	^.+(uptodown.com).*$
^.+(pelispedia.net).*$	^.+(xvideos.com).*$	^.+(qq.com).*$	^.+(bethesda.com).*$	^.+(filehippo.com).*$
	^.+(xnxx.com).*$	^.+(qzone.com).*$	^.+(e3expo.com).*$	^.+(softpedia.com).*$
	^.+(videoscaseros.com).*$	^.+(weibo.com).*$	^.+(505games.com).*$	^.+(downloads.zdnet.com).*$
	^.+(brazzers.com).*$	^.+(plusgoogle.com).*$	^.+(gamespot.com).*$	^.+(majorgeeks.com).*$
	^.+(realitykings.com).*$	^.+(plus.google.com).*$	^.+(twitch.tv).*$	^.+(sotf32.com).*$
	^.+(iknowthatgirl.com).*$	^.+(googleplus.com).*$	^.+(twitch.com).*$	^.+(brothersoft.com).*$
	^.+(mofosnetwork.com).*$	^.+(Pinterest.com).*$	^.+(atlus.com).*$	^.+(kioskea.net).*$
	^.+(naughtyamerica.com).*$	^.+(LinkedIn.com).*$	^.+(capcom.com).*$	^.+(portableapps.com).*$
	^.+(bangbros.com).*$	^.+(MySpace.com).*$	^.+(gameloft.com).*$	
	^.+(exxxtrasmall.com).*$	^.+(hi5.com).*$	^.+(2k.com).*$	
	^.+(blacked.com).*$	^.+(ning.com).*$	^.+(take2games.com).*$	
	^.+(porntube.com).*$	^.+(tagged.com).*$	^.+(epicgames.com).*$	
	^.+(eporner.com).*$	^.+(meetme.com).*$	^.+(ign.com).*$	
	^.+(babosas.com).*$	^.+(meetup.com).*$	^.+(konami.com).*$	
	^.+(pornhd.com).*$	^.+(bebo.com).*$	^.+(lienzo.com).*$	
	^.+(porn.com).*$||	^.+(multiply.com).*$	^.+(sega.com).*$	
	^.+(motherless.com).*$	^.+(skyrock.com).*$	^.+(square-enix.com).*$	
	^.+(4tube.com).*$	^.+(badoo.com).*$	^.+(tencent.com).*$	
	^.+(beeg.com).*$	^.+(twoo.com).*$	^.+(thqnordic.com).*$	
	^.+(youjizz.com).*$	^.+(taringa.com).*$	^.+(inovajuegos.com).*$	
	^.+(cnnamador.com).*$	^.+(vimeo.com).*$	^.+(gratisjuegos.com).*$	
	^.+(xnalgas.com).*$	^.+(soundcloud.com).*$	^.+(moddb.com).*$	
	^.+(sexmex.com).*$		^.+(old-games.com).*$	
	^.+(porndig.com).*$		^.+(angernet.com).*$	
	^.+(zzcartoon.com).*$		^.+(projectw.com).*$	
	^.+(hentaihaven.com).*$		^.+(dgemu.com).*$	
	^.+(hentaifox.com).*$		^.+(planetddl.com).*$	
	^.+(hentai2read.com).*$		^.+(emudesc.com).*$	
	^.+(nhentai.com).*$		^.+(guidobot.com).*$	
	^.+(hentaiid.com).*$		^.+(gba-rom-news.com).*$	
	^.+(hentaipros.com).*$		^.+(espalpsp.com).*$	
	^.+(toonpass.com).*$		^.+(juegos).*$	
	^.+(enjoy3dporn.com).*$		^.+(games).*$	
	^.+(chochox.com).*$			
	^.+(buenaisla.com).*$			
	^.+(8muses.com).*$			
	^.+(pasaelpack.com).*$||			
	^.+(puritanas.com).*$||			
	^.+(4chan.com).*$||			
	^.+(ichan.com).*$			
	^.+(openload.com).*$||			
	^.+(videowood.com).*$||			
	^.+(cam4.com).*$||			
	^.+(cams.com).*$||			
	^.+(myfreecams.com).*$||			
	^.+(xxx).*$||			
	^.+(noporn).*$			
	^.+(porn).*$||			
	^.+(porno).*$||			
	^.+(hentai).*$||			
	^.+(hentay).*$||			
	^.+(sex).*$||			
	^.+(sexo).*$||			
	^.+(poringa.net).*$			

Ilustración 5.3 Expresiones regulares

5.4 PROCEDIMIENTO DE CONFIGURACIONES.

a) ACCESO A FIREWALL.

Por medio de un cliente llamado winbox, se accesa a la configuración del firewall teniendo previamente conectado la laptop al firewall a través de un cable de red UTP a cualquier puerto ethernet del firewall. Refiérase al **anexo I**.

b) ASIGNACIÓN DE SERVICIOS A USUARIOS.

Estando dentro de la configuración del firewall nos vamos a la opción de usuarios y creamos 2 operadores uno administrador con todos los permisos y otro de monitoreo restringido de permisos. Refiérase al **anexo II**.

c) ASIGNACIÓN DE INTERFACES A LA RED WAN Y LAN.

En el siguiente paso asignamos las interfaces que vamos utilizar, el puerto 1 será la conexión con el router, el puerto 2 será la Interface LAN en donde se crearan las 4 Vlans (vlan dirección, vlan gerentes, vlan operadores y vlan visitas). Refiérase al **anexo III.**

d) ASIGNACIÓN DE DIRECCIONAMIENTO IP A LA RED.

El siguiente paso es asignar el direccionamiento IP a los puertos creados anteriormente, la interfaz WAN del puerto 1 tendrá la IP (10.10.10.1) y la interfaz LAN del puerto 2 contaran con el rango de IP (172.10.2.1-254). Refiérase al **anexo IV.**

e) ASIGNACIÓN DE DNS.

Continuando con la configuración se asignan los DNS primario 8.8.8.8 y secundario 8.8.2.2. Refiérase al **anexo V.**

f) CREACIÓN DE DHCP SERVER PARA LAS VLAN.

Se crea el servidor DHCP para las VLAN creando el pool para cada vlan para el siguiente paso. Refiérase al **anexo VI.**

g) ASIGNACIÓN DE POOL DE DIRECCIONES A LAS VLAN.

En el siguiente paso se asigna el segmento ip que tendrá cada VLAN que son los siguientes:

- Vlan dirección 172.10.2.2 – 172.10.2.5.
- Vlan gerentes 172.10.2.6 – 172.10.2.10.
- Vlan operadores 172.10.2.11 – 172.10.2.35.
- Vlan visitas 172.10.2.36 – 172.10.2.50.

Refiérase al **anexo VII.**

h) CONFIGURACIÓN DE LAS CATEGORIAS DE FILTRADO DE CONTENIDO.

En este paso se crean las categorías que se van a restringir, en el menú IP firewall y en la pestaña layer 7 protocol vamos a agregar las siguientes categorías:

- Media
- Pornografía
- Juegos
- Descarga
- Redes sociales

En cada categoría se deben poner las expresiones regulares (regex) son las encargadas de prohibir el acceso a ciertas páginas que deseamos restringir el acceso. Refiérase al **anexo VIII.**

i) APLICACIÓN DE POLITICAS DE FILTRADO DE CONTENIDO A LOS GRUPOS DE TRABAJO.

En este paso nos dirigimos a IP-firewall y en la pestaña filter rules vamos a agregar las reglas de filtrado, se seleccionara la interface, es decir; a que vlan se va a asignar esta regla (dirección, gerentes, operadores, visitas), después vamos a seleccionar la regla que creamos anteriormente en layer 7 protocol (pornografía, media, descarga, redes sociales, juegos), por último en acción le vamos a asignar “drop” lo que quiere decir que cuando tenga una solicitud para una página prohibida no va a dejar navegar por ese sitio. El criterio utilizado es: Abierto todo, cerrar con políticas. Refiérase al **anexo IX.**

5.5 PRUEBAS DE FILTRADO DE CONTENIDO POR GRUPOS (VLAN).

5.5.1 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE DIRECCIÓN.

VLAN DIRECCIÓN: RESTRICCIÓN MEDIA.

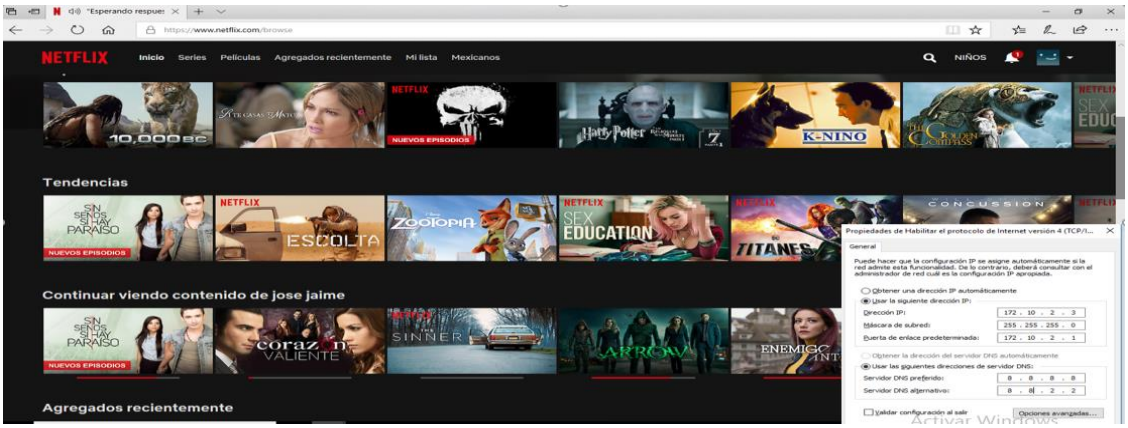


Ilustración 5.4 Restricción media

VLAN DIRECCIÓN: RESTRICCIÓN PORNOGRAFÍA.

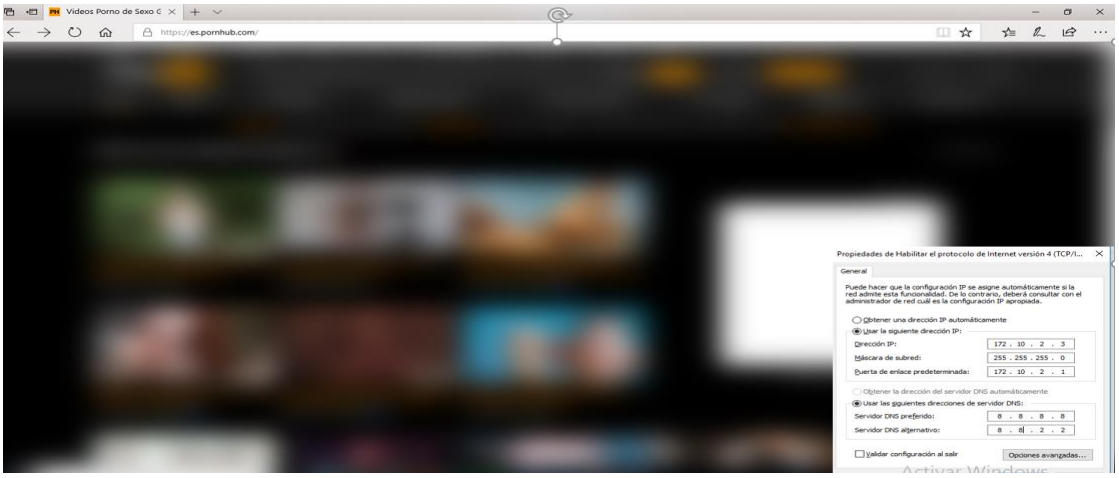


Ilustración 5.5 Restricción pornografía

VLAN DIRECCIÓN: RESTRICCIÓN DESCARGAS.

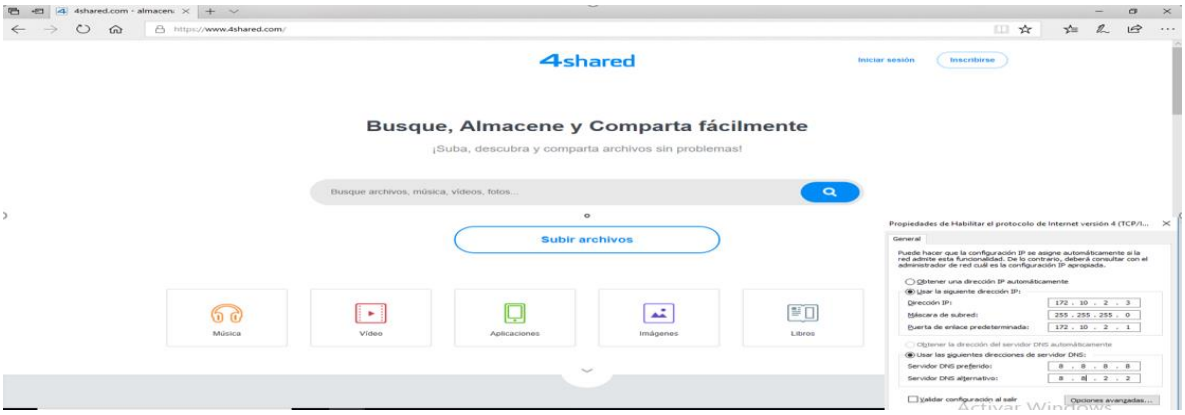


Ilustración 5.6 Restricción descargas

VLAN DIRECCIÓN: RESTRICCIÓN JUEGOS.

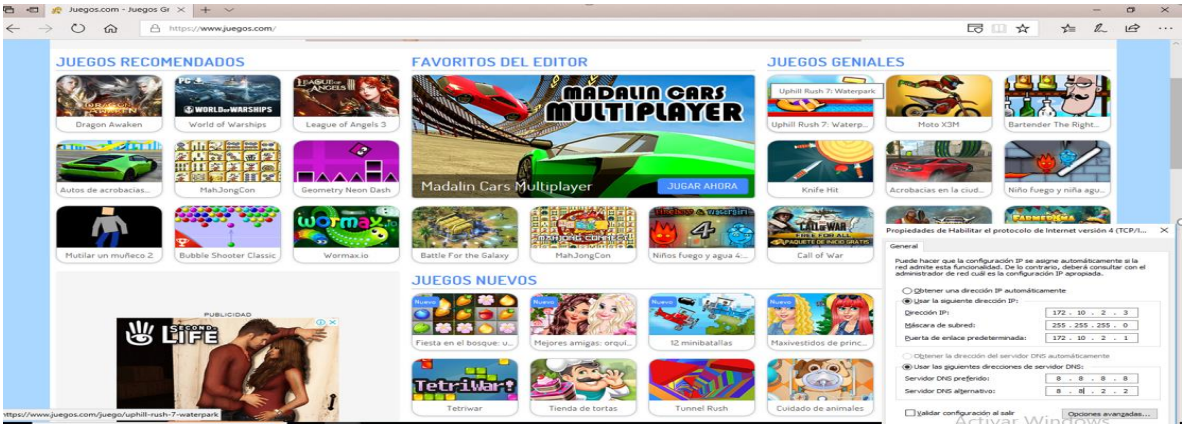


Ilustración 5.7 Restricción juegos

VLAN DIRECCIÓN: RESTRICCIÓN REDES SOCIALES.

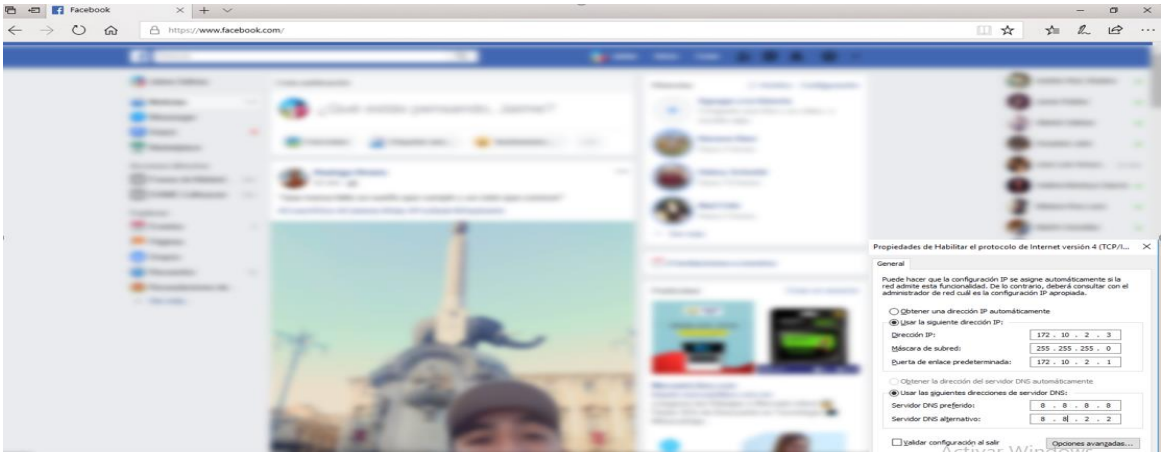


Ilustración 5.8 Restricción redes sociales

5.5.2 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE GERENTES.

VLAN GERENTES: RESTRICCIÓN MEDIA.

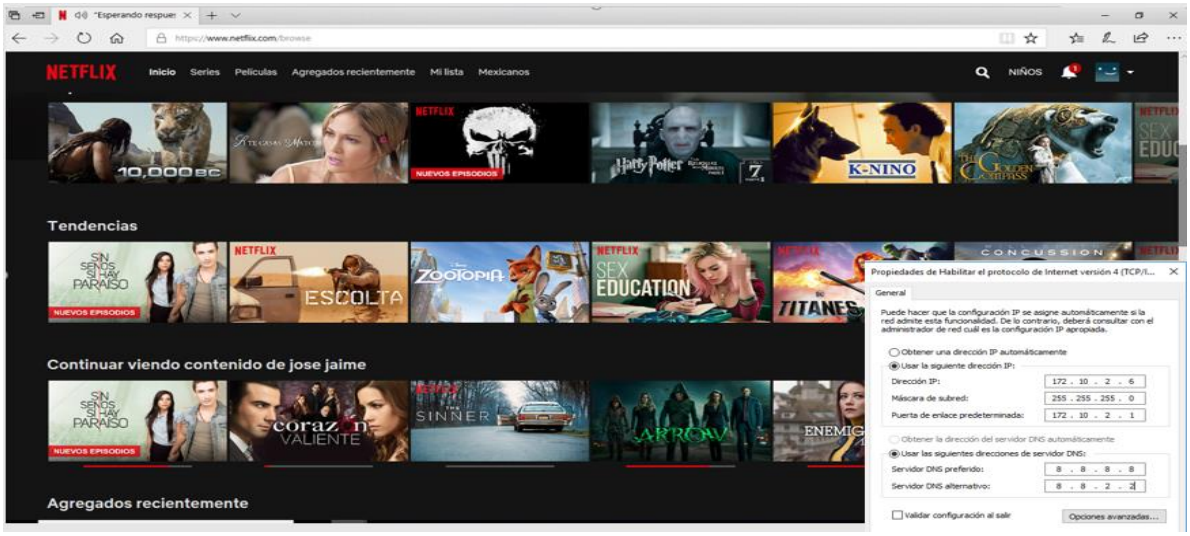


Ilustración 5.9 Restricción media

VLAN GERENTES: RESTRICCIÓN PORNOGRAFIA.

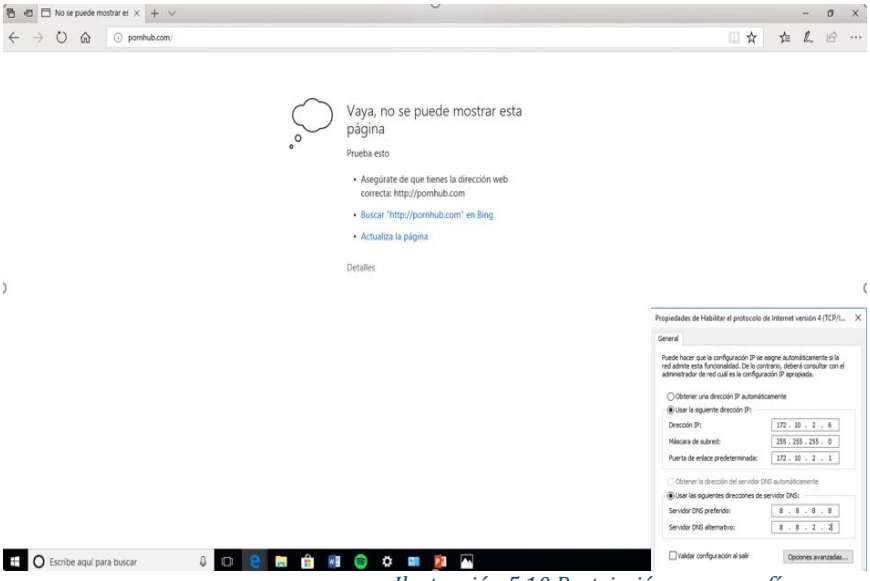


Ilustración 5.10 Restricción pornografía

VLAN GERENTES: RESTRICCIÓN DESCARGAS.

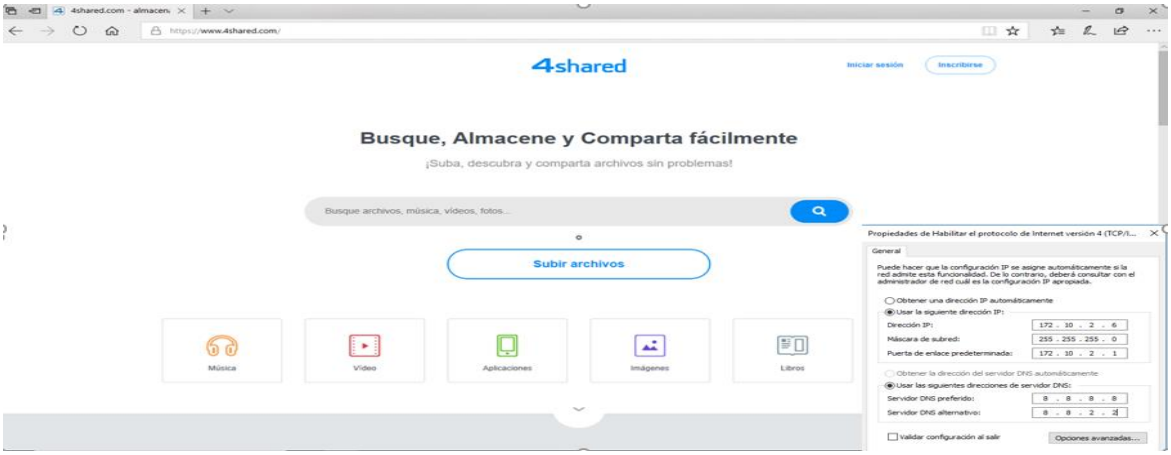


Ilustración 5.11 Restricción descargas

VLAN GERENTES: RESTRICCIÓN JUEGOS.

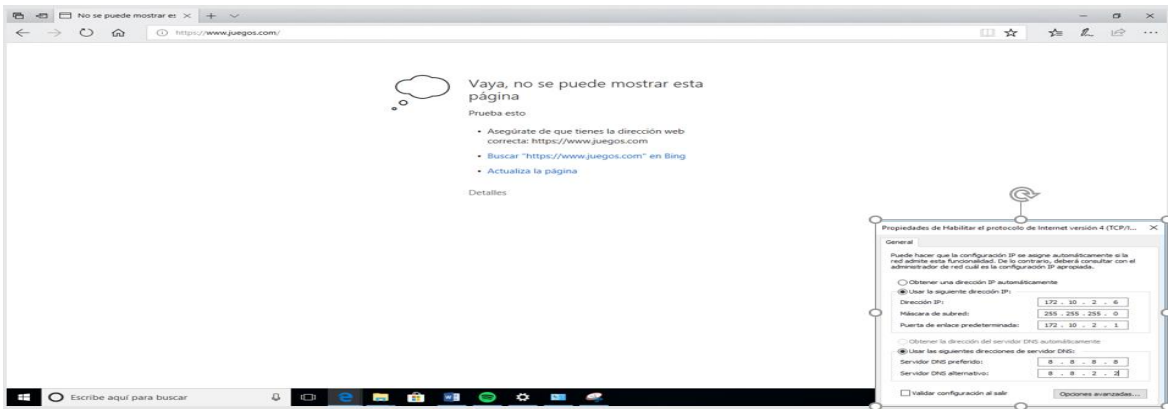


Ilustración 5.12 Restricción juegos

VLAN GERENTES: RESTRICCIÓN REDES SOCIALES.

Ilustración 5.13 Restricción redes sociales

5.5.3 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE OPERADORES.

VLAN OPERADORES: RESTRICCIÓN MEDIA.

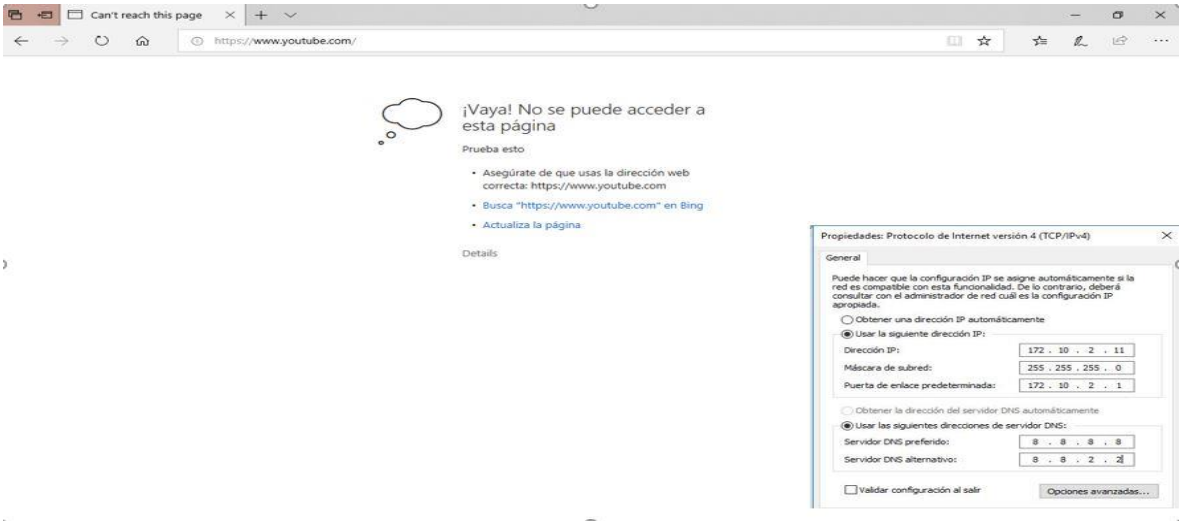


Ilustración 5.14 Restricción media

VLAN OPERADORES: RESTRICCIÓN PORNOGRAFIA.

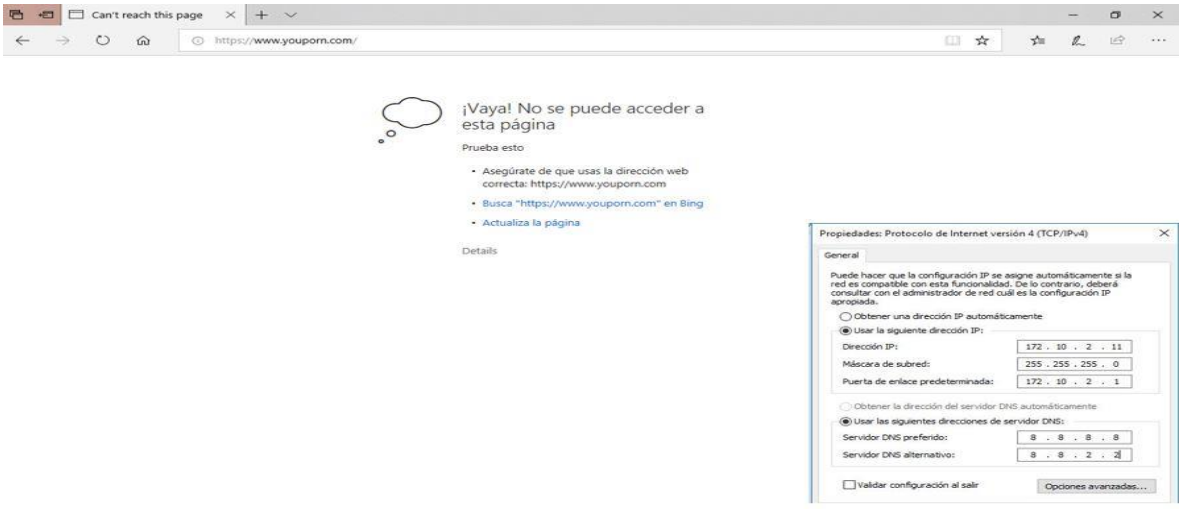


Ilustración 5.15 Restricción pornografía

VLAN OPERADORES: RESTRICCIÓN DESCARGAS.

Ilustración 5.16 Restricción descargas

VLAN OPERADORES: RESTRICCIÓN JUEGOS.

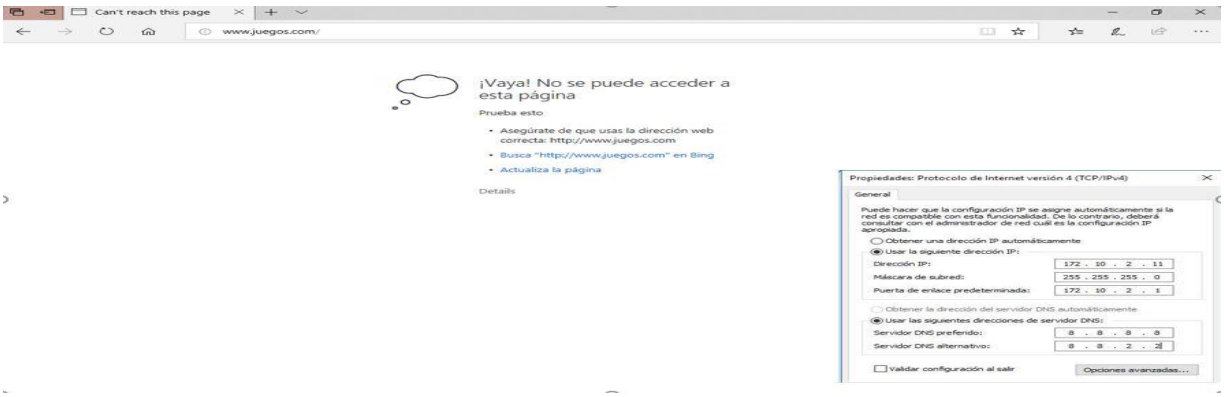


Ilustración 5.17 Restricción juegos

VLAN OPERADORES: RESTRICCIÓN REDES SOCIALES.

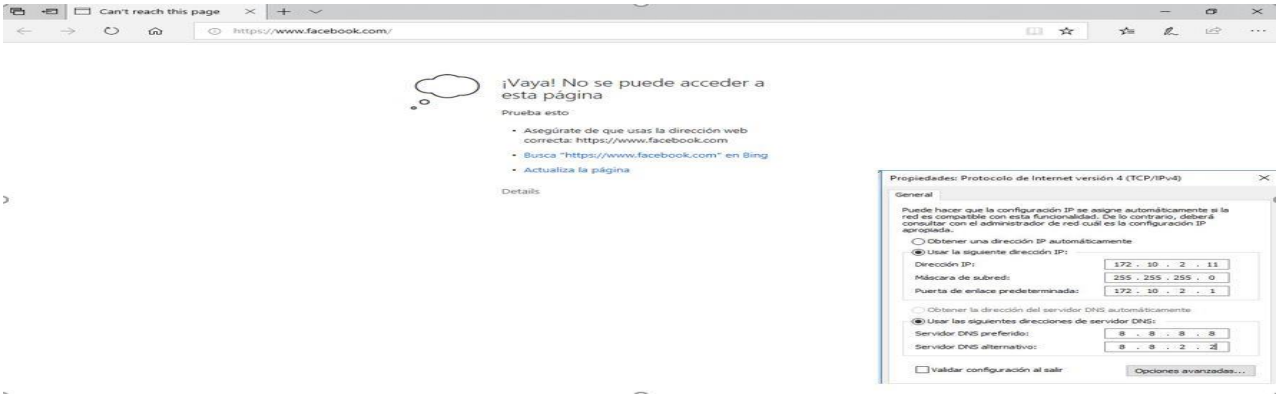


Ilustración 5.18 Restricción redes sociales

5.5.3 PRUEBA DE FILTRADO DE CONTENIDO PARA LA VLAN DE VISITAS.

VLAN VISITAS: RESTRICCIÓN MEDIA.

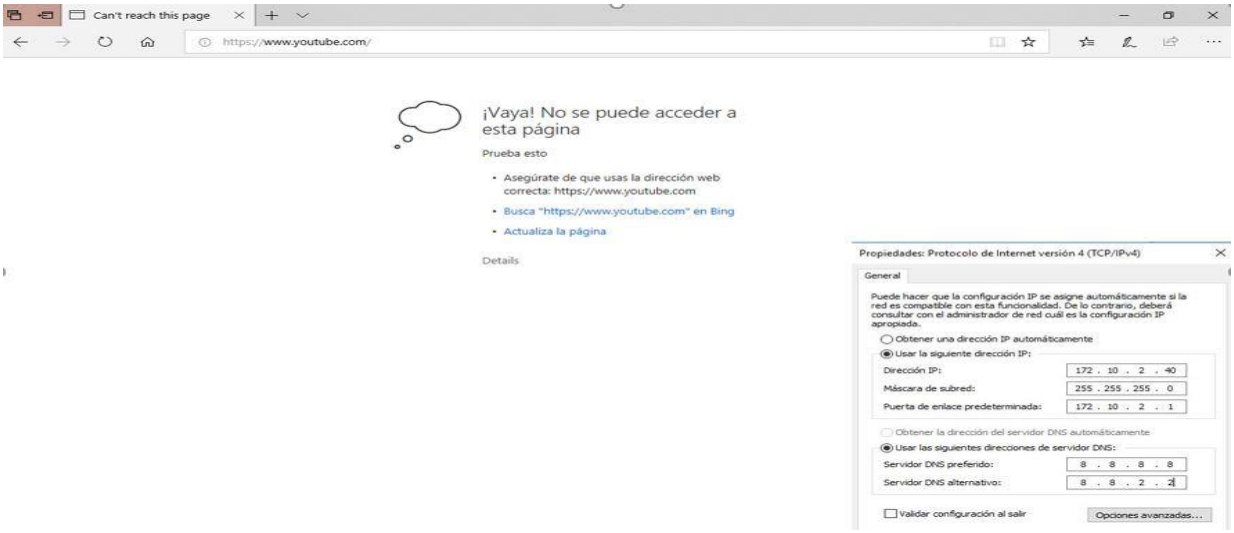


Ilustración 5.19 Restricción media

VLAN VISITAS: RESTRICCIÓN PORNOGRAFIA.

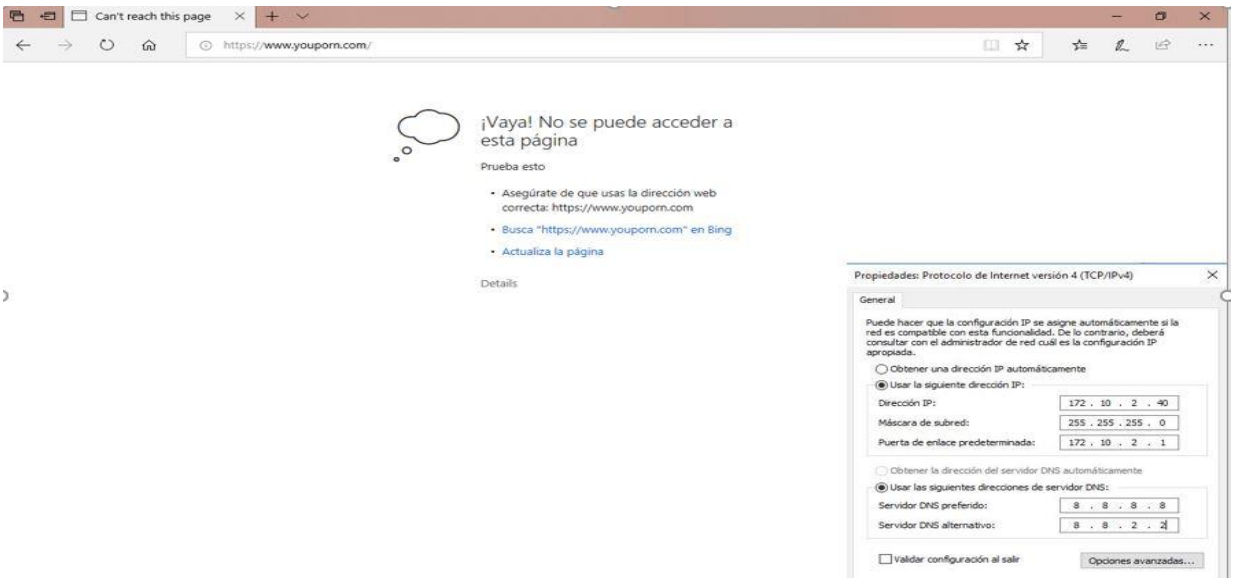


Ilustración 5.20 Restricción pornografía

VLAN VISITAS: RESTRICCIÓN DESCARGAS.

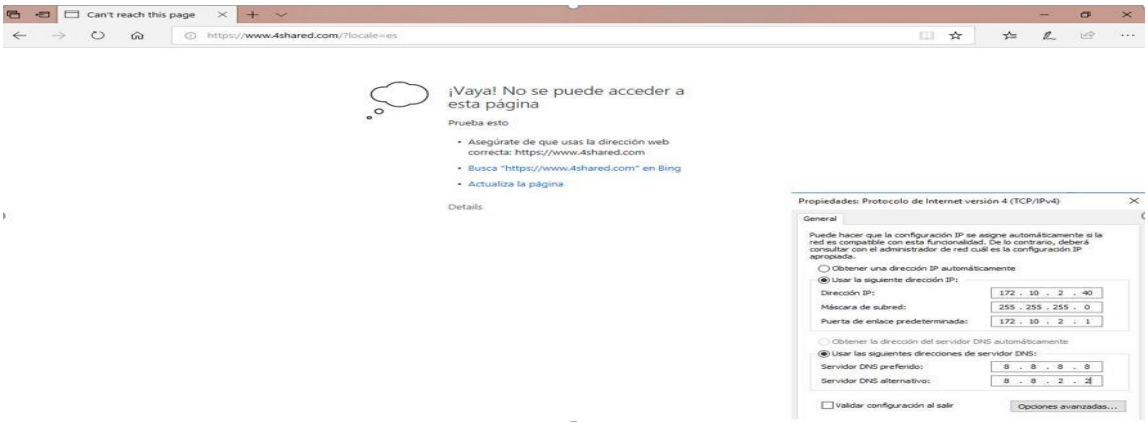


Ilustración 5.21 Restricción descargas

VLAN VISITAS: RESTRICCIÓN JUEGOS.

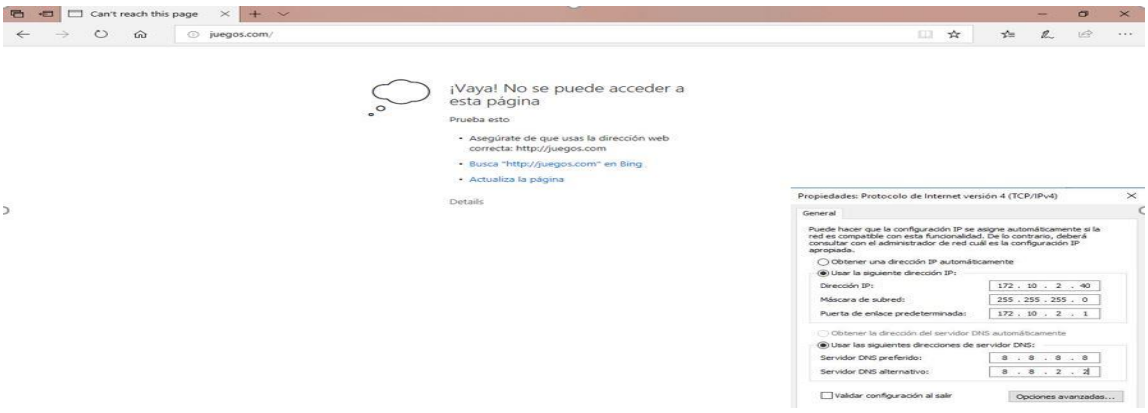


Ilustración 5.22 Restricción juegos

VLAN VISITAS: RESTRICCIÓN REDES SOCIALES.

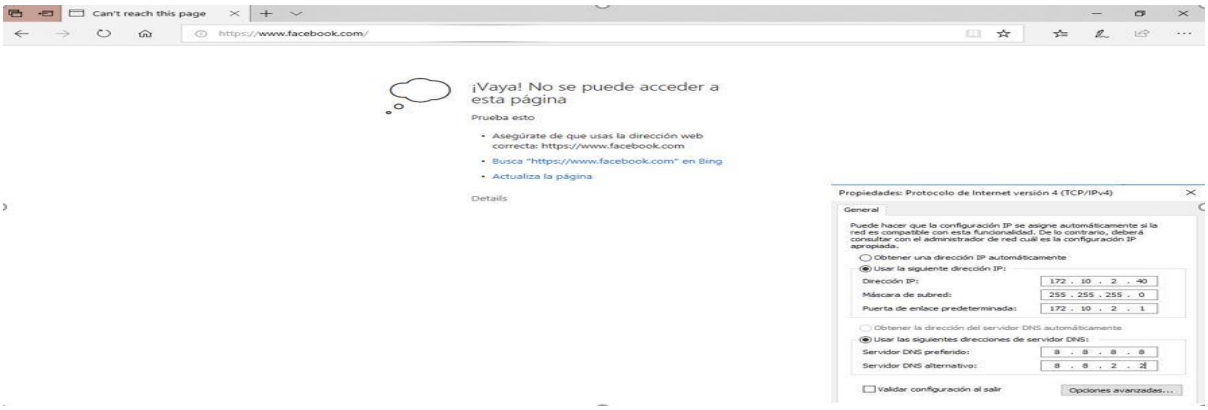


Ilustración 5.23 Restricción redes sociales

CONCLUSIONES.

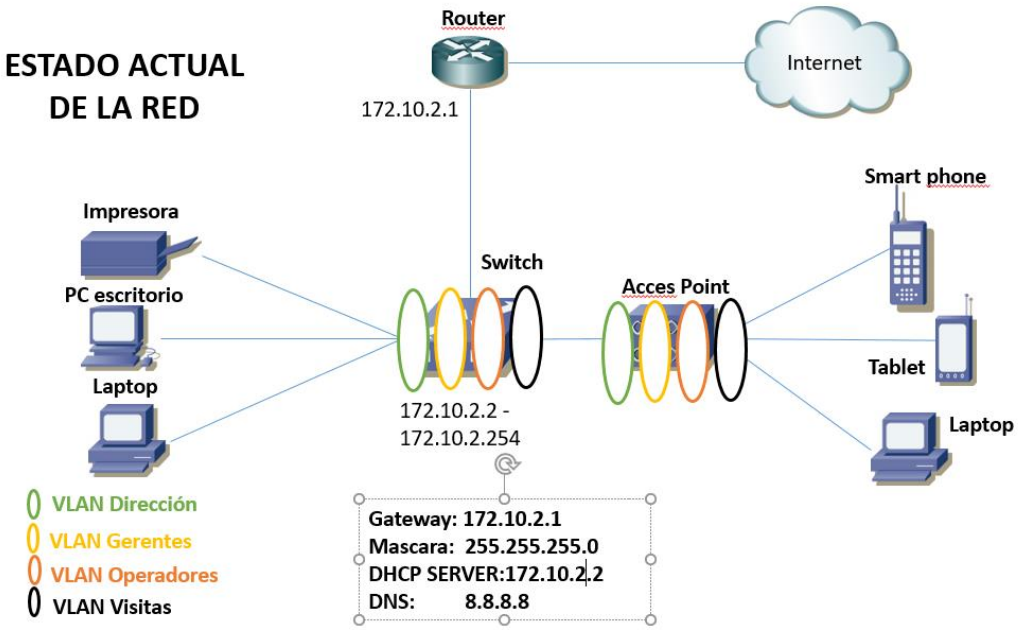
En conclusión, la eficiencia de un firewall dependerá de las políticas configuradas, la delimitación de los servicios y el correcto uso de ellos, no obstante, es un equipo poderoso en contra de los más comunes males de las redes.

Se alcanzó el objetivo al poder implementar el filtrado de contenido para mantener el uso correcto del ancho de banda y el mal uso del servicio de Internet.

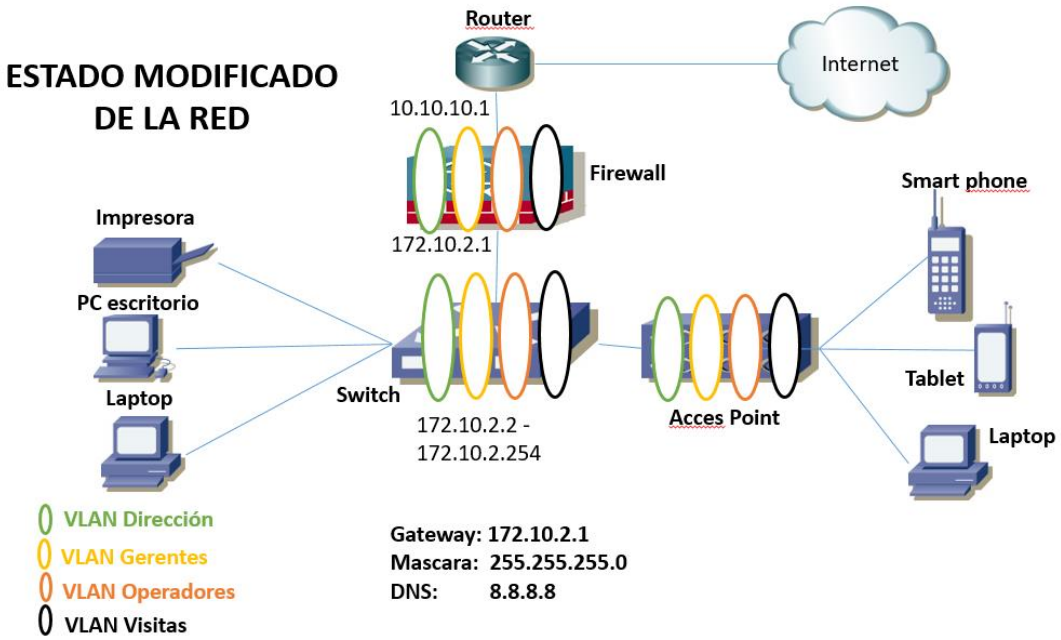
Con lo anterior los usuarios de la red tendrán una mayor eficiencia y podrán enfocarse a su trabajo sin perder el tiempo con distractores externos.

La productividad de la red es mejor debido a que no se destina ancho de banda para otros servicios que no sean únicamente de trabajo.

ANEXO 1 DIAGRAMA DE RED ACTUAL.

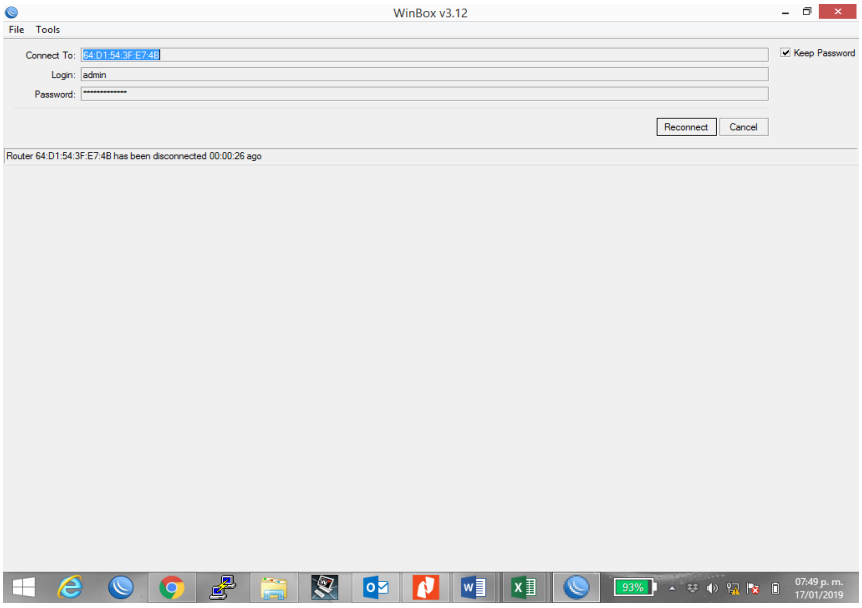


ANEXO 2 DIAGRAMA DE RED MODIFICADO.

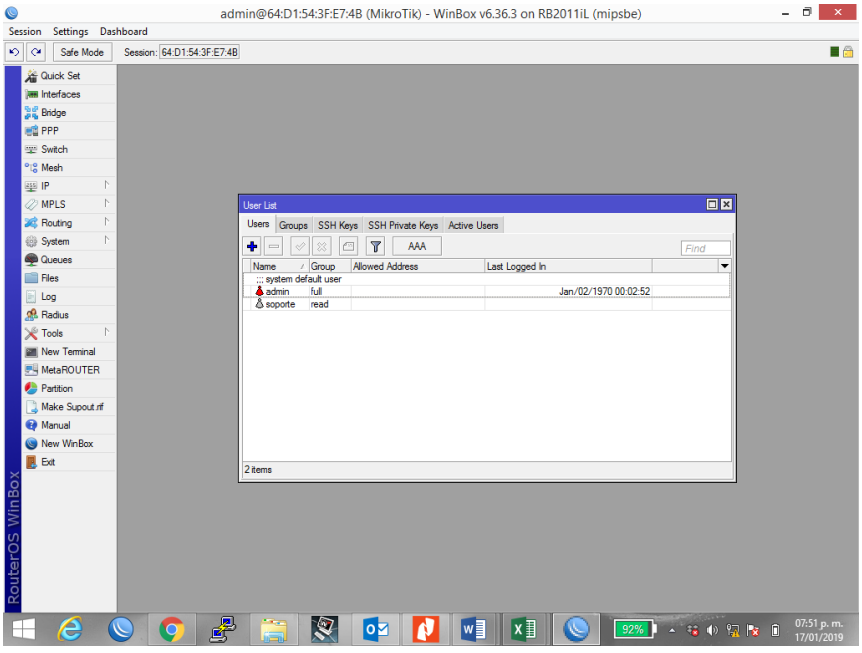


PROCEDIMIENTO DE CONFIGURACIONES.

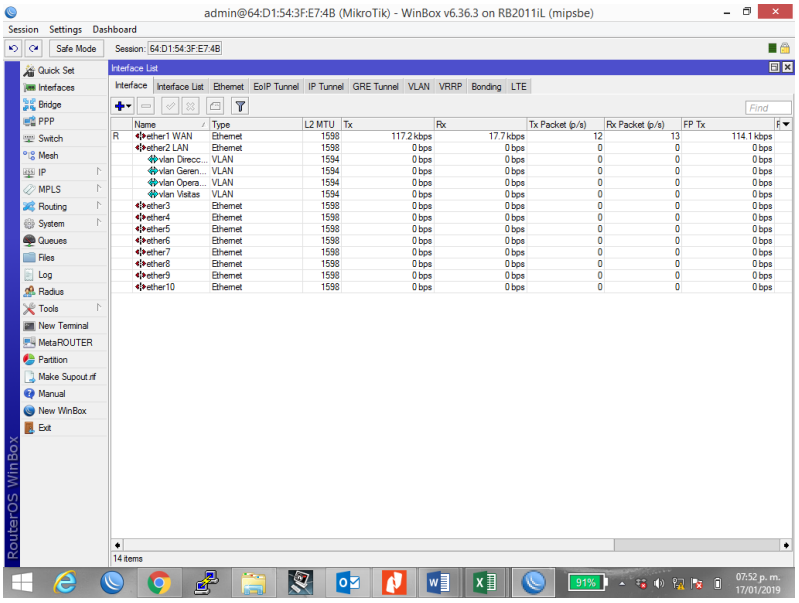
ANEXO I: ACCESO A FIREWALL.



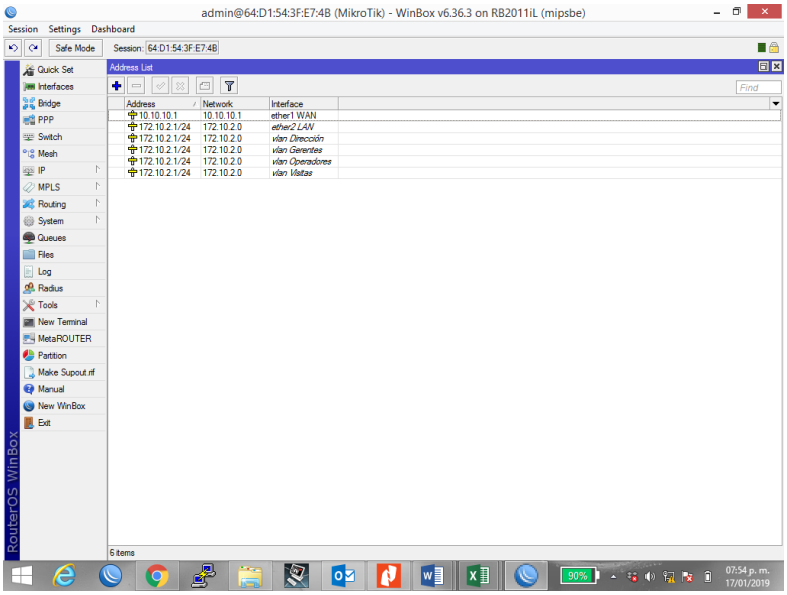
ANEXO II: ASIGACIÓN DE SERVICIOS A USUARIOS.



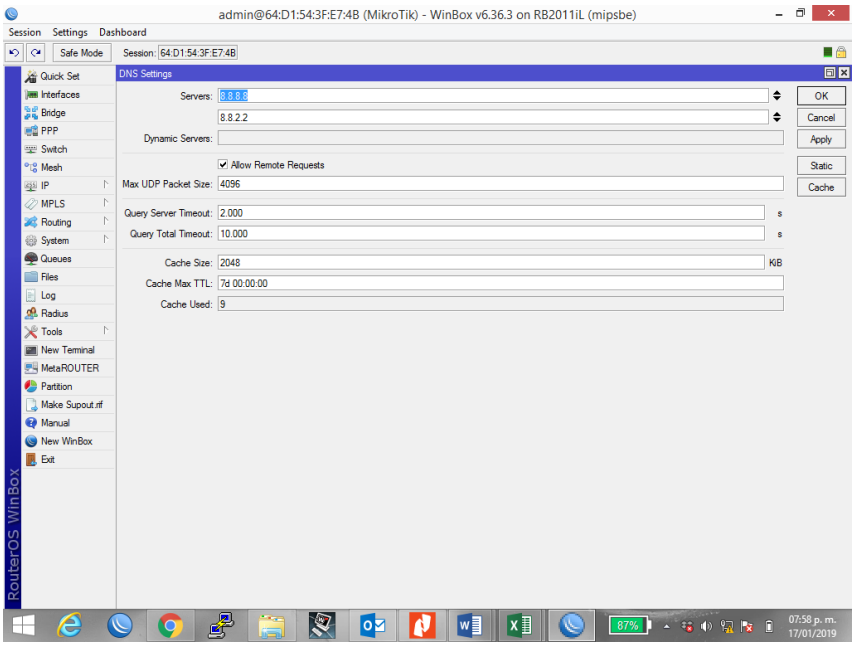
ANEXO III: ASIGACIÓN DE INTERFACES A LA RED WAN Y LAN.



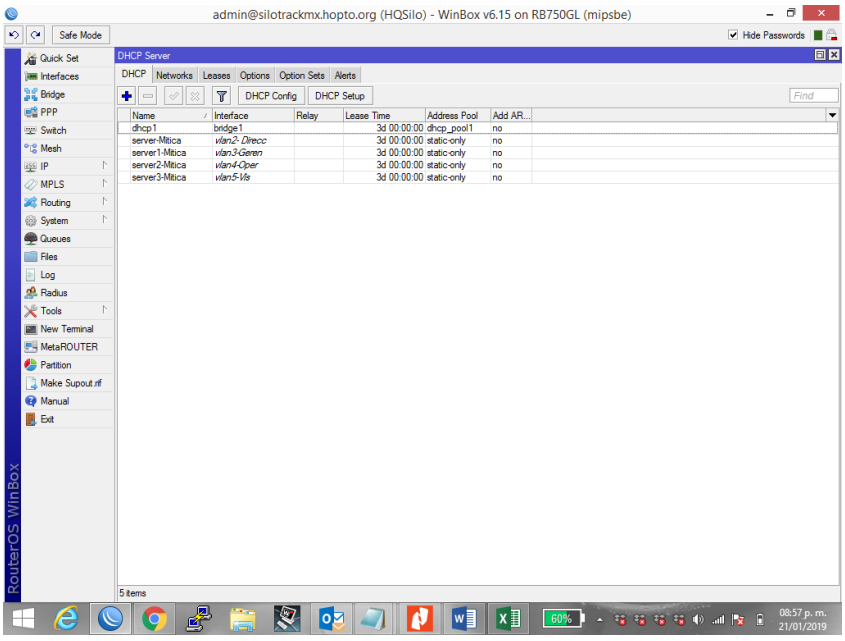
ANEXO IV: ASIGACIÓN DE DIRECCIONAMIENTO IP A LA RED.



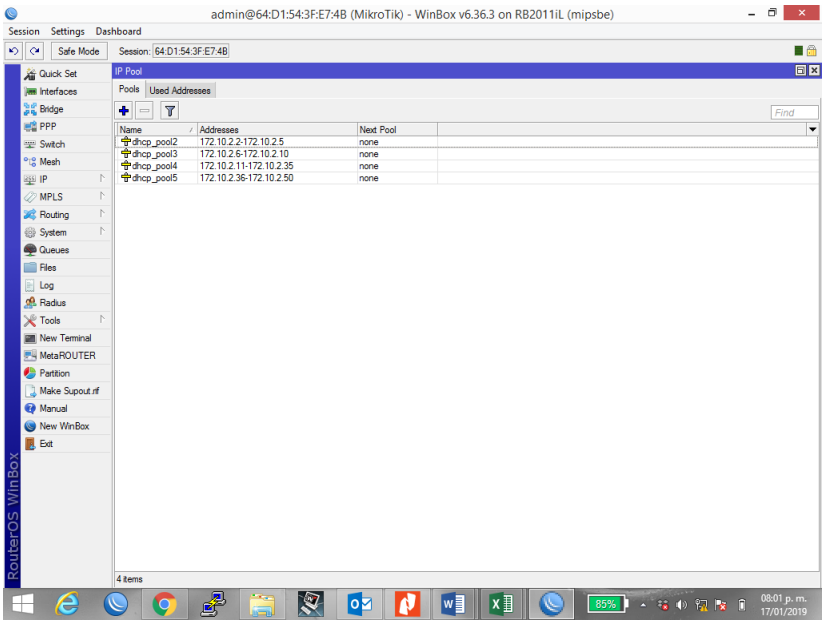
ANEXO V: ASIGNACIÓN DE DNS.



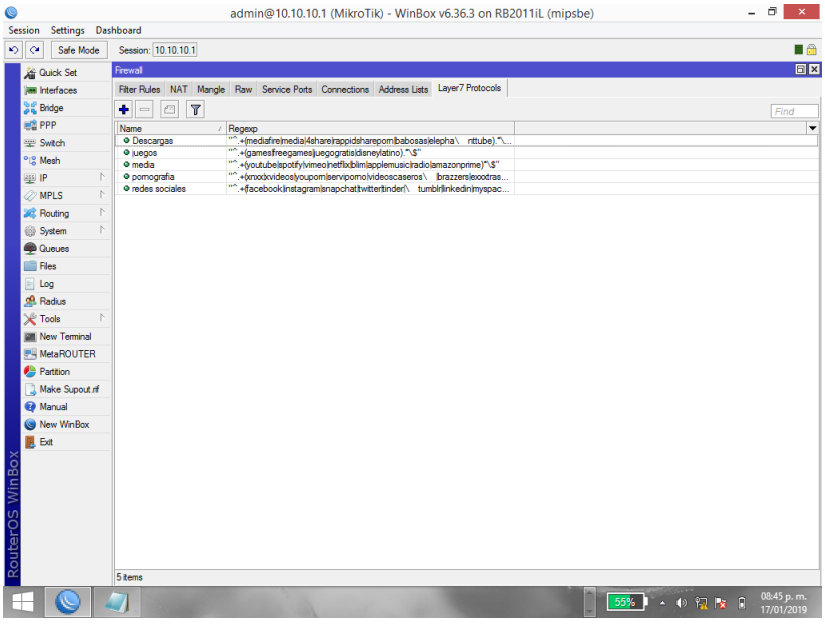
ANEXO VI: CREACIÓN DE DHCP SERVER PARA LAS VLAN.



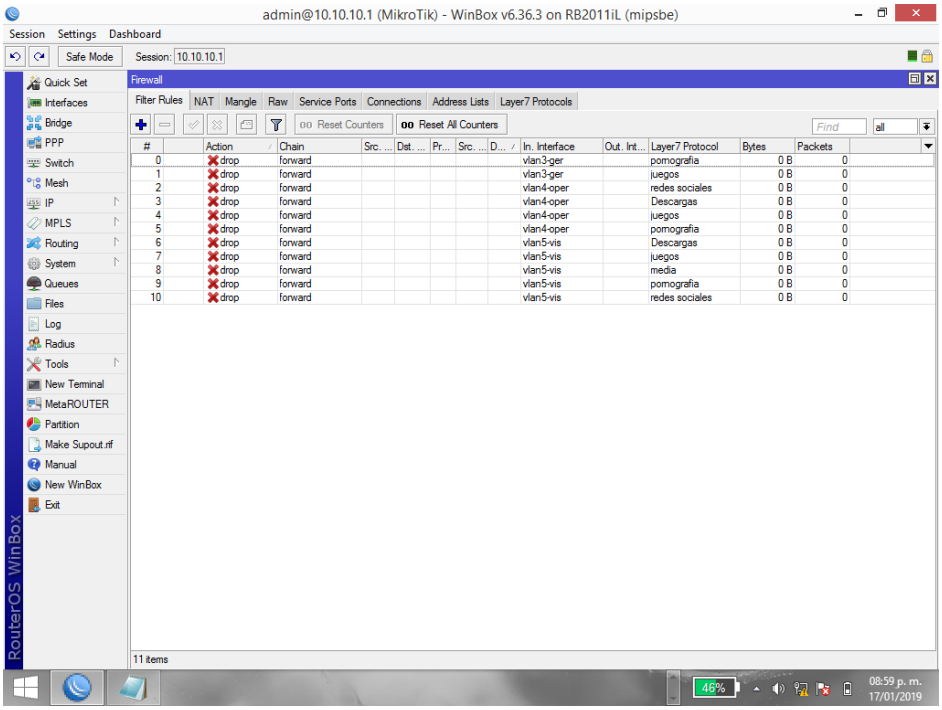
ANEXO VII: ASIGNACIÓN DE POOL DE DIRECCIONES A LAS VLAN.



ANEXO VIII: CONFIGURACION DE LAS CATEGORIAS DE FILTRADO DE CONTENIDO.



ANEXO IX: APLICACIÓN DE POLITICAS DE FILTRADO DE CONTENIDO A LOS GRUPOS DE TRABAJO.



ANEXO 3 DESCRIPCIÓN DE EQUIPOS UTILIZADOS.

CCR1072-1G-8S+

Our new flagship router, the CCR1072, is powered by a Tilera 72 core CPU, each core is clocked at 1GHz, and to fully utilise this power, the CCR1072 is equipped with eight independently connected 10G SFP+ ports.

Thanks to the unique 72 core processor and ports that are directly connected to the CPU, CCR1072 is capable of over 120 million packets per second throughput.

Full set of features

- 8x SFP+ ports
- 16GB ECC RAM
- Ports directly connected to CPU
- microSD and 2x M.2

Highest performance

- over 120 million pps packet throughput
- up to 80 Gbps throughput

New generation CPU

- 72 core CPU
- 1 GHz clock per core
- State of the art TILE GX architecture

The unit comes equipped with two removable (hot plug) power supplies for redundancy, smart card slot, eight SFP+ ports and 16GB of built in ECC RAM.

The CCR1072 also has two built-in M.2 slots, microSD and 2x USB for adding storage, to use for proxy cache, user manager and other features. The M.2 slots accept 800mm Key-M x4 PCIe 2.0 modules.

Specifications

Product code	CCR1072-1G-8S+
CPU nominal frequency	1 GHz
CPU core count	72
Size of RAM	16 GB
Storage	128 MB Onboard NAND, also see *expansion*
10/100/1000 Ethernet ports	1
Power supply	2x IEC C14 standard connectors 110/220V (Two redundant PSU)
Supported input voltage	12 V
CPU temperature monitor	Yes
PCB temperature monitor	Yes
Voltage Monitor	Yes
Current monitor	Yes
Dimensions	443x315x40mm, weight: 3.8 kg, weight with packaging: 5.125 kg
License level	6
Operating System	RouterOS
CPU	Tilera Tile-Gx72 CPU
Max Power consumption	100 W
Display	Color LCD, touchscreen
SFP	8x 10G Ethernet SFP+ cages (Mini-GBIC; SFP module not included), DDMI support
Expansion	1x microUSB 2.0, 1x regular USB 2.0, full size Smart Card slot, microSD slot, 2x M.2 slots with x4 PCIE 2.0, Key-M, module size support: 2242,2260,2280
Serial port	RJ45
Suggested price	$3,050

Included

2x IEC cords

Screw and feet kit

Rackmount ears

Performance test results

CCR1072-1G-8S+		Tile 72 Core (1200Mhz, DDR1333) Max possible throughput					
Mode	Configuration	1518 byte		512 byte		64 byte	
		Mbps	kpps	Mbps	kpps	Mbps	kpps
Bridging	none (fast path)	78,960.3	6,502.0	76,963.8	18,790.0	60,952.4	119,047.6
Bridging	25 bridge filter rules	74,448.8	6,130.5	33,557.3	8,192.7	5,293.8	10,339.5
Routing	none (fast path)	78,960.3	6,502.0	76,963.8	18,790.0	44,291.6	86,507.0
Routing	25 simple queues	78,960.3	6,502.0	50,669.2	12,370.4	6,898.8	13,474.2
Routing	25 ip filter rules	56,683.3	4,667.6	24,515.0	5,985.1	3,007.4	5,873.8

1. All tests are done with Xena Networks specialized test equipment (XenaBay),and done according to RFC2544 (Xena2544)
2. Max throughput is determined with 30+ second attempts with 0,1% packet loss tolerance in 64, 512, 1518 byte packet sizes
3. Values in italic indicate that max throughput was reached without maxing out CPU, but because board interface configuration was maxed out
4. Test results show device maximum performance, and are reached using mentioned hardware and software configuration, different configurations most likely will result in lower results

GLOSARIO

ACRÓNIMOS

ACK Un tipo de mensaje que se envía para indicar que un bloque de datos ha llegado a su destino sin errores.

ARP Protocolo de resolución de direcciones.

BRIDGE (Puente entre redes utilizando la misma topología)

CERT Equipo de Respuesta a Incidentes de Seguridad en Cómputo

CLI interface de línea de comandos

DASHBOARD interface gráfica del firewall accesado por la Web

DNS servidor de dominio

DHCP protocolo de configuración dinámica de host

DOMINIO nombre que sustituye una dirección ip

FIREWALL cortafuegos, dispositivo de seguridad

FTP protocolo de transferencia de archivos

HTTP protocolo de transferencia de hipertexto

HTML lenguaje de marcación de hipertexto

HUB dispositivo que solo interconecta varios equipos

IRC protocolo de comunicación en tiempo real

ICMP protocolo de control de mensajes de Internet

IP protocolo de Internet

LINK conectado o en conexión

MAC dirección física de la tarjeta de red

NETMASK mascara de subred

NAT traducción de la dirección de red

OSI sistema de Interconectividad abierta

P2P punto a punto

PING realiza una petición hacia una IP

POP3 servidor de correo

PROXY tipo de firewall que realiza filtrado de paquetes

PROTOCOLO conjunto de reglas que controlan la secuencia de un mensaje

ROUTER dispositivo que define la ruta a seguir en la red

SPAM envío de mensajes electrónicos no solicitados

SPOOFING suplantación de un atacante por una persona autorizada

SWITCH dispositivo de interconexión que opera en capa 2 de OSI

SNMP protocolo simple de gestión de redes

SMTP protocolo simple de transferencia de correo electrónico

TELNET protocolo para acceder a una maquina desde otra

TCP Conjunto básico de protocolos de comunicación de redes

TOPOLOGIA disposición física en la que se conectan los nodos de una red

UDP protocolo de uso de datagramas