



**SEP**

SECRETARÍA DE  
EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL  
DE MÉXICO



**Gobierno  
del Estado  
de Oaxaca**

2010 - 2016

OAXACA



SAI GLOBAL  
ISO 9001  
Quality

# INSTITUTO TECNOLÓGICO SUPERIOR DE TEPOSCOLULA

TESIS

IMPLEMENTACIÓN DE UN FIREWALL  
RESTRICTIVO DE BAJO COSTO PARA  
SOLUCIONES PYMES CON CONTROL DE  
ANCHO DE BANDA Y FILTRADO WEB; BASADO  
EN SOFTWARE LIBRE EN EL ITEC


PARA OBTENER EL TÍTULO DE

INGENIERO EN  
SISTEMAS COMPUTACIONALES

PRESENTA:  
LUIS SOREL MORALES CRUZ

ASESOR:  
ING. CINTHYA PÉREZ HERNÁNDEZ

SAN PEDRO Y SAN PABLO TEPOSCOLULA, OAXACA,  
NOVIEMBRE DE 2016

	<b>Nombre del Documento: Formato para la Autorización de Impresión</b>	<b>Código: ITSTE/D-AC-PO-004-06</b>
		<b>Revisión: 0</b>
	<b>Referencia a la Norma ISO 9001:2008 7.1, 7.2.1, 7.5.1, 7.6</b>	<b>Página 1 de 1</b>

San Pedro y San Pablo Teposcolula, Oax., 01/diciembre/2016  
 OFICIO No. DISC/0548/2016  
 ASUNTO: Autorización de impresión

**C. LUIS SOREL MORALES CRUZ  
 PASANTE DE LA LICENCIATURA  
 DE INGENIERÍA EN SISTEMAS  
 COMPUTACIONALES  
 PRESENTE**

En apego al Lineamiento de Titulación Integral Versión 1.0 para los planes de estudio 2009–2010 y en base a la liberación del proyecto de titulación integral denominado **“Implementación de un firewall restrictivo de bajo costo para soluciones pymes con control de ancho de banda y filtrado web; basado en software libre en el ITEC”**, para obtener el título de la Licenciatura en Ingeniería en Sistemas Computacionales.

**SE AUTORIZA LA IMPRESIÓN DE LA TESIS**


Sin más por el momento, me place felicitarlo y recomendarle continuar con los trámites correspondientes para la presentación del acto protocolario de Titulación integral.

**ATENTAMENTE**  
 INNOVACIÓN TECNOLÓGICA Y DESARROLLO REGIONAL SUSTENTABLE

  
**ING. CINTHYA PÉREZ HERNÁNDEZ**  
**JEFA DE LA DIVISIÓN DE INGENIERÍA**  
**EN SISTEMAS COMPUTACIONALES**

  
 NACIONAL  
 DE MÉXICO  
 DITD  
 INSTITUTO  
 TECNOLÓGICO  
 SUPERIOR DE  
 TEPOSCOLULA  
 20EIT9999A  
 DIVISIÓN DE  
 SISTEMAS  
 COMPUTACIONALES

Copia. Archivo.

	<b>Nombre del Documento: Formato de Liberación del Proyecto para la Titulación</b>	<b>Código: ITSTE/D-AC-PO-004-05</b>
	<b>Referencia a la Norma ISO 9001:2008 7.1, 7.2.1, 7.5.1, 7.6</b>	<b>Revisión: 0</b> <b>Página 1 de 1</b>

San Pedro y San Pablo Teposcolula, Oaxaca, 03/Noviembre/2016

ASUNTO: Liberación de proyecto para titulación.



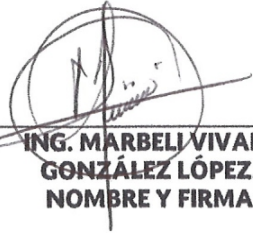
**ING. CINTHYA PÉREZ HERNÁNDEZ**  
**JEFA DE DIVISIÓN DE INGENIERÍA EN**  
**SISTEMAS COMPUTACIONALES**  
**PRESENTE.**

Por este medio le informo que ha sido liberado el siguiente proyecto para la Titulación:

a) Nombre del Egresado:	LUIS SOREL MORALES CRUZ
b) Plan de Estudios:	ISIC-2004-296
c) No. de Control	10ISC0117
d) Nombre del proyecto	IMPLEMENTACIÓN DE UN FIREWALL RESTRICTIVO DE BAJO COSTO PARA SOLUCIONES PYMES CON CONTROL DE ANCHO DE BANDA Y FILTRADO WEB ; BASADO EN SOFTWARE LIBRE EN EL ITEC.
d) Producto	TESIS

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados.

**ATENTAMENTE.**

 <b>ING. CINTHYA PÉREZ HERNÁNDEZ.</b> <b>NOMBRE Y FIRMA</b>	 <b>ING. ANTONIO GARCÍA CRUZ.</b> <b>NOMBRE Y FIRMA</b>	 <b>ING. MARBELI VIVANI GONZÁLEZ LÓPEZ.</b> <b>NOMBRE Y FIRMA</b>
<b>ASESOR</b>	<b>REVISOR</b>	<b>REVISOR</b>

## ÍNDICE

INTRODUCCIÓN .....	11
CAPITULO I. MARCO CONTEXTUAL .....	13
1.1 Planteamiento del problema .....	14
1.2 OBJETIVOS .....	15
1.2.1 Objetivo general.....	15
1.2.2 Objetivos específicos .....	15
1.3 JUSTIFICACIÓN .....	16
1.4 HIPÓTESIS .....	17
CAPITULO II. MARCO TEÓRICO.....	18
2.1 REDES DE COMPUTADORAS .....	19
2.1.1 Concepto de red .....	19
2.1.2 Redes de Área Local .....	20
2.1.3 Redes de Área Metropolitana .....	20
2.1.4 Redes de Área Amplia .....	21
2.1.5 Topologías de redes .....	22
2.1.6 Topología de bus .....	22
2.1.7 Topología de estrella .....	23
2.1.8 Topología de anillo .....	24
2.1.9 Topología de árbol.....	25
2.1.10 Topologías lógicas.....	25
2.2 MODELO OSI.....	26
2.2.1 Capa de aplicación .....	27
2.2.2 Capa de presentación.....	28
2.2.3 Capa de Sesión .....	28
2.2.4 Capa de Transporte.....	28
2.2.5 Capa de Red.....	28

2.2.6 Capa de enlace de datos .....	29
2.2.7 Capa Física.....	29
2.3 IEEE .....	30
2.4 REDES INALÁMBRICAS .....	30
2.4.1 Cómo funcionan las redes inalámbricas .....	30
2.4.2 Ventajas de utilizar redes inalámbricas.....	31
2.4.3 Desventajas de utilizar redes inalámbricas .....	31
2.4.4 Componentes de las redes inalámbricas .....	32
2.4.5 Vulnerabilidad en las redes Wi-Fi .....	34
2.5 SEGURIDAD EN REDES INALÁMBRICAS .....	35
2.5.1 WEP (Wired Equivalent Privacy) .....	35
2.5.2 WPA (Wireless Protected Access).....	35
2.6 IEEE 802.11X (WIRELESS LAN, WI-FI) .....	36
2.7 DISPOSITIVOS DE RED.....	37
2.7.1 Dispositivos activos.....	37
2.7.2 Dispositivos pasivos.....	38
2.8 PROTOCOLOS Y ARQUITECTURA DE REDES .....	41
2.8.1 Protocolo TCP .....	42
2.8.2 Protocolo IP .....	42
2.8.3 El protocolo TCP/IP .....	43
2.8.3.1 La capa física .....	43
2.8.3.2 La capa de acceso a la red .....	43
2.8.3.3 La capa internet.....	44
2.8.3.4 La capa de transporte .....	44
2.8.4 Versiones del protocolo TCP/IP .....	45
2.8.4.1 TCP/IP v4.....	45
2.8.4.2 TCP/IP v6.....	45

2.9 PROTOCOLOS DE ENRUTAMIENTO .....	45
2.9.1 Enrutamiento estático .....	45
2.9.2 Enrutamiento Predeterminado .....	46
2.9.3 Enrutamiento dinámico .....	46
2.9.3.1 Vector Distancia .....	47
2.9.3.2 Estado de enlace .....	47
2.9.3.3 Métrica .....	47
2.9.3.4 Convergencia .....	48
2.9.3.5 Distancia administrativa y métrica .....	48
2.10 SEGURIDAD DE REDES.....	49
2.10.1 Seguridad .....	49
2.10.2 Seguridad en redes.....	50
2.11 FIREWALL .....	52
2.11.1 Firewall basado en red.....	52
2.11.2 Firewall basado en aplicación .....	52
2.11.3 Características adicionales de los Firewall's.....	53
2.11.4 Ventajas de un firewall.....	55
2.11.5 Desventajas de un firewall .....	55
2.12 AMENAZA .....	56
2.13 ATAQUE.....	56
2.14 VULNERABILIDAD .....	56
2.14.1 Definición de vulnerabilidad .....	57
2.14.2 Tipos de Vulnerabilidades.....	57
2.14.2.1 Vulnerabilidades físicas.....	57
2.14.2.2 Vulnerabilidades naturales .....	58
2.14.2.3 Vulnerabilidades de hardware .....	58
2.14.2.4 Vulnerabilidades de Software.....	58
2.14.2.5 Vulnerabilidades de red.....	58
2.14.2.6 Factor humano .....	59

2.14.3 Ataques a la seguridad .....	60
2.14.3.1 Ataques pasivos .....	60
2.14.3.2 Ataques activos: .....	62
2.14.3.3 Ataques DoS .....	63
2.14.3.4 Métodos de ataque DoS.....	64
2.14.3.5 Ataques DDoS.....	64
2.14.4 Servidores espejo .....	64
2.14.5 Honeypots.....	65
2.14.6 Servidor Proxy .....	66
2.14.7 Software libre .....	66
2.14.8 Software Privativo .....	67
2.14.9 Software privado .....	68
2.14.10 Filtrado web .....	68
2.14.11 Software de filtrado .....	68
CAPITULO III. METODOLOGÍA.....	70
3.2 Requerimientos.....	72
3.3 Análisis .....	73
3.3.1 Ubicación geográfica.....	74
3.3.1.1 Macro localización .....	74
3.3.1.2 Micro localización .....	74
3.4 Desarrollo .....	76
3.5 Implementación .....	83
3.5.1 Restructuración del cableado.....	83
3.5.2 instalación y configuración .....	83
CAPITULO IV. RESULTADOS.....	128
4.1 Cableado estructurado.....	129
4.2 Firewall. ....	130
4.3 Análisis de resultados.....	131
CONCLUSIONES.....	133

ANEXOS .....	134
ANEXO 1. ENCUESTAS .....	135
ANEXO 2. GRÁFICAS .....	160
ANEXO 3. EVIDENCIAS.....	168
REFERENCIAS BIBLIOGRÁFICAS.....	175
REFERENCIAS VIRTUALES.....	176



## ÍNDICE DE TABLAS.

TABLA 1. Censo económico y clasificación de las MPYME'S .....	13
TABLA 2. Comparación de las diferentes tecnologías normalizadas por la IEEE .....	37
TABLA 3. Tabla de distancias administrativas por protocolo de enrutamiento .....	49
TABLA 4. Comparación de los tipos de ataques a la seguridad de una red .....	60
TABLA 5. Características de los dispositivos que se encuentran en el ITEC. 1 de 3.....	78
TABLA 6. Características de los dispositivos que se encuentran en el ITEC. 2 de 3.....	79
TABLA 7. Características de los dispositivos que se encuentran en el ITEC. 3 de 3.....	80
TABLA 8. Comparativa de equipos firewall .....	82

## ÍNDICE DE FIGURAS.

FIGURA 1. Clasificación de las redes de acuerdo a su amplitud .....	19
FIGURA 2. Ejemplificación de una red MAN .....	20
FIGURA 3. Ejemplificación de una red WAN.....	21
FIGURA 4. Topología de BUS.....	23
FIGURA 5. Topología de estrella .....	23
FIGURA 6. Topología de anillo.....	24
FIGURA 7. Topología de árbol .....	25
FIGURA 8. Capas del modelo OSI.....	27
FIGURA 9. AP inalámbrico de doble banda N300 linksys WAP300N .....	32
FIGURA 10. Router inalámbrico Wireless-G Linksys WRT54GL .....	33
FIGURA 11. Tipos de antenas para la distribución de señal inalámbrica.....	33
FIGURA 12. Placas de red inalámbricas .....	34
FIGURA 13. Capas del protocolo TCP/IP .....	43
FIGURA 14. Comparación entre las arquitecturas OSI Y TCP/IP .....	44
FIGURA 15. Obtención de contenido de mensaje.....	61
FIGURA 16. Análisis de tráfico.....	62
FIGURA 17. Mapa de la república mexicana con división política .....	74
FIGURA 18. Mapa del estado de oaxaca por regiones .....	75
FIGURA 19. Ciudad de Oaxaca de Juárez .....	75
FIGURA 20. Región de Valles Centrales .....	75
FIGURA 21. Plano de la planta baja de las instalaciones del ITEC .....	76
FIGURA 22. Plano correspondiente a la planta alta del ITEC .....	81
FIGURA 23. Tarjeta de red Ethernet .....	84
FIGURA 24. Procesador .....	84
FIGURA 25. Disco duro Samsung.....	84
FIGURA 26. Tarjeta de memoria RAM Kingston .....	84
FIGURA 27. Switch alámbrico 3COM .....	84
FIGURA 28. Router Linksys inalámbrico/alámbrico .....	84
FIGURA 29. Página del sistema IPCOP .....	85
FIGURA 30. Tarjetas de red instaladas.....	85

FIGURA 31. Sector descargas del sitio web de IPCOP .....	85
FIGURA 32. Pantalla de guardado de la descarga .....	85
FIGURA 33. Pantalla de la aplicación para grabación .....	86
FIGURA 34. Pantalla inicial de encendido .....	86
FIGURA 35. Selección de arranque .....	87
FIGURA 36. Selección de idioma de instalación .....	87
FIGURA 37. Pantalla de bienvenida a la instalación .....	87
FIGURA 38. Selección de idioma del teclado.....	88
FIGURA 39. Selección de la zona horaria.....	88
FIGURA 40. Configuración de la fecha y hora .....	89
FIGURA 41. Pantalla de búsqueda de los ficheros .....	89
FIGURA 42. Selección del disco duro para la instalación .....	90
FIGURA 43. Configuración o cancelación de la instalación .....	90
FIGURA 44. Confirmación de la unidad seleccionada .....	91
FIGURA 45. Creación del sistema de archivos .....	91
FIGURA 46. Avance del copiado de archivos .....	91
FIGURA 47. Conclusión del copiado de archivos.....	92
FIGURA 48. Pantalla de selección de Back UP .....	92
FIGURA 49. Pantalla final de la instalación.....	93
FIGURA 50. Asignación del nombre del HOST.....	93
FIGURA 51. Asignación del nombre del dominio .....	94
FIGURA 52. Selección de la función de la interfaz RED .....	95
FIGURA 53. Selección de tarjetas para las interfaces.....	95
FIGURA 54. Selección de tarjeta para la interfaz GREEN .....	96
FIGURA 55. Asignación de la interfaz RED .....	96
FIGURA 56. Confirmación de la selección de interfaces.....	96
FIGURA 57. Configuración de la dirección IP .....	97
FIGURA 58. Asignación del nombre del HOST.....	97
FIGURA 59. Pantalla de configuración de los DNS.....	98
FIGURA 60. Activación del DHCP y asignación de la IP.....	99
FIGURA 61. Asignación de la contraseña del usuario "ROOT".....	99

FIGURA 62. Asignación de la contraseña del usuario “ADMIN” .....	100
FIGURA 63. Asignación de contraseña para respaldos .....	100
FIGURA 64. Pantalla final de la instalación.....	101
FIGURA 65. Reinicio del sistema .....	101
FIGURA 66. Pantalla de inicio del Firewall.....	101
FIGURA 67. Inicio de procesos del Firewall.....	102
FIGURA 68. Sistema Firewall iniciado .....	102
FIGURA 69. Solicitud de inicio de sesión .....	102
FIGURA 70. Inicio de sesión con el usuario “ROOT” .....	103
FIGURA 71. Programa WINS CP.....	104
FIGURA 72. Programa PUTTY .....	104
FIGURA 73. Autorización para el programa WINS CP .....	105
FIGURA 74. Instalador del programa WINS CP.....	105
FIGURA 75. Bienvenida al asistente de instalación .....	106
FIGURA 76. Pantalla de aceptación de licencias .....	106
FIGURA 77. Selección del tipo de instalación .....	107
FIGURA 78. Selección de la interfaz para la aplicación .....	107
FIGURA 79. Informe de las configuraciones .....	108
FIGURA 80. Barra de estado de la instalación.....	108
FIGURA 81. Final de la instalación del WINS CP .....	108
FIGURA 82. Pantalla inicial del programa WINS CP .....	109
FIGURA 83. Inicio de sesión con usuario ADMIN .....	109
FIGURA 84. Pantalla principal del Firewall.....	110
FIGURA 85. Acceso ssh en el menú sistema.....	110
FIGURA 86. Pantalla principal del menú acceso SSH .....	111
FIGURA 87. Activación del servicio SSH .....	111
FIGURA 88. WINS CP con parámetros para conexión .....	112
FIGURA 89. Inicio de la conexión con el WINS CP.....	112
FIGURA 90. Pantalla principal del programa WINS CP .....	112
FIGURA 91. Copiado de los ficheros al Firewall .....	113
FIGURA 92. Directorio de los archivos en el Firewall.....	114

FIGURA 93. Extracción de archivos firewall con WINS SCP.....	114
FIGURA 94. Ficheros descomprimidos en Firewall.....	115
FIGURA 95. Pantalla principal del programa PUTTY.....	115
FIGURA 96. Pantalla de la consola de comandos .....	116
FIGURA 97. Utilización del comando # ls en PUTTY.....	116
FIGURA 98. Utilización del comando # cd en PUTTY.....	117
FIGURA 99. Instalación del COPFILTER desde PUTTY .....	117
FIGURA 100. Proceso de instalación del COPFILTER.....	118
FIGURA 101. Mensaje de confirmación para la instalación .....	118
FIGURA 102. Final de la instalación del COPFILTER.....	119
FIGURA 103. Ubicación del COPFILTER en el Firewall .....	119
FIGURA 104. Acceso al submenú Servicios/ Proxy .....	120
FIGURA 105. Pantalla principal del submenú PROXY.....	120
FIGURA 106. Acceso al menú Filtro URL .....	121
FIGURA 107. Pantalla principal del menú Filtro URL.....	121
FIGURA 108. Activación de los servicios del Filtro URL .....	121
FIGURA 109. Botón guardar y reiniciar del Filtro URL .....	122
FIGURA 110. Inicio satisfactorio del Filtro URL.....	122
FIGURA 111. Pantalla de la página: URLBLACKLIST.COM.....	123
FIGURA 112. Sección de instalación de listas negras .....	123
FIGURA 113. Selección del archivo de la Black LIST .....	124
FIGURA 114. Correcta instalación de la Black LIST .....	124
FIGURA 115. Contenido wep separado por categorías .....	125
FIGURA 116. Página bloqueada por el firewall.....	126
FIGURA 117. Apartado de control de tráfico del firewall .....	126
FIGURA 118. Configuración de rangos de subida y bajada.....	127
FIGURA 120. Canaletas en la dirección.....	129
FIGURA 119. Canaletas fuera de la dirección.....	129
FIGURA 121. Cable de red .....	129
FIGURA 122. Canaletas en el centro de cómputo .....	130
FIGURA 123. Canaleta en el centro de cómputo .....	130

FIGURA 124. Firewall ipcop en la dirección del ITEC.....	130
FIGURA 125. Cable de red en la dirección .....	168
FIGURA 126. Instalación telefónica y eléctrica .....	168
FIGURA 127. Cable de red en los pasillos.....	168
FIGURA 128. Cable de red en los pasillos.....	168
FIGURA 129. Cable de red en el centro de cómputo.....	168
FIGURA 130. Canaletas en la dirección .....	169
FIGURA 131. CCanaletas del centro de cómputo.....	169
FIGURA 132. Canaletas en los pasillos .....	169
FIGURA 133. Canaletas en los pasillos .....	169

## INTRODUCCIÓN

En la actualidad las redes de computadoras son de gran importancia en diversos sectores, uno de estos es el empresarial, por lo cual es necesario que las empresas cuenten con redes informáticas para el mejor manejo y administración de sus recursos, por ello es necesario que su infraestructura cuente con sistemas o herramientas que proporcionen seguridad tanto a los equipos como a su información, optimizando costos.

Hay diversos tipos de métodos que sirven para dar seguridad a las redes de computadoras, uno de los elementos que se puede instalar es un **Firewall** (corta fuegos), pero la adquisición de equipos avanzados y modernos en el mercado actualmente pueden alcanzar altos precios, por ello la instalación y configuración de un **Firewall** basado en **Software libre** con equipos de bajos costos, da como resultado una reducción considerable de la inversión.

La función principal de un **Firewall** es la de formar una barrera entre una red y una conexión a internet de manera que esté protegida la red de posibles ataques ya que funciona como filtro de peticiones entre el internet y la red, de esta manera se pueden evitar sitios maliciosos, con poca seguridad o que puedan resultar en algún problema de seguridad.

Al realizar la instalación de un equipo que desempeñe las actividades de filtrado de contenidos y administración del ancho de banda en una conexión, se optimiza el rendimiento de la navegación ya que al controlar estos dos aspectos se puede brindar un mejor servicio.

En la presente tesis se da a conocer el análisis y el desarrollo de la implementación de un sistema de firewall restrictivo de bajo costo en el ITEC Oaxaca, este documento se divide en cuatro capítulos siendo los siguientes:

Capítulo I. Marco contextual: En este capítulo se lleva a cabo el planteamiento del problema, el cual se enfoca en la seguridad y el mejor rendimiento de la red de computadoras del ITEC, también se aborda el objetivo general, los objetivos específicos, la justificación para la implementación del firewall, así como el establecimiento de la hipótesis a demostrar.

Capítulo II. Marco teórico: En este capítulo se abordan los temas relacionados con dispositivos, modelo OSI, protocolos, arquitectura, vulnerabilidades, tipos de ataques y seguridad en redes, mediante este capítulo se toma como medio de información para sustentar los conocimientos que son de importancia para el desarrollo de este documento.

Capítulo III. Metodología: Mediante este capítulo se presenta la información y clasificación de las MPyME's, los requerimientos obtenidos para la sustentación, también se detalla el análisis, desarrollo y el transcurso de la implementación del sistema de firewall en el ITEC.

Capítulo IV. Resultados: En este capítulo se muestran los resultados obtenidos y su análisis tras la instalación del sistema de firewall con el cual se desarrolla este documento y poder determinar si se cumple con la hipótesis que se planteó en el capítulo I.

Anexos: En el apartado de anexos se muestra una serie de resultados mediante material fotográfico como evidencia con el cual sustentar el trabajo realizado para la elaboración de este documento.



## CAPITULO I. MARCO CONTEXTUAL

Dentro de la clasificación de las empresas se encuentran las micro, pequeña, mediana y gran empresa, siendo agrupadas de acuerdo al número de sus trabajadores y su cantidad de ingresos registrados, las micro, pequeñas y medianas empresas o mejor conocidas por el acrónimo **MPyME's** tienen una gran importancia en la economía y el empleo a nivel regional y nacional.

En México la actual Secretaría de Comercio estableció los criterios para la clasificación de la industria de acuerdo a su tamaño.

Tabla 1 Censo Económico y Clasificación de las MPyME's.

Tamaño	Sector		
	Clasificación según empleados		
	Industria	Comercio	Servicios
Micro	De 0 a 10	De 0 a 10	De 0 a 10
Pequeña	De 11 a 50	De 11 a 30	De 11 a 50
Mediana	De 51 a 250	De 31 a 100	De 51 a 100

Fuente: Censo Económico INEGI 2014.

Las pequeñas y medianas empresas o **MPyME's** han crecido de gran manera en el país; enfocándonos en el Estado de Oaxaca estas han aumentado considerablemente en los últimos años, por ello los pequeños y medianos empresarios se han preocupado por mejorar sus actividades lo cual los ha encaminado a mejorar y proporcionar servicios tales como prestar conexión de internet a sus empleados y clientes dentro de sus instalaciones, al mismo tiempo que mejoran su infraestructura, tienen que implementar medidas de seguridad para no comprometer la integridad de sus datos y su red.

## 1.1 Planteamiento del problema

La seguridad y el óptimo rendimiento en una red son dos de los elementos más importantes para que esta tenga un funcionamiento adecuado, por ello las **MPyME's** que cuentan con una, deben disponer de medidas para cumplir con estas dos necesidades; dado que este tipo de empresas son de capital moderado, tienen que considerar la reducción de costos y encontrar herramientas eficientes, confiables, que representen una inversión mínima.

El **ITEC** es una institución que tiene una red local la cual no tiene los elementos adecuados que brinden seguridad y mejoren su rendimiento, otra deficiencia es el cableado estructurado que no cuenta con las especificaciones basadas en las normas y estándares, por esta razón la calidad de la conexión se ve disminuida también al encontrarse el cableado en malas condiciones pueden existir fallas considerables de comunicación en los equipos, las circunstancias en las que se encuentra la instalación de red son: cables con recubrimientos externos rotos o desgarrados, recubrimientos de los cables de cobre en condiciones similares, conectores RJ45 con problemas de sujeción debido a que las pestañas de seguridad se encuentran rotas lo cual causa que al mínimo movimiento de este se pierda el contacto con los puertos de Ethernet de los distintos equipos.

## 1.2 Objetivos

### 1.2.1 Objetivo general

Mejorar el servicio de internet que se proporciona dentro de las instalaciones del **ITEC** suministrando una herramienta potente, segura y estable de bajo costo para la administración de los contenidos en la red.

### 1.2.2 Objetivos específicos

- Proporcionar una potente herramienta de seguridad y administración a empresas **MPYME's** a un costo bajo.
- Realizar un documento que forme parte de la bibliografía del **ITSTE** y sirva como herramienta didáctica en la carrera de Ingeniería en Sistemas Computacionales, el cual les permita conocer, manejar sistemas de seguridad y administración para redes basados en Software libre, con lo cual complementen sus conocimientos y genere la inquietud en ellos para aprovechar los recursos con los que se cuentan en la actualidad.

### 1.3 Justificación

Actualmente la comunicación y los medios por los cuales se lleva a cabo son muy importantes para las empresas; por ello es primordial ofrecer un servicio de conexión a internet para sus trabajadores y usuarios procurando que sea eficiente.

En las instituciones educativas es importante proporcionar una herramienta de apoyo a los integrantes del cuerpo educativo para realizar sus actividades docentes, facilitar a los alumnos los servicios adecuados sin comprometer la velocidad de la conexión, de igual forma delimitar el acceso a sitios no permitidos para reducir el riesgo en la seguridad de los datos y los equipos.

En el **ITEC** tienen la necesidad de mejorar los servicios de seguridad y comunicación en su red, optimizar la comunicación entre los equipos del centro de cómputo y los distintos dispositivos que se ubiquen dentro de las instalaciones, de la misma manera proveer una conexión segura.

La instalación y configuración de un Firewall dentro del ITEC representa el mejoramiento de los servicios de red y seguridad en la navegación.

Considerando que en las instalaciones tienen una red cableada que se encuentra desorganizada; es decir, la falta de una estructura de cableado, que permita una conexión eficiente y segura; por lo cual se pretende realizar una propuesta de mejora.

## **1.4 Hipótesis**

La implementación de un Firewall basado en Software libre en la red local del ITEC tendría como consecuencia un mejor aprovechamiento del servicio de internet dentro de sus instalaciones ya que además de representar un bajo costo, permitirá que los equipos tengan un mejor desempeño dentro de la red local y se cuente con mayor seguridad.

## CAPITULO II. MARCO TEÓRICO

En este capítulo se establecen los conceptos e ideas que se desarrollan durante este trabajo, los temas abordados pertenecen al área de redes de computadoras y telecomunicaciones.

Se iniciará presentando el concepto de redes de computadoras, los tipos que existen y las topologías empleadas. A continuación, se define el modelo (OSI) que es el modelo de interconexión para sistemas abiertos con el cual se definen los métodos y protocolos necesarios para conectar un dispositivo con cualquier otro para formar una red; subsecuentemente se aborda una pequeña reseña de lo que es la (IEEE) ya que es importante conocer acerca del instituto que regula los estándares en las tecnologías de la información. Después se desarrollará el tema de redes inalámbricas para conocer sobre su funcionamiento ya que actualmente son empleadas por las ventajas que ofrecen puesto que para estar conectados a una red de este tipo no es necesario un cable o encontrarse en un solo lugar de manera fija, se conocerán sus ventajas, desventajas y vulnerabilidades; se darán a conocer algunos de los dispositivos de red más importantes así como su clasificación, si son activos, estos se encargarán de distribuir en forma activa la información a través de la red, estos dispositivos pueden ser routers, switches, hub's, etc., si pertenecen a la clasificación de pasivos quiere decir que no intervienen en los métodos de transmisión sino que son solamente para interconectar los dispositivos en la red, estos pueden ser los cables, rosetas, canaletas jack's etc. También se conocerá el protocolo de transmisión (TCP) cuya función principal es el uso bidireccional en origen destino de comunicación para transmitir datos; posteriormente se definirá el protocolo de internet (IP), que consta principalmente en el direccionamiento y enrutamiento de paquetes de información dentro de una red, asimismo se detallarán los protocolos de enrutamiento más relevantes. Consecutivamente se definirá lo que es la seguridad en redes para poder abordar el tema de firewall, que es una herramienta o una parte de un sistema que está diseñada para formar una división entre dos redes el cual se encarga de filtrar las peticiones que hay entre ellas y de esta manera proporcionar mayor seguridad en el intercambio de información, se darán a conocer los tipos de firewall más comunes, así como sus ventajas y desventajas.

## 2.1 Redes de computadoras

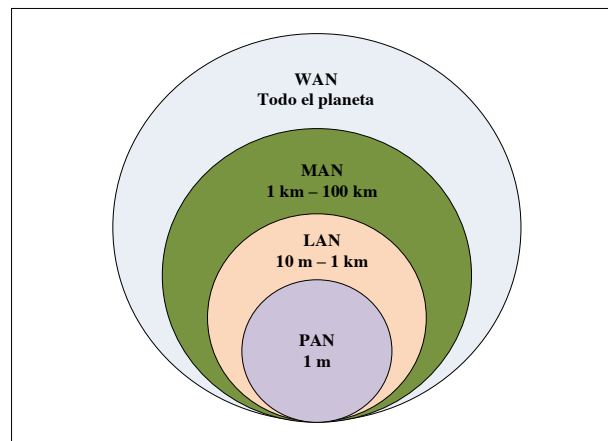
### 2.1.1 Concepto de red

Una red de computadoras es un conjunto de dispositivos electrónicos interconectados que cuentan con la capacidad de compartir información y recursos entre ellos, los cuales se denominan nodos, estos pueden estar conectados a la red de forma cableada o inalámbrica mediante distintos dispositivos.

Con lo anterior se entiende que una red es una forma por el cual se transportan datos con los distintos elementos que se encuentran interconectados a la misma, tales como computadoras, impresoras y otros dispositivos.

Las redes de computadoras como se ha planteado anteriormente son equipos interconectados con la capacidad de compartir recursos entre ellos, las redes de computadoras se clasifican en base a su alcance como: Red de Área Personal (**PAN**), Redes de Área Local (**LAN**), Red de Área Metropolitana (**MAN**) y Redes de Área Ampla (**WAN**), en la figura 1 se puede apreciar dicha clasificación.

Figura 1. Clasificación de las redes de acuerdo a su amplitud.



Fuente: (Stallings, Comunicaciones y Redes de Computadores, 2010)

## 2.1.2 Redes de Área Local

Las redes de área local o mayormente conocidas como LAN's son redes privadas que por lo general se encuentran en un solo edificio o complejo que abarque pocos kilómetros de longitud, normalmente son implementadas para interconectar equipos de cómputo personales y estaciones de trabajo dentro de empresas, escuelas u hogares para compartir recursos tales como impresoras y compartir información. Ver figura 2.

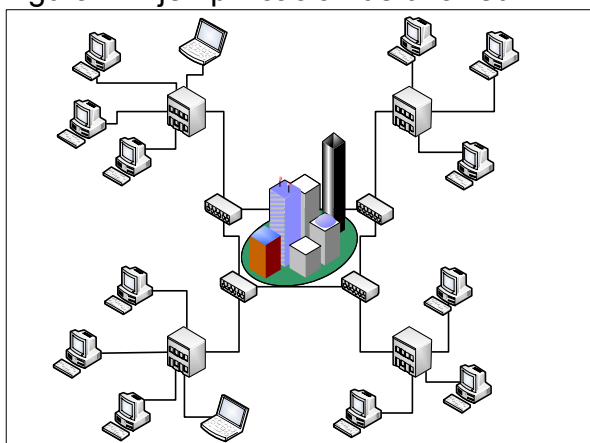
“Las LAN's tradicionales se ejecutan a una velocidad de 10 a 100 Mbp's, tienen un retardo bajo (microsegundos o nanosegundos) y cometen muy pocos errores. Las LAN's más nuevas funcionan hasta a 10 Gbps.”. (Tanenbaum & J. Wetherall, 2012)

## 2.1.3 Redes de Área Metropolitana

“Una red MAN abarca una ciudad. El ejemplo más conocido de una MAN es la red de televisión por cable disponible en muchas ciudades.” (Tanenbaum & J. Wetherall, 2012)

Las redes MAN interconectan varias redes LAN dentro de una gran área geográfica, por lo tanto una MAN permite que dos nodos remotos se comuniquen como si estos estuvieran conectados en una LAN. Ver figura 2.

Figura 2. Ejemplificación de una red MAN.



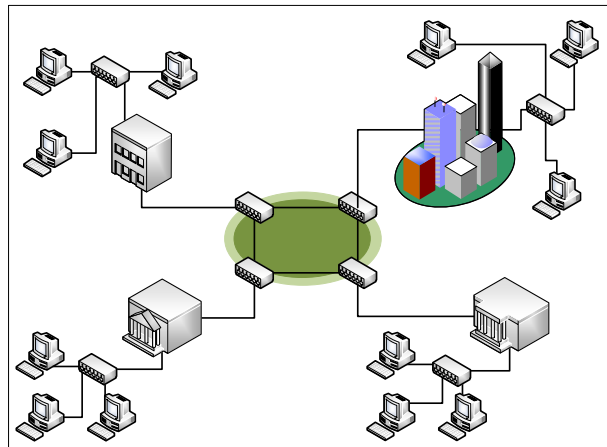
Fuente: (Stallings, Network Security Essentials: Applications And Standards, 2011)



## 2.1.4 Redes de Área Ampla

“Generalmente, se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación”. (Stallings, Comunicaciones y Redes de Computadores, 2010). Ver figura número 3.

Figura 3. Ejemplificación de una red **WAN**



Fuente: (Stallings, Network Security Essentials: Applications And Standards, 2011)

Una WAN es una red que une varias redes LAN por lo que los usuarios de esta red no se encuentran ubicados en la misma área geográfica, estas redes son implementadas mayormente por empresas privadas, pero el más claro ejemplo de estas redes es el internet.

### **2.1.5 Topologías de redes**

Las redes cuentan con una forma de interconectarse ya sea de forma física o inalámbrica a esto se le conoce como **topología** y juega un papel muy importante en la estructura de las redes, la importancia de la forma en la que una red de computadoras se encuentra conectada es para saber cuál será su correcto funcionamiento así como su rapidez, confiabilidad y también si es posible su modificación u expansión en caso de que sea necesario llevar a cabo dicha acción; Existen dos tipos de topologías, las topologías lógicas y las topologías físicas, estas últimas se pueden implementar de distintas formas.

Una topología lógica es la forma en la que se transmite la información en la red, independientemente de la conexión física de la red.

Por lo contrario la topología física como su clasificación lo dice es la forma física en la que se encuentran conectados cada uno de los nodos en la red, dentro de estas topologías se encuentran las siguientes:

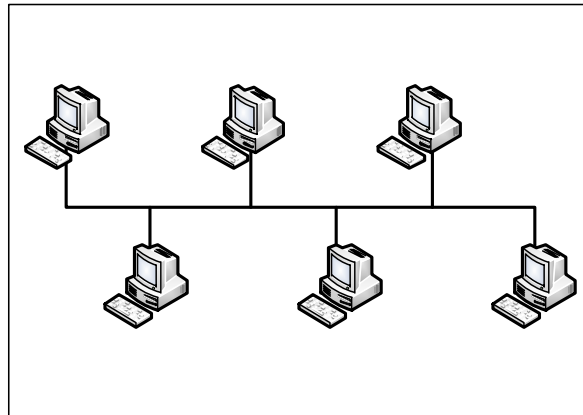
### **2.1.6 Topología de bus**

Una Topología bus, es una red donde se utiliza un solo cable que corre desde un extremo al otro de la red y que tiene diferentes dispositivos (llamados nodos) de red conectados a un cable en puntos diferentes. La figura 4 muestra una red con Topología bus.

Los diferentes tipos de red en bus tienen distintas especificaciones, las cuales incluyen los factores siguientes:

- Cuántos nodos pueden tener un solo segmento.
- Cuántos segmentos se pueden tener si se utilizan repetidores.
- La cercanía a la que pueden estar los nodos entre sí.
- La longitud total de un segmento.
- Qué tipo de cable coaxial se requiere.
- Cómo deben terminarse los extremos del bus.

Figura 4. Topología de bus.



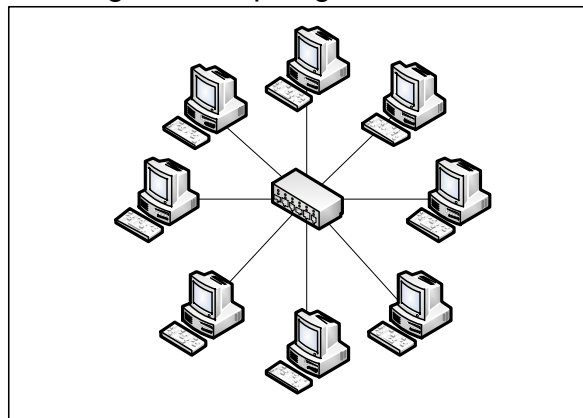
Fuente: (Stallings, Comunicaciones y Redes de Computadores, 2010)

### 2.1.7 Topología de estrella

La topología de estrella es un arreglo físico donde un concentrador trabaja como punto principal para interconectar a cada nodo dentro de la red.

Todo el tráfico que existe de cualquier conexión en la red hacia el concentrador es difundido a todos los nodos conectados al mismo concentrador, por lo que todo el ancho de banda de cualquier conexión a los nodos se comparte con todos los demás nodos, la topología de estrella se representa en la figura 5 se ejemplifica la topología de estrella.

Figura 5. Topología de estrella.



Fuente: (Stallings, Comunicaciones y Redes de Computadores, 2010)

“Las redes con topología de estrella tienen dos desventajas implícitas en comparación con las redes de bus, son más costosas. Es necesaria una mayor cantidad de cable y se necesita mayor cantidad de mano de obra”. (Hallberg, 2014)

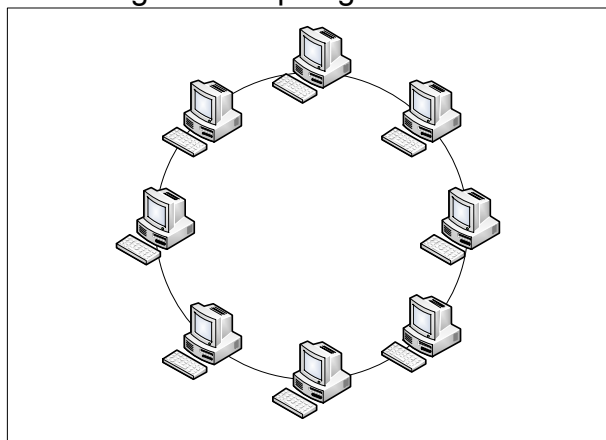
Una de las ventajas que se tiene con esta topología a comparación de la de bus es que si una de las conexiones con alguno de los nodos se ve afectada o dañada solamente dejara de funcionar dicha conexión y no afectara a toda la red como como sucedería en el caso de la topología de bus.

### 2.1.8 Topología de anillo

“En la topología de anillo, la red consta de un conjunto de **repetidores** unidos por enlaces punto a punto formando un bucle cerrado. El repetidor es un dispositivo relativamente simple, capaz de recibir datos a través del enlace y de transmitirlos”. (Stallings, Comunicaciones y Redes de Computadores, 2010)

Los datos en esta red se transmiten por medio de **tramas**, las cuales circulan por el anillo entrando y saliendo de los equipos hasta que el equipo destino identifica la trama, en este punto la trama deja de circular por la red. Ver la figura 6.

Figura 6. Topología de anillo.



Fuente: (Stallings, Comunicaciones y Redes de Computadores, 2010)



estaciones de trabajo en una topología lógica de bus deben lograr obtener el derecho de transmisión. A diferencia de las transmisiones en un anillo lógico, todas las computadoras reciben los datos. Las computadoras miran la dirección de destino en los datos. Si esa dirección no está destinada a ellas, las computadoras descartan los datos.

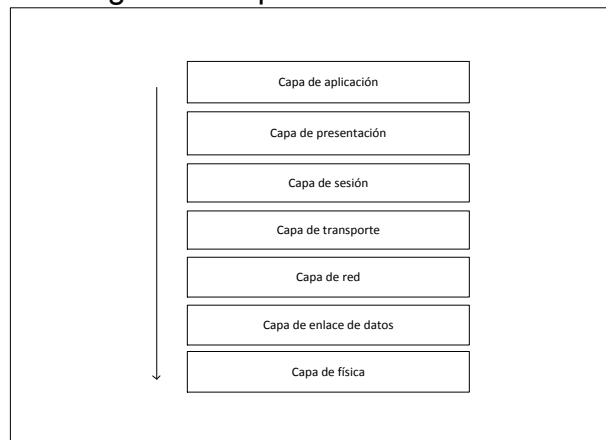
En una topología lógica de bus, cuando se produce una falla, la comunicación entre todos los dispositivos también falla. Una ventaja para la topología lógica de anillo es que, si se produce una falla, no todas las comunicaciones fallan, si no sólo las comunicaciones del segmento afectado.

Una red puede tener un tipo de topología lógica y un tipo de topología física completamente distintas. Por ejemplo, Ethernet, el tipo de red más frecuente, utiliza una estrella o una topología física en estrella extendida y una topología lógica en bus. Token Ring utiliza una estrella física y un anillo lógico. La Interfaz de datos distribuidos por fibra (**FDDI**) utiliza una topología física de anillo y una topología lógica de anillo.

## **2.2 Modelo OSI**

Se le llama **Modelo OSI** a la Interconexión de Sistemas Abiertos, del inglés Open Systems Interconnection (**OSI**), dicho modelo se basa en la propuesta desarrollada por la Organización Internacional de Normas (**ISO**), el modelo OSI cuenta con siete capas las cuales se muestran en la figura 8.

Figura 8. Capas del modelo OSI.



Fuente: (Stallings, Comunicaciones y Redes de Computadores, 2010)

### 2.2.1 Capa de aplicación

La capa de aplicación o capa siete, controla la forma en la que el sistema operativo y sus aplicaciones interactúan en la red, Esta capa suministra las herramientas que el usuario, de hecho ve. También ofrece los servicios de red relacionados con estas aplicaciones, como la gestión de mensajes, la transferencia de archivos y las consultas a base de datos.

Dentro de esta capa se encuentran aplicaciones que utilizan los usuarios de las cuales se pueden destacar las siguientes:

- Navegadores
- Motores de búsqueda
- Programas de correo electrónico
- Grupos de noticias y programas de chat
- Servicios de transacciones
- Audio/videoconferencia

### **2.2.2 Capa de presentación**

La capa de presentación, o capa seis, toma los datos que le proporcionan las capas inferiores y los procesa a fin de que puedan presentarse al sistema. Dentro de las funciones que se llevan a cabo en la capa de presentación se encuentran la compresión y descompresión de datos, así como el cifrado y descifrado de los mismos.

### **2.2.3 Capa de Sesión**

La capa de sesión, o capa cinco, define la conexión de una computadora de usuario a un servidor de red y de una computadora a otra en una red con configuración de igual a igual. Estas conexiones virtuales se conocen como sesiones. Incluyen la negociación entre el cliente y el anfitrión, o de igual a igual, en aspectos como el control de flujo, el procesamiento de transacciones, la transferencia de información de usuario y la autenticación de la red.

### **2.2.4 Capa de Transporte**

La capa de transporte o capa cuatro, realiza la administración de flujo de información desde un nodo de red hasta otro, se encarga de que los paquetes sean decodificados en la secuencia correcta y que se reciban todos, así mismo identifica de manera única a cada una de las computadoras o nodos de la red.

### **2.2.5 Capa de Red**

La capa de red o capa tres, es en la cual se define la forma en que los paquetes de datos llegan de un punto a otro en la red y lo que va dentro de cada paquete, además define los diferentes protocolos de paquete, como el Protocolo Internet (**IP**), y el Protocolo de Intercambio de Internet (**IPX**). Estos protocolos de paquetes incluyen información de enrutamiento fuente destino. La información de enrutamiento que contiene cada paquete le dice a la red dónde enviarlo para que llegue a su destino.



## 2.2.6 Capa de enlace de datos

La capa de enlace de datos, o capa dos, define los estándares que asignan un significado a los bit's que transporta la capa física. Establece un protocolo confiable a través de la capa física a fin de que la capa de red (capa tres) pueda transmitir sus datos. La capa de enlace de datos típicamente detecta y corrige los errores para asegurar un flujo de datos confiable. A los elementos de datos que transporta la capa de enlace de datos se les llama tramas.

La capa de enlace de datos se divide generalmente en dos subcapas, llamadas control de enlace lógico (**LLC**) y control de acceso al medio (**MAC**). Si se utilizan, la subcapa LLC lleva a cabo tareas como establecer y terminar una llamada y transferir datos. La subcapa MAC es responsable del ensamblado y desensamblado de las tramas, la detección y corrección de errores y el direccionamiento.

## 2.2.7 Capa Física

La primera capa, la capa física, define las propiedades del medio físico de transmisión que se utiliza para llevar a cabo la conexión de la red. Las especificaciones de la capa física se resumen en un medio físico de transmisión (un cable de red) que transmite un flujo de bit's entre los nodos a través de la red física. La conexión física puede ser punto a punto o multipunto y puede consistir en transmisiones **half-duplex** (en una dirección a la vez) o **full-duplex** (en ambas direcciones simultáneamente). Además, los bits pueden transmitirse ya sea en serie o en paralelo. La especificación de la capa física también define el cable que debe utilizarse, los voltajes en el cable, la temporización de las señales eléctricas, la distancia que puede soportar, etc.

## **2.3 IEEE**

Las siglas **IEEE** corresponden a The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros en eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación.

Su creación se remonta al año 1884, contando entre sus fundadores a personalidades de la talla de Thomas Alva Edison, Alexander Graham Bell y Franklin Leonard Pope. En 1963 adoptó el nombre de IEEE al fusionarse asociaciones como el **AIEE** (American Institute of Electrical Engineers) y el **IRE** (Institute of Radio Engineers). (IEEE Advancing Technology for Humanity SECCION MEXICO, s.f.)

## **2.4 Redes Inalámbricas**

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

### **2.4.1 Cómo funcionan las redes inalámbricas**

En estas redes se utilizan las ondas electromagnéticas para enlazar mediante un concentrador, los dispositivos de una red, remplazando los cables de las redes LAN convencionales.

## 2.4.2 Ventajas de utilizar redes inalámbricas

La primera ventaja que aparece y una de la más importante es la **movilidad** que adquiere el usuario de estas redes. Una computadora o cualquier dispositivo. Puede acomodarse en cualquier punto dentro del área de cobertura de la red, sin tener que preocuparnos si es posible o no hacer llegar un cable de red hasta este lugar. No es necesario estar atado a un cable.

La **portabilidad** es otro punto importante de las redes inalámbricas, ya que permite a los usuarios moverse junto con los dispositivos conectados a la red inalámbrica, tales como notebooks, netbooks o similares, sin perder el acceso a la red. Se facilita el trabajo permitiendo la movilidad por toda el área de cobertura.

La flexibilidad es otra ventaja de las redes sin cables. Podemos situar nuestra notebook sobre la mesa del escritorio para luego desplazarla hacia el dormitorio, sin tener que realizar el más mínimo cambio de configuración de la red. (Salveti, 2011)

## 2.4.3 Desventajas de utilizar redes inalámbricas

Las redes inalámbricas también presentan ciertas desventajas, las redes cableadas en la actualidad, trabajan a velocidades de 100 Mbp's a 10.000 Mp's, que se reduce en redes sin cables y se traduce en menor velocidad, Wi-Fi trabaja a velocidades de 11 a 108 Mbp's.

Una de las ventajas que se convierte en una desventaja si hablamos de que para estas redes no es necesario un medio físico de transmisión para la información debido a que cualquier persona con una computadora o un teléfono con Wi-Fi pueden intentar acceder a nuestra red tan solo estando en el área de cobertura, ya que esta área no está delimitada por paredes u otras barreras.

El alcance de una red inalámbrica está delimitado por la potencia de los equipos y la ganancia de las antenas, así si estos puntos no son lo suficientemente buenos habrá sitios sin cobertura en las instalaciones donde se encuentre nuestra red. (Salveti, 2011)

## 2.4.4 Componentes de las redes inalámbricas

Los dispositivos que son necesarios en las redes inalámbricas son:

- **AP** o Access Point: Se considera como el punto principal de emisión y recepción. Este punto concentra la señal de los nodos inalámbricos y centraliza el reparto de la información en toda la red local. También realiza el vínculo entre los nodos inalámbricos y la red cableada, por esto se suele llamar puente. Ver figura 9.

Figura 9. AP inalámbrico de doble banda N300 Linksys WAP300N.



Fuente: linksys.com

- **Router inalámbrico:** Si se cuenta con una conexión **ADSL** que nos da acceso a Internet a través de nuestra línea telefónica, este dispositivo permite distribuir Internet mediante cables y de forma inalámbrica con el punto de acceso que tiene integrado.

También realiza restricciones de acceso, por usuarios, servicios, horarios, entre otros y en muchos casos puede controlar el ancho de banda y las prioridades de acceso por cliente conectado o servicio. Todas estas facilidades nos permiten tener un control de lo que ocurre en nuestra red inalámbrica o cableada. Ver figura 10.

Figura 10. Router inalámbrico Wireless-G Linksys WRT54GL.



Fuente: linksys.com

- **Antenas:** Son un elemento muy importante en una red, ya que se encargan de transformar la energía de corriente alterna, generada en los equipos inalámbricos de la red, en un campo electromagnético o viceversa para que la comunicación pueda realizarse, Existen diferentes tipos de antenas, algunas son complejas y robustas pero otras son fáciles de instalar y con buen rendimiento. Lo que siempre se busca es que la transformación de energía sea realizada sin pérdidas, o sea de forma óptima. Se pueden diferenciar las antenas por su forma de irradiar la energía electromagnética, así tenemos antenas omnidireccionales (que irradian en todas las direcciones) y las direccionales (que difunden la energía electromagnética en una sola dirección). Ver figura 11.

Figura 11. Tipos de antenas para la distribución de señal inalámbrica.



Fuente: activeb.es

- **Tarjetas de red inalámbrica:** recibe y envía información entre las computadoras de la red, es una parte imprescindible para conectarnos de forma inalámbrica. Existen placas de diferentes velocidades, entre 54 Mbp's y 108 Mbp's. Todas tienen una antena (que puede ser externa o interna) en general de baja ganancia, que puede ser reemplazada por otra de mayor ganancia para mejorar la conexión (cuando el dispositivo lo permita).

Existen tres tipos de adaptadores: **PCI**, usados en nuestras PC's de escritorio, PCMCIA/PCcard, utilizados en las primeras laptops o notebooks, y USB, que son muy comunes hoy en día para notebooks o netbook's. Ver figura 12.

Figura 12. Placas de red inalámbricas.



Fuente: seguridadwireless.net

#### 2.4.5 Vulnerabilidad en las redes Wi-Fi

Las vulnerabilidades en las redes Wi-Fi son la principal fuente de atención para quienes pretenden aprovecharse de ellas mediante distintos tipos de ataques tales como:

- Acceso: wardriving.
- Cifrado WEP: Ataques FSM, KoreK, etc.
- Ataques de Man-in-the-Middle: Rogue AP's.
- Vulnerabilidades en AP's en modo "Bridge":
- Ataques de Denegación de Servicio.

## 2.5 Seguridad en redes inalámbricas

La seguridad en las redes inalámbricas es un tema muy importante ya que por la naturaleza de estas es más propensa a sufrir ataques ya que los dispositivos que pueden conectarse no se están obligados a encontrarse físicamente en un área específica.

### 2.5.1 WEP (Wired Equivalent Privacy)

Es el protocolo de encriptación por defecto incluido en el primer estándar de **IEEE** 802.11, está basado en el algoritmo de encriptación RC4 con una llave secreta de 40 bit's o 104 bit's.

**WEP** Ofrece dos niveles de seguridad, encriptación a 64 o 128 bit's. La encriptación usa un sistema de claves. La clave de la tarjeta de red del ordenador debe coincidir con la clave del router.

64-bit's (10 dígitos hexadecimales): Se pueden introducir 5 **caracteres ASCII** o 10 dígitos hexadecimales (0 a 9 y a a F).

128-bit **WEP**: usa una clave más larga y, por tanto, más complicada de acertar. Es prácticamente la misma, sólo que ahora hay que introducir 13 caracteres **ASCII** o 26 dígitos hexadecimales.

### 2.5.2 WPA (Wireless Protected Access)

Ofrece dos tipos de seguridad, con servidor de seguridad y sin servidor. Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor). No todos los dispositivos wireless lo soportan.

**WPA** incluye las siguientes tecnologías:

- **IEEE 802.1X**: estándar de IEEE que proporciona control de acceso en redes basado en puertos. El concepto de puerto, en un principio pensado para las ramas de un Switch, también se pueden aplicar a las distintas conexiones de un AP con las estaciones. Las estaciones tratarán de conectarse a un puerto del AP, el cual mantendrá el puerto bloqueado hasta que el usuario se identifique.
- **EAP**: (Extensible Authentication Protocol) Definido como el protocolo de autenticación extensible, el cual tiene como propósito llevar a cabo las tareas de autenticación, autorización y contabilidad.
- **TKIP**: (Temporal Key Integrity Protocol) Es el protocolo encargado de la generación de la clave para cada trama.
- **MIC**: (Message Integrity Code) Código que verifica la integridad de los datos de las tramas.

**WPA2 o IEEE 802.11i**: incluye un algoritmo de **cifrado AES** (Advanced Encryption Standard), se trata de un algoritmo de cifrado de bloque con claves de 128 bit's. El cual requiere un **hardware** potente para realizar sus algoritmos.

## **2.6 IEEE 802.11x (Wireless LAN, Wi-Fi)**

**IEEE 802.11** también recibe el nombre de Wi-Fi y hace referencia a los **sistemas DSS** operando a 1, 2, 5.5 y 11 Mbp's, donde todos cumplen con la norma de forma retrospectiva (o sea ofrecen compatibilidad con productos anteriores). Tener esta compatibilidad para atrás es importante, ya que nos permite actualizar nuestra red sin necesidad de cambiar nada.

Luego, en el estándar IEEE 802.11a abarcamos los dispositivos WLAN que operan en la banda de 5 GHz, por lo tanto no se permite la interoperabilidad con dispositivos funcionando a 2,4 GHz como los de 802.11b, dada su frecuencia.

Una nueva enmienda llamada IEEE 802.11g nos ofrece compatibilidad para atrás para dispositivos 802.11b utilizando una tecnología de modulación llamada **Multiplexión**



por División de Frecuencia Ortogonal (**OFDM** por sus siglas en inglés) y además obtenemos la misma tasa de transferencia que 802.11a.

Tabla 2 . Comparación de las diferentes tecnologías normalizadas por la IEEE.

ESTÁNDAR WLAN	EEE 802.11B	EEE 802.11A	EEE 802.11G	EEE 802.11N
<b>Organismo</b>	IEEE	IEEE	IEEE	IEEE
<b>Financiación</b>	1999	2002	2003	2005
<b>Denominación</b>	Wi-Fi	Wi-Fi 5	Wi-Fi	
<b>Banda de frecuencia</b>	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz y 5.8 GHz
<b>Velocidad máxima</b>	11 Mbp's	54 Mbp's	54 Mbp's	108 Mbp's
<b>Throughput medio</b>	5.5 Mbp's	36 Mbp's		
<b>Interface aire</b>	DSSS	OFDM	OFDM	OFDM

Fuente: (Salvetti, 2011)

## 2.7 Dispositivos de red

Los dispositivos de red son aquel hardware que permite la comunicación entre dos computadoras conectados en una red y así mismo, conectarse a proveedores de servicios de internet, estos dispositivos se dividen en activos y pasivos.

### 2.7.1 Dispositivos activos

Son aquellos dispositivos electrónicos que se encargan de distribuir el **ancho de banda** a determinada cantidad de equipos en una red. Estos dispositivos se encargan de distribuir de forma activa la información a través de la red.

- **Hub**: realiza sus funciones en la capa física del **modelo OSI**.
- **Bridge**: este dispositivo es capaz de interconectar dos redes, utilizando un direccionamiento a nivel de enlace de datos, por lo que sus funciones se encuentran en la capa de enlace del modelo OSI.
- **Tarjetas de red**: las tarjetas de red son consideradas en la capa de enlace del modelo OSI ya que cada una de estas cuenta con una dirección de control de acceso al medio o Media Access Control Address mejor conocida como **MAC**

**Address**, que es utilizada para el control de comunicaciones de datos para el host dentro de la red y controla el acceso al medio.

- **Switch**: la función de este dispositivo es la de interconectar dos o más segmentos de red de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección **MAC** de destino de las tramas en la red por ello este dispositivo es considerado en la capa de enlace del modelo OSI.
- **Router**: es un router es un dispositivo que se encarga de pasar paquetes de datos entre redes, basado en las direcciones de la capa de red del modelo OSI y puede tomar decisiones de la mejor ruta para entregar dichos paquetes en la red.

## 2.7.2 Dispositivos pasivos

Los dispositivos pasivos son aquellos elementos que se utiliza para interconectar los enlaces de una red de datos.

Los dispositivos pasivos que se consideran dentro de la capa física del **modelo OSI** son los siguientes.

- **Jack's**
- **Conectores**
- **Cable UTP**
  - El cable **UTP** par trenzado es un tipo de cableado de cobre que se utiliza para las comunicaciones telefónicas y la mayoría de las redes **Ethernet**. Un par de hilos forma un circuito que transmite datos. El par está trenzado para proporcionar protección contra **crosstalk**, que es el ruido generado por pares de hilos adyacentes en el cable. Los pares de hilos de cobre están envueltos en un aislamiento de plástico con codificación de color y trenzados entre sí. Un revestimiento exterior protege los paquetes de pares trenzados.
  - Cuando circula electricidad por un hilo de cobre, se crea un campo magnético alrededor del hilo. Un circuito tiene dos hilos y, en un circuito, los dos hilos tienen campos magnéticos opuestos. Cuando los dos hilos

del circuito se encuentran uno al lado del otro, los campos magnéticos se cancelan mutuamente. Esto se denomina efecto de cancelación. Sin el efecto de cancelación, las comunicaciones de la red se ralentizan debido a la interferencia que originan los campos magnéticos.

- **Tipos básicos de cables de par trenzado:**

- Par trenzado no blindado (**UTP**): Cable que tiene dos o cuatro pares de hilos. Es te tipo de cable cuenta sólo con el efecto de cancelación producido por los pares trenzados de hilos que limita la degradación de la señal que causa la interfaz electromagnética (**EMI**) y la interferencia de radiofrecuencia (**RFI**). El cableado **UTP** es más comúnmente utilizado en redes. Los cables **UTP** tienen un alcance de 100 m.
- Par trenzado blindado (**STP**): Cada par de hilos está envuelto en un papel metálico para aislar mejor los hilos del ruido. Los cuatro pares de hilos están envueltos juntos en una trenza o papel metálico. El cableado **STP** reduce el ruido eléctrico desde el interior del cable. Asimismo, reduce la **EMI** y la **RFI** desde el exterior del cable.

- **Clasificación en categorías**

Los cables **UTP** vienen en varias categorías que se basan en dos factores:

- La cantidad de hilos que contiene el cable.
- La cantidad de trenzas de dichos hilos.

El cable **UTP categoría 1** realizaba la transmisión de datos con un ancho de banda de 0.4 MHz normalmente utilizado para líneas telefónicas y módems de banda ancha, actualmente se encuentra obsoleto, al igual que la **categoría 2**, solo que esta categoría la transferencia la realizaba a 4 MHz. La **Categoría 3** es el cableado que se utiliza para los sistemas de telefonía y para **LAN, Ethernet** a 10 Mbp's. La **Categoría 3** tiene cuatro pares de hilos.

La **Categoría 5** y la **Categoría 5e** tienen cuatro pares de hilos con una velocidad de transmisión de 100 Mbp's. Estas dos categorías de cable son las más comúnmente utilizadas. El cableado **Categoría 5e** tiene más trenzas por pie que el de **Categoría 5**. Estas trenzas adicionales contribuyen a evitar

la interferencia de fuentes externas y de otros hilos que se encuentran dentro del cable.

Algunos cables **Categoría 6** tienen un divisor plástico para separar los pares de hilos, lo que evita la interferencia. Los pares también tienen más trenzas que los del cable **Categoría 5e**.

- **Cable coaxial**

El cable coaxial es un cable con núcleo de cobre envuelto en un blindaje grueso. Se utiliza para conectar computadoras en una red. Existen diversos tipos de cable coaxial:

- Thicknet o 10BASE5: Cable coaxial que se utilizaba en redes y funcionaba a 10 megabits por segundo con una longitud máxima de 500 m.
- Thinnet 10BASE2: Cable coaxial que se utilizaba en redes y funcionaba a 10 megabits por segundo con una longitud máxima de 185 m.
- RG-59: El más comúnmente utilizado para la televisión por cable en los Estados Unidos.
- RG-6: Cable de mayor calidad que RG-59, con más ancho de banda y menos propensión a interferencia.

- **Cable de fibra óptica**

Una fibra óptica es un conductor de cristal o plástico que transmite información mediante el uso de luz. El cable de fibra óptica, tiene una o más fibras ópticas envueltas en un revestimiento. Debido a que está hecho de cristal, el cable de fibra óptica no se ve afectado por la interferencia electromagnética ni por la interferencia de radiofrecuencia. Todas las señales se transforman en pulsos de luz para ingresar al cable y se vuelven a transformar en señales eléctricas cuando salen de él.

El cable de fibra óptica puede alcanzar distancias de varias millas o kilómetros antes de que la señal deba regenerarse. El cable de fibra óptica es generalmente más costoso que el cable de cobre, y los conectores son más costosos y difíciles de ensamblar. Los conectores comunes para las redes de fibra óptica son **SC**, **ST** y **LC**.

- **Los dos tipos de cable de fibra óptica de cristal son:**
  - Multimodo: Cable que tiene un núcleo más grueso que el cable monomodo. Es más fácil de realizar, puede usar fuentes de luz (**LED**) más simples y funciona bien en distancias de hasta unos pocos kilómetros.
  - Monomodo: Cable que tiene un núcleo muy delgado. Es más difícil de realizar, usa láser como fuente de luz y puede transmitir señales a docenas de kilómetros con facilidad.
- **Canaleta**
- **Rosetas**
- **Patchpanel**

## **2.8 Protocolos y arquitectura de redes**

Una arquitectura de protocolos es una estructura en capas de elementos hardware y Software que facilita el intercambio de datos entre sistemas y posibilita aplicaciones distribuidas, como el comercio electrónico y la transferencia de archivos.

En los sistemas de comunicación, en cada una de las capas de la arquitectura de protocolos se implementa uno o más protocolos comunes. Cada protocolo proporciona un conjunto de reglas para el intercambio de datos entre sistemas.

La arquitectura de protocolos más utilizada es **TCP/IP**, constituida por las siguientes capas: física, acceso a la red, internet, transporte y aplicación.

Otra arquitectura de protocolos importante es el modelo de siete capas **OSI** (Open Systems Interconnection). (Stallings, Comunicaciones y Redes de Computadores, 2010)

## 2.8.1 Protocolo TCP

**TCP** permite a las aplicaciones comunicarse entre sí como si estuvieran conectadas físicamente. TCP envía los datos en un formato que se transmite carácter por carácter, en lugar de transmitirse por paquetes discretos. Esta transmisión consiste en lo siguiente:

- Punto de partida, que abre la conexión.
- Transmisión completa en orden de bytes.
- Punto de fin, que cierra la conexión.

TCP conecta un encabezado a los datos transmitidos. Este encabezado contiene múltiples parámetros que ayudan a los procesos del sistema transmisor a conectarse a sus procesos correspondientes en el sistema receptor.

También confirma que un paquete ha alcanzado su destino estableciendo una conexión de punto a punto entre los hosts de envío y recepción. Por tanto, el protocolo TCP se considera un protocolo fiable orientado a la conexión. (ORACLE, 2010)

## 2.8.2 Protocolo IP

El protocolo **IP** y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

- **Direcciones IP:** Las convenciones de direcciones IP forman parte del protocolo IP. Cómo diseñar un esquema de direcciones IPv4 introduce las direcciones IPv4 y las direcciones IPv6.
- **Comunicaciones de host a host:** El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.
- **Formato de paquetes:** el protocolo IP agrupa paquetes en unidades conocidas como datagramas.
- **Fragmentación:** Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete

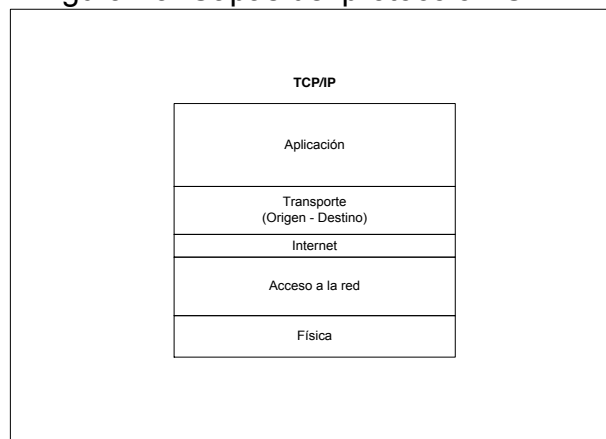
en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original. (ORACLE, 2010)

### 2.8.3 El protocolo TCP/IP

El protocolo **TCP/IP** estructura el problema de la comunicación en cinco capas las cuales son las siguientes:

- Capa física
- Capa de acceso a la red
- Capa internet
- Capa extremo-a-extremo o de transporte
- Capa de aplicación. Ver la figura 13.

Figura 13. Capas del protocolo **TCP/IP**.



**Fuente:** (Stallings, Comunicaciones y Redes de Computadores, 2010)

#### 2.8.3.1 La capa física

Define la interfaz física entre el dispositivo de transmisión de datos (por ejemplo, la estación de trabajo o el computador) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos y cuestiones afines.

#### 2.8.3.2 La capa de acceso a la red

Responsable del intercambio de datos entre el sistema final y la red a la cual está conectado. El emisor debe proporcionar a la red la dirección del destino, de tal manera que ésta pueda encaminar los datos hasta el destino apropiado. El emisor puede

requerir ciertos servicios que pueden ser proporcionados por el nivel de red, por ejemplo, solicitar una determinada prioridad. El Software en particular que se use en esta capa dependerá del tipo de red que se disponga.

### 2.8.3.3 La capa internet

El protocolo internet (**IP**, Internet Protocol) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los sistemas finales como en los en caminadores intermedios. Un encaminado es un procesador que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar al destino.

### 2.8.3.4 La capa de transporte

Independientemente de la naturaleza de las aplicaciones que estén intercambiando datos, es usual requerir que los datos se intercambien de forma fiable. Esto es, sería deseable asegurar que todos los datos llegan a la aplicación destino y en el mismo orden en el que fueron enviados. Por ello esta capa es en la que se agrupan todos los mecanismos que se requieren para cumplir con la función del transporte de los paquetes de datos, el Protocolo para el Control de Transmisión o Transmission Control Protocol por sus siglas en ingles TCP es el más utilizado para proporcionar esta funcionalidad.

En la figura 14 se puede apreciar una comparación entre las capas del modelo OSI y el **Protocolo TCP/IP**.

Figura 14. Comparación entre las arquitecturas OSI y TCP/IP.

OSI	TCP/IP
Aplicación	Aplicación
Presentación	
Sesión	Transporte (Origen - Destino)
Transporte	
Capa de red	Internet
Enlace de datos	Acceso a la red
Capa de física	Física

Fuente: (Stallings, Comunicaciones y Redes de Computadores, 2010)



## **2.8.4 Versiones del protocolo TCP/IP**

La importancia de la evolución del protocolo TCP/IP es de gran relevancia ya que en la actualidad el manejo de las direcciones IP para los dispositivos que se conectan al internet ha superado las expectativas que se tenían en las décadas pasadas, por ello es necesario la mejora de la distribución de dichas direcciones.

### **2.8.4.1 TCP/IP v4**

La versión utilizada en la actualidad del protocolo **TCP/IP** es la 4, en uso desde 1981, esta versión corresponde a 32 **bit's** por lo que dispone de  $2^{32}$  direcciones posibles, cada una de las cuales consta de cuatro grupos binarios de 8 bit's cada uno de ( $8 \times 4 = 32$ ), o lo que es lo mismo, cuatro grupos decimales, formado cada uno por tres dígitos.

### **2.8.4.2 TCP/IP v6**

La nueva versión del Protocolo de Internet cuenta con direcciones que poseen 128 **bit's** es decir  $2^{128}$  direcciones disponibles, una dirección IPv6 (128 bit's) se representa mediante ocho grupos de cuatro dígitos hexadecimales, cada grupo representando 16 bit's (dos octetos). Los grupos se separan mediante dos puntos (:). Un ejemplo de dirección IPv6 podría ser:

**2001:0db8:85a3:0000:0000:8a2e:0370:7334**

## **2.9 Protocolos de enrutamiento**

Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunican con otros routers con el fin de compartir información de enrutamiento. Dicha información es usada para construir y mantener las tablas de enrutamiento.

### **2.9.1 Enrutamiento estático**

El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los router's toda la información que contienen,

es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red.

Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- Existe una sola conexión con un solo **ISP**. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
- Un cliente no desea intercambiar información de enrutamiento dinámico.

### 2.9.2 Enrutamiento Predeterminado

Es una ruta estática que se refiere a una conexión de salida o Gateway de “último recurso”. El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida.

Esta ruta se indica como la red de destino **0.0.0.0/0.0.0.0**

### 2.9.3 Enrutamiento dinámico

Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de utilización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al **Software** del router que actualice la tabla de enrutamiento en consecuencia.

**Algunos protocolos de enrutamiento dinámicos son:**

- **RIP**: Protocolo de enrutamiento de **gateway** Interior por vector distancia.
- **IGRP**: Protocolo de enrutamiento de **gateway** Interior por vector distancia, del cual es propietario **CISCO**.
- **EIGRP**: Protocolo de enrutamiento de **gateway** Interior por vector distancia, es una versión mejorada de **IGRP**.
- **OSPF**: Protocolo de enrutamiento de **gateway** Interior por estado de enlace.
- **BGP**: Protocolo de enrutamiento de **gateway** exterior por vector distancia

Los algoritmos de enrutamiento se dividen en:

### **Vector Distancia**

Determina la dirección y la distancia hacia cualquier enlace de la red.

Su métrica se basa en lo que se le llama en redes “Numero de Saltos”, es decir la cantidad de router’s por los que tiene que pasar el paquete para llegar a la red destino, la ruta que tenga el menor número de saltos es la más óptima y la que se publicará:

- Visualiza la red desde la perspectiva de los vecinos
- Actualizaciones periódicas
- Transmite copias completas o parciales de las tablas de enrutamiento
- Convergencia lenta
- Incrementa las métricas a través de las actualizaciones

### **Estado de enlace**

También llamado “Primero la Ruta Libre más Corta” (**OSPF** – Open Shortest Path First), recrea la topología exacta de toda la red.

Su métrica se basa el retardo, ancho de banda, carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo prefiere una ruta por sobre otra. Estos protocolos utilizan un tipo de publicaciones llamadas Publicaciones de estado de enlace (**LSA**), que intercambian entre los router’s, mediante estas publicaciones cada router crea una base datos de la topología de la red completa. - Buscan una unión común de la topología de la red.

- Cada dispositivo calcula la ruta más corta a los otros router’s.
- Las actualizaciones se activan por los eventos (cambios en la topología) de la red.
- Trasmite actualizaciones.

### **Métrica**

La métrica es el análisis, y en lo que se basa el algoritmo del protocolo de enrutamiento dinámico para elegir y preferir una ruta por sobre otra, basándose en eso el protocolo creará la tabla de enrutamiento en el router, publicando sólo las mejores rutas.

Un protocolo de enrutamiento utiliza métrica para determinar qué vía utilizar para transmitir un paquete a través de un Intercambio.

**La métrica utilizada por protocolos de enrutamiento incluye:**

- **Número de saltos:** Número de router's por los que pasará un paquete.
- **Pulsos:** Retraso en un enlace de datos usando pulsos de reloj de PC.
- **Coste:** Valor arbitrario, basado generalmente en el ancho de banda, el coste económico u otra medida.
- **Ancho de banda:** Capacidad de datos de un enlace.
- **Retraso:** Cantidad de actividad existente en un recurso de red, como un router o un enlace.
- **Carga:** Cantidad de actividad existente en un recurso de red, como un router o un enlace.
- **Fiabilidad:** Se refiere al valor de errores de bits de cada enlace de red.
- **MTU:** Unidad máxima de transmisión. Longitud máxima de trama en octetos que puede ser aceptada por todos los enlaces de la ruta.

**2.9.3.4 Convergencia**

Es el objetivo principal de todos los protocolos de enrutamiento. Cuando un conjunto de enrutadores converge significa que todos sus elementos se han puesto de acuerdo y reflejan la situación real del entorno de red donde se encuentran. La velocidad con la que los protocolos convergen después de un cambio es una buena medida de la eficacia del protocolo de enrutamiento.

**Distancia administrativa y métrica**

Es una medida de la confianza otorgada a cada fuente de información de enrutamiento cada protocolo de enrutamiento lleva asociado una distancia administrativa. Los valores más bajos significan una mayor fiabilidad. Un enrutador puede ejecutar varios protocolos de enrutamiento a la vez, obteniendo información de una red por varias fuentes. En estos casos usará la ruta que provenga de la fuente con menor distancia administrativa de los protocolos de enrutamiento.

Cada protocolo de enrutamiento da prioridad a los caminos de mayor a menor fiabilidad usando un valor de distancia administrativa. Es preferible un valor bajo: por ejemplo, una ruta **OSPF** con una distancia administrativa de 110 prevalecerá sobre una ruta **RIP** con una distancia administrativa de 120. La siguiente tabla muestra las distancias administrativas por defecto usadas por los router's **CISCO**:

Tabla 3. Tabla de distancias administrativas por protocolo de enrutamiento.

<b>Protocolo</b>	<b>Distancia administrativa</b>
Directamente conectados	0
Ruta <b>EIGRP</b> sumariada	1
<b>BGP</b> externa	5
<b>EIGRP</b> interna	20
<b>IGRP</b>	90
<b>OSPF</b>	110
<b>RIP</b>	120
<b>EIGRP</b> externa	170
<b>BGP</b> interna	200
Desconocida	255

Fuente: (Bornhager, 2012)

## 2.10 Seguridad de redes

La seguridad en las redes de computadoras es uno de los aspectos con más importancia, ya que, si no se cuentan con medidas suficientes y adecuadas para asegurar la integridad de los dispositivos que se encuentran interconectados, así como los datos que se transfieren en ellas existe el riesgo de comprometer de forma parcial o total los recursos de la red.

### 2.10.1 Seguridad

El termino seguridad proviene del latín *securitas* hace referencia a la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligros, daños ni riesgos. (Larousse, 2015)

## 2.10.2 Seguridad en redes

Son las medidas para impedir, prevenir, detectar y corregir las violaciones de seguridad que se tienen implementadas en una red; así como durante la transmisión de información dentro de la misma.

Existen servicios y mecanismos de seguridad que se pueden implementar como medidas de seguridad o mejoramiento de la misma tales como:

### Medidas:

- **Autenticación:** es el servicio de seguridad que se encarga de garantizar la autenticidad de la comunicación.
  - **Autenticación de entidades origen/destino:** proporciona la confirmación de la identidad de una entidad de una asociación. Se proporciona en el establecimiento de una conexión o a veces durante la fase de transmisión de datos de dicha conexión. Intenta asegurar que una entidad no está realizando una suplantación o una repetición no autorizada de una conexión anterior.
  - **Autenticación del origen de los datos:** corrobora la fuente de una unidad de datos. No aporta protección contra la repetición o la alteración de unidades de datos.
- **Control de acceso:** es la capacidad de limitar y controlar el acceso a sistemas host y aplicaciones por medio de enlaces de comunicación
- **Confidencialidad de los datos:** es la confidencialidad de los datos transmitidos por medio de ataques pasivos. En función del contenido de una transmisión de datos.
- **Integridad de los datos:** Al igual que ocurre con la confidencialidad, la integridad se puede aplicar a una serie de mensajes, a un solo mensaje o a campos seleccionados de un mensaje. Nuevamente, el enfoque más útil y claro es la protección del flujo completo. Un servicio de integridad orientado a la conexión que funcione sobre un flujo de mensajes garantiza que los mensajes se reciben tal y como son enviados, sin duplicación, inserción, modificación, reordenación ni repeticiones.

- **No repudio:** El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje.
- **Servicio de disponibilidad:** es aquel que protege un sistema para asegurar su disponibilidad y trata los problemas de seguridad que surgen a raíz de ataques de interrupción de servicio. Depende de la gestión y control adecuados de los recursos del sistema y, por lo tanto, del servicio de control de acceso y otros servicios de seguridad.

#### **Mecanismos:**

- **Cifrado:** es el uso de algoritmos matemáticos para transformar datos en una forma inteligible. La transformación y la posterior recuperación de los datos depende de un algoritmo y cero o más claves de cifrado.
- **Firma digital:** datos añadidos a, o una transformación criptográfica de, una unidad de datos que permite al receptor verificar la fuente y la integridad de la unidad de datos y protegerla de la falsificación (por parte del receptor).
- **Intercambio de autenticación:** un mecanismo diseñado para comprobar la identidad de una entidad por medio del intercambio de información.
- **Relleno de tráfico:** la inserción de bits en espacios en un flujo de datos para frustrar los intentos de análisis de tráfico.
- **Control de enrutamiento:** permite la selección de rutas físicamente seguras para de terminados datos y permite los cambios de enrutamiento, especialmente cuando se sospecha de una brecha en la seguridad.
- **Notarización:** uso de un tercero confiable para asegurar ciertas propiedades en el intercambio de datos.

## **2.11 Firewall**

Un firewall es un sistema que promueve la política de seguridad entre dos redes, como una LAN e Internet. Los Firewall's pueden utilizar muchas técnicas diferentes para promover las políticas de seguridad y puede ser Software, hardware o mixtos.

(que puede ser una computadora configurada para esta tarea en particular, que corra Software de Firewall o un dispositivo dedicado de Firewall que contenga una computadora dedicada) que se instala entre las dos redes y refuerza las políticas de seguridad. En general, Firewall's se colocan entre la LAN de una compañía e Internet.

Existen básicamente dos diferentes tipos de Firewall's basados en red y en aplicación.

### **2.11.1 Firewall basado en red**

Trabaja a nivel paquetes y, usualmente, implementa técnicas de filtrado que permite que éstos entren a la red y se comparen con un conjunto de reglas programadas en Firewall antes de que se les permita a los paquetes cruzar la frontera entre las dos redes.

Las reglas del filtrado de paquetes pueden admitir o rechazar paquetes que estén basados en la dirección fuente o la dirección destino, o basados en un puerto **TCP/IP**.

### **2.11.2 Firewall basado en aplicación**

Actúa como Proxy entre las dos redes, de forma que no circule tráfico directamente entre las dos redes. En lugar de ello, actúa como un Proxy para que los usuarios de una red interactúen con los servicios de otra red.

Un Firewall puede ayudar a impedir que hackers o Software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un Firewall también puede ayudar a impedir que el equipo envíe Software malintencionado a otros equipos.

Un Firewall crea una barrera entre Internet y el equipo, igual que la barrera física que constituiría una pared de ladrillos. (Microsoft, 2016)



Un sistema de Firewall actúa como una barrera central para reforzar el acceso a los servicios que se ejecutan tanto en el interior como en el exterior de la red. El Firewall intentará prevenir los ataques del exterior contra las máquinas del interior de la red, denegando intentos de conexión desde lugares no autorizados.

Al momento de instalar y configurar un sistema de Firewall en nuestra red tenemos que tener en cuenta lo siguiente:

- Todo el tráfico que sale del interior hacia el exterior de la red que se quiere proteger, y viceversa, debe pasar por el Firewall.
- Solo el tráfico autorizado, definido en las políticas de seguridad locales del sistema, podrá traspasar el bloqueo.
- El propio Firewall debe estar protegido contra posibles intrusiones. Esto implica el uso de un sistema operativo confiable con suficientes características de seguridad.

### **2.11.3 Características adicionales de los Firewall's**

Debido a que los sistemas de **Firewall** se ubican en un punto de choque, estos sistemas pueden ofrecer algunas funciones interesantes, algunas de estas características adicionales incluyen:

- **Filtrado de contenido:** Muchas de las organizaciones desean evitar que sus usuarios utilicen los recursos corporativos para navegar por determinados sitios web no deseados. El filtrado de contenido ofrecido por algunos sistemas de Firewall puede bloquear el acceso a estos sitios web, al mismo tiempo que protege la red de cualquier código malicioso insertado en sus páginas.
- **Red Privada Virtual:** o **VPN** por sus siglas en inglés, este tipo de funcionalidad ofrecido por la mayoría de los sistemas de Firewall actuales, permite la construcción de un túnel seguro entre dos puntos de la red, normalmente para proteger las comunicaciones de una red a través de una red hostil (como la internet).

- **Traducción de Direcciones de Red:** o **NAT** aunque no se trata estrictamente de una funcionalidad relacionada con la seguridad, la mayoría de los sistemas de Firewall ofrecen la posibilidad de realizar NAT y poder así asociar direcciones IP reservadas a direcciones válidas.
- **Balanceo de la carga:** el balanceo de la carga ofrecida por muchos sistemas cortafuegos es la tarea de segmentar el tráfico de una red de forma distribuida. Algunos sistemas cortafuegos ofrecen actualmente funcionalidades que pueden ayudar, por ejemplo, la distribuir tráfico **FTP** o **HTTP** de forma totalmente distribuida.
- **Tolerancia de fallos:** algunos sistemas cortafuegos ofrecen actualmente soporte para determinar tipos de fallos. Para ello, se suele utilizar funcionalidades de Alta Disponibilidad o por sus siglas en ingles **HA** (High-Availability), En estas situaciones, la mayor parte de las estrategias incluyen la utilización de distintos sistemas cortafuegos sincronizados, de manera que uno de los sistemas estará a la espera de que se produzca un fallo en el equipo original para ponerse en funcionamiento y sustituirlo.
- **Detección de ataques e intrusiones:** muchos de los fabricantes de sistemas cortafuegos incorporan a sus productos la capacidad de detectar exploraciones y ataques conocidos. Aunque este tipo de funcionalidad no comporta un problema en sí mismo, deberíamos tener presente que puede llegar a suponer una carga de trabajo adicional y que puede entorpecer la actividad principal del sistema cortafuegos.
- **Autenticación de usuarios:** debido a que un sistema de Firewall es un punto de entrada a la red, puede llevar a cabo una autenticación adicional a la que efectúan los servicios ofrecidos por la misma. Así, la autenticación de un sistema de Firewall tendrá la finalidad de permitir o rechazar la conexión al usuario que solicita una conexión con un servicio no permitido.
- **Proxy:** es un intermediario anónimo, generalmente para los usuarios de una red por ejemplo, puede existir un Proxy para navegar por las páginas web, de forma que la computadora del usuario no tenga que estar conectada al sistema remoto, excepto a través del servidor Proxy.

## 2.11.4 Ventajas de un firewall

- **Control.** Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al Proxy.
- **Ahorro.** Por tanto, sólo uno de los usuarios (el Proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad.** Si varios clientes van a pedir el mismo recurso, el Proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- **Filtrado.** El **Proxy** puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación.** Como intermediario que es, un **Proxy** puede falsificar información, o modificarla siguiendo un algoritmo.
- **Anonimato.** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo, cuando hay que hacer necesariamente la identificación.

## 2.11.5 Desventajas de un firewall

- **Abuso:** Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- **Carga:** Un **Proxy** ha de hacer el trabajo de muchos usuarios.
- **Intromisión:** Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el **Proxy**. Y menos si hace de caché y guarda copias de los datos.
- **Incoherencia:** Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.

- **Irregularidad:** El hecho de que el **Proxy** represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como **TCP/IP**).

## 2.12 Amenaza

Una posibilidad de violación de la seguridad, existe cuando se da una circunstancia, capacidad acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro que podría explotar una vulnerabilidad.

Consiste en la presencia de una o más factores de diversa índole (personas, maquinas o sucesos) que de tener oportunidad atacarían al sistema provocando daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las cuales hay que proteger a los sistemas, desde los físicos como los cortes eléctricos, fallos de hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de Software malicioso (**virus, troyanos, gusanos**) o el robo, destrucción o modificación de la información. (Stallings, Network Security Essentials: Applications And Standards, 2011)

## 2.13 Ataque

Un salto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado para aludir los servicios de seguridad y violar la política de seguridad de un sistema.

Un ataque a la seguridad es cualquier acción que comprometa la seguridad de la información de cualquier organización. (Stallings, Network Security Essentials: Applications And Standards, 2011)

## 2.14 Vulnerabilidad

Dependiendo del enfoque que se le dé a la seguridad informática, un sistema informático está expuesto al peligro por medio de dos factores: Las amenazas y las vulnerabilidades.

Las vulnerabilidades constituyen el otro factor que pone en peligro la seguridad de un sistema, generalmente se cree que una vulnerabilidad es un punto débil de un sistema y aunque no es una definición incorrecta, tampoco expresa en su totalidad lo que es una vulnerabilidad. (Stallings, Network Security Essentials: Applications And Standards, 2011)

### **2.14.1 Definición de vulnerabilidad**

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

### **2.14.2 Tipos de Vulnerabilidades**

Las vulnerabilidades son el resultado de errores de programación (**bugs**), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes.

Para esta investigación, se clasifican las vulnerabilidades en seis tipos: Físicas, naturales, de hardware, de Software, de red y de factor humano.

#### **2.14.2.1 Vulnerabilidades físicas**

Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema. (UNAM, s.f.)

Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada. (UNAM, s.f.)

### **2.14.2.2 Vulnerabilidades naturales**

Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.

Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo no disponer de reguladores, **no-breaks**, mal sistema de ventilación o calefacción, etc. (UNAM, s.f.)

### **2.14.2.3 Vulnerabilidades de hardware**

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema. (UNAM, s.f.)

### **2.14.2.4 Vulnerabilidades de Software**

Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo, controles de acceso, seguridad, implantación, etc.). Ambos factores hacen susceptible al sistema a las amenazas de Software. (UNAM, s.f.)

### **2.14.2.5 Vulnerabilidades de red**

Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible interceptación de la información por personas no autorizadas y con fallas en la disponibilidad del servicio. (UNAM, s.f.)

Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de **hardware**, **Software**, físicas e incluso naturales. (UNAM, s.f.)

#### **2.14.2.6 Factor humano**

Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema. Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo.

Los actos contra la seguridad realizados a conciencia por un elemento humano (Como el robo de información o la destrucción de los sistemas) pueden ser el resultado de una vulnerabilidad humana, ya sea por un usuario que accidentalmente revela las contraseñas de acceso o no revisa periódicamente las bitácoras de actividades del equipo de cómputo a fin de buscar actividades sospechosas por citar algunos ejemplos. Un usuario resentido o con poca lealtad a la organización es una amenaza y una vulnerabilidad humana al mismo tiempo, pues él puede convertirse en el autor directo de ataques al sistema o revelar intencionalmente información del sistema a personas no convenientes.

Finalmente es importante hacer una reflexión en el sentido de que las vulnerabilidades se pueden reducir, eliminar o controlar lo que ayuda entonces a contrarrestar la posibilidad de que una amenaza se materialice y llegue a convertirse en un ataque.

De manera que el riesgo es el daño potencial que puede surgir por un proceso presente o suceso futuro, es decir, es la posibilidad de que un peligro pueda materializarse.

“El riesgo es el producto de la ocurrencia de la amenaza y su consecuencia” (UNAM, s.f.)

### 2.14.3 Ataques a la seguridad

Los ataques que se pueden sufrir en una red pueden ser clasificados en dos tipos, los pasivos, que son aquellos en los que los usuarios que están realizando el ataque no realizan alguna actividad en la cual se pueda interferir en el flujo de información, ocultando de esta manera su intrusión por lo cual son más difíciles de detectar. Por otra parte el segundo tipo de ataque denominado activo es en el cual los intrusos se encargan de realizar algún tipo de alteración en la información o red que están atacando.

Tabla 4. Comparación de los tipos de ataques a la seguridad de una red.

Ataques a la seguridad	
Ataques pasivos	Ataques activos
Los ataques pasivos se dan en forma de escucha o de observación no autorizadas de las transmisiones.	Los ataques activos constan en hacer una modificación del flujo de datos.
Dos categorías: la <b>obtención de contenidos de mensajes</b> y el <b>análisis del tráfico</b> .	Cuatro categorías: <b>suplantación de identidad, repetición, modificación de mensajes e interrupción de servicio</b>
No implican alteraciones en los datos	Implican la modificación o alteración de los datos

Fuente: Elaboración Propia

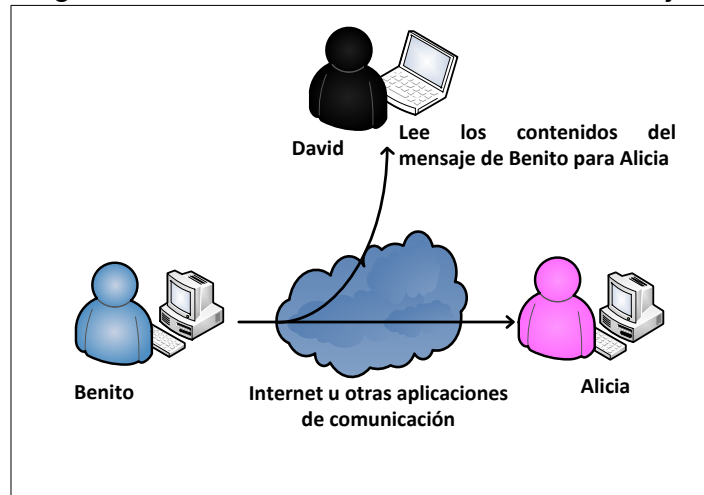
#### 2.14.3.1 Ataques pasivos

##### La obtención de contenidos

Se entiende fácilmente. (Figura 16). Una conversación telefónica, un mensaje por correo electrónico y un fichero que es enviado pueden contener información confidencial. Queremos evitar que un oponente conozca los contenidos de estas transmisiones.



Figura 15. Obtención de contenido de mensaje.



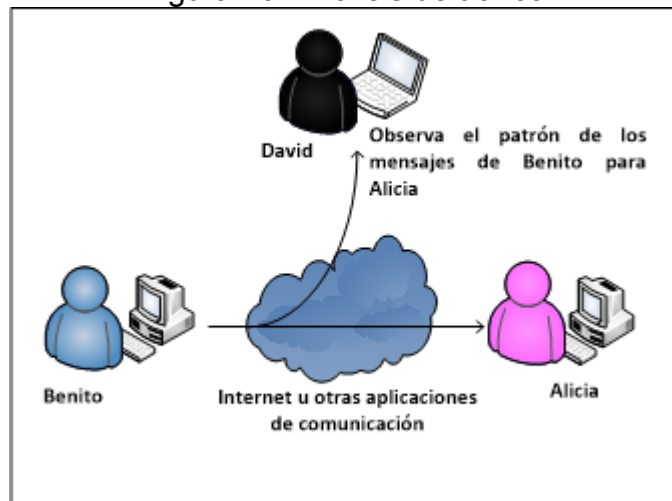
Fuente: (Stallings, Network Security Essentials: Applications And Standards, 2011)

### El análisis del tráfico:

Es más sutil. (Figura 17). Supongamos que hemos enmascarado los contenidos de los mensajes u otro tráfico de Información de forma que el oponente, incluso habiendo capturado el mensaje, no pueda extraer la información que contiene. La técnica común para enmascarar los contenidos es el cifrado. Incluso si tuviésemos protección mediante cifrado, un oponente podría.

Observar el patrón de los mensajes, determinar la localización y la identidad de los servidores que se comunican y descubrir la frecuencia y la longitud de los mensajes que se están intercambiando.

Figura 16. Análisis de tráfico.



Fuente: (Stallings, Network Security Essentials: Applications And Standards, 2011)

Los ataques pasivos son muy difíciles de detectar ya que no implican alteraciones en los datos. Normalmente, el mensaje se envía y recibe de una forma aparentemente normal y ni el emisor ni el receptor son conscientes de que una tercera persona ha leído los mensajes o ha observado el patrón del tráfico.

#### 2.14.3.2 Ataques activos:

Los ataques activos implican alguna modificación del flujo de datos o la creación de un flujo falso.

- **La suplantación:**

Se produce cuando una entidad finge ser otra. Un ataque de este tipo incluye habitualmente una de las otras formas de ataque activo.

- **La repetición:**

Implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado.

- **La modificación de mensajes:**

Significa que una parte del mensaje original es alterado. Estos ataques también implican la modificación de archivos o documentos, en caso de que el atacante logre obtener permisos de administrador puede implicar la pérdida total de la información.

- **La interrupción de servicio:**

Impide el uso o la gestión normal de las utilidades de comunicación.

Los ataques activos presentan las características opuestas a los pasivos, aunque los ataques pasivos son más difíciles de detectar existen medidas para prevenir su éxito. Sin embargo, es bastante difícil prevenir por completo los ataques activos. (Stallings, Network Security Essentials: Applications And Standards, 2011)

- **Ataques de intromisión:**

Suelen ser ataques internos o de alguien que consigue colarse a la red y navega por ella explorando archivos y documentos hasta que localiza información importante que puede ser de utilidad, normalmente utilizada para fines delictivos.

- **Ataques de interceptación:**

La información que queremos controlar o bien toda la información, es desviada de su destino original para ser analizada con detenimiento.

- **Ataques de espionaje en línea:**

Normalmente se da a través de redes inalámbricas, donde alguien no autorizado analiza el tráfico observando las comunicaciones. (Stallings, Network Security Essentials: Applications And Standards, 2011)

### **2.14.3.3 Ataques DoS**

Los ataques **DoS** o ataques de denegación de servicios tienen la finalidad de provocar que un servicio o recurso sea inaccesible para los usuarios legítimos.

Estos ataques pueden provocar:

- Parada de todos los servicios de una máquina.
- La máquina solo puede dar determinados servicios.
- La máquina no puede dar servicios a determinados usuarios.

#### 2.14.3.4 Métodos de ataque DoS

Los ataques **DoS** pueden llevar a cabo de diferentes formas y cubren infinidad de servicios, Existen tres tipos de ataques básicos.

- Consumo de recursos básicos.
- Destrucción o alteración de datos.
- Destrucción o alteración física de componentes de la red.

#### Ejemplos de ataques DoS:

- Consumo de ancho de banda.
  - **Smurf Attack**
  - **ICMP Ping Flood**
  - **Fraggle Attack**
- Ataques a la conectividad
  - **SYN Flood Attacks**

#### 2.14.3.5 Ataques DDoS

Un ataque de Denegación de Servicio Distribuido (**DDoS**) es un tipo especial de ataque **DoS** en el que se utilizan varios equipos para realizar un ataque coordinado contra una máquina.

- En este tipo de ataque se suelen utilizar máquinas denominadas Zombis que el atacante consigue controlar gracias a algún tipo de malware.
- Al conjunto de máquinas Zombis que controla un atacante se las suele denominar BotNets.

#### 2.14.4 Servidores espejo

Los servidores espejo son servidores de archivos que realizan la función de crear un respaldo o en inglés (**Back Up**) de otro servidor que se encuentre en la red de ahí su nombre ya que replican la información haciendo una copia fiel de la información de un servidor principal.

Por lo general cada servidor espejo se implementa para realizar los respaldos de un solo servidor cada determinado tiempo y de esta manera así procurar la seguridad de estos respaldos.

### 2.14.5 Honeypots

Un **Honeypot** es un sistema diseñado para analizar cómo los **hackers** emplean sus armas para intentar entrar en un sistema (analizan las vulnerabilidades) y alterar, copiar o destruir sus datos o la totalidad de éstos (por ejemplo borrando el disco duro del servidor). Por medio del aprendizaje de sus herramientas y métodos se puede, entonces, proteger mejor los sistemas. Pueden constar de diferentes aplicaciones, una de ellas sirve para capturar al intruso o aprender cómo actúan sin que ellos sepan que están siendo vigilados.

Los Honeypot's son en su forma más básica son servidores de información falsos, posicionados estratégicamente en una red de prueba, los cuales son alimentados con información falsa que es disfrazada como archivos de naturaleza confidencial.

Las funciones de los Honeypot's son:

- Desviar la atención del atacante de la red real del sistema, de manera que no se comprometan los recursos principales de información.
- Capturar nuevos virus o gusanos para su estudio posterior.
- Formar perfiles de atacantes y sus métodos de ataque preferidos de manera similar a la usada por una corporación policiaca para construir el archivo de un criminal con su modus operandi.
- Conocer nuevas vulnerabilidades y riesgos en los distintos sistemas operativos, entornos y programas las cuales aún no se encuentren debidamente documentadas.

### 2.14.6 Servidor Proxy

Un Servidor **Proxy** es un intermediario generalmente para los usuarios de una red. Por ejemplo, puede existir un Proxy para navegar por las páginas web, de forma que la computadora del usuario no tenga que estar conectada al sistema remoto, excepto a través del servidor Proxy. En el proceso de dar acceso Proxy a las páginas web, un servidor Proxy también puede acelerar el acceso a la web al almacenar las páginas web que se acceden, de forma que los demás usuarios se beneficien de contar con ellas de manera más rápida desde el servidor **Proxy** local; además puede ofrecer alguna protección de Firewall a la LAN. (Hallberg, 2014)

### 2.14.7 Software libre

Es el **Software** que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el Software. Es decir, el “Software libre” es una cuestión de libertad, no de precio.

Para entender el concepto, piense en “libre” como en “libre expresión”, no como en “barra libre”. En inglés a veces decimos “libre Software”, en lugar de “free Software”, para mostrar que no queremos decir que es gratuito.

Un programa es Software libre si los usuarios tienen las cuatro libertades esenciales:

- La libertad de ejecutar el programa como se desea, con cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.
- La libertad de redistribuir copias para ayudar a su prójimo (libertad 2).
- La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3). Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

Un programa es Software libre si otorga a los usuarios todas estas libertades de manera adecuada. De lo contrario no es libre. Existen diversos esquemas de distribución que no son libres, y si bien podemos distinguirlos en base a cuánto les falta para llegar a ser libres, nosotros los consideramos contrarios a la ética a todos por igual.

En cualquier circunstancia, estas libertades deben aplicarse a todo código que se planea usar o hacer que otros lo usen. Tomemos por ejemplo un programa A que automáticamente ejecuta un programa B para que realice alguna tarea. Si se tiene la intención de distribuir A tal cual, esto implica que los usuarios necesitarán B, de modo que es necesario considerar si tanto A como B son libres. No obstante, si se piensa modificar A para que no haga uso de B, solo A debe ser libre y se puede ignorar B.

**Software libre** no significa que no es comercial. Un programa libre debe estar disponible para el uso comercial, la programación comercial y la distribución comercial. La programación comercial de Software libre ya no es inusual; el Software libre comercial es muy importante. Puede haber pagado dinero para obtener copias de Software libre, o puede haber obtenido copias sin costo. Pero sin tener en cuenta cómo obtuvo sus copias, siempre tiene la libertad de copiar y modificar el Software, incluso de vender copias. (Free Software Foundation, 2015)

### **2.14.8 Software Privativo**

El término ha sido creado para designar al antónimo del concepto de Software libre, por lo cual en diversos sectores se le han asignado implicaciones políticas relativas al mismo. Para la Fundación para el Software Libre (**FSF**), este concepto se aplica a cualquier programa informático que no es libre o que sólo lo es parcialmente (semilibre), sea porque su uso, redistribución o modificación está prohibida, o sea porque requiere permiso expreso del titular del Software.

Por conclusión entendemos que el Software privativo es otro nombre para designar el Software que no es libre.

### 2.14.9 Software privado

El **Software privado** o **Software personalizado** es aquel que ha sido desarrollado para un usuario (generalmente una organización o una empresa). El usuario lo mantiene y utiliza, y no lo publica, ni como código fuente ni como binarios.

En particular, si el usuario tiene todos los derechos sobre el programa privado, el programa es libre. Sin embargo, si el usuario distribuye copias sin otorgar las cuatro libertades para las mismas, esas copias no son libres.

### 2.14.10 Filtrado web

Un filtro web, comúnmente conocido como "Software de control del contenido", es un Software diseñado para restringir los sitios web que un usuario puede visitar en su equipo. Estos filtros pueden funcionar con una lista blanca o una lista negra: la primera solo permite el acceso a sitios elegidos específicamente por quien configura el filtro; la última restringe el acceso a sitios no deseados según lo determinado por las normas instaladas en el filtro. Estos programas observan la **URL** del sitio deseado y realizan búsquedas en el contenido del sitio a fin de advertir las palabras clave restringidas; luego, deciden si bloquean o permiten la conexión. Los filtros se instalan como una extensión del navegador, como un programa independiente en el equipo o como parte de una solución completa de seguridad. Sin embargo, un **ISP** (Proveedor de Servicios de Internet) o una empresa también pueden instalarlos de forma paralela a la red, a fin de restringir el acceso a la web de varios usuarios al mismo tiempo. Algunos motores de búsqueda también incluyen filtros rudimentarios para eliminar páginas no deseadas en los resultados de búsqueda. (kaspersky Latam, 2016)

### 2.14.11 Software de filtrado

El software de filtrado web tiene dos grandes grupos de clientes: los padres que desean evitar que sus hijos accedan a contenido no deseado o inapropiado, y las empresas que desean evitar que los empleados accedan a sitios web que no se vinculan a sus trabajos. Los filtros web también se utilizan a menudo como herramienta de prevención de malware, ya que los filtros bloquean el acceso a los sitios que



comúnmente alojan malware, como aquellos relacionados con la pornografía o los juegos de azar. Los filtros más avanzados también pueden bloquear la información que se envía a través de Internet para evitar la divulgación de información confidencial.

Existen diferentes formas de software de filtrado web, como el uso de un proxy basado en Internet, el uso de sitios web en otros idiomas o la creación de una VPN para un servidor de proxy personal. Debido a estos espacios de bucle, los administradores de redes o padres preocupados deben asegurarse de que el filtro elegido sirva para más que solo bloquear o permitir ciertos sitios web. (kaspersky Latam, 2016)

### **CAPITULO III. METODOLOGÍA**

En este capítulo se plasma la metodología de una investigación científica, que fue empleada para el desarrollo de este documento, ya que cuenta con los elementos adecuados para su implementación tales como las técnicas de encuesta, entrevista, observación y resultados obtenidos.

Esta metodología consta del planteamiento del objeto de estudio, en el caso de este trabajo es “Implementación de un firewall restrictivo de bajo costo para soluciones PyME’s con control de ancho de banda y filtrado web; basado en software libre en el ITEC”.

La delimitación del estudio consiste en señalar desde un punto de vista objetivo cual será el inicio de la investigación y los contenidos a desarrollar para su culminación, de acuerdo al enfoque de esta tesis los temas que delimitarán este documento son: las redes de computadoras y los firewall’s; los contenidos que se englobarán dentro de estas demarcaciones son; los protocolos de red, estándares, dispositivos de red, amenazas, ataques, vulnerabilidades y seguridad.

En el capítulo uno de este trabajo se encuentra plasmado la formulación de la problemática, los objetivos, la enunciación de una hipótesis y en el capítulo dos se desarrolla el marco teórico.

La técnica utilizada para la recolección de datos en esta tesis es la encuesta, la cual se estructura mediante una serie de preguntas que permiten obtener información numérica; de esta manera se adquirieron datos de una muestra de usuarios de la red del ITEC, con los resultados conseguidos se procedió a su cuantificación y representación en forma gráfica para un análisis posterior, con el cual se comprueban las condiciones de servicio proporcionado en la red del ITEC y de esta manera realizar una propuesta para su mejora.

También mediante el uso de la técnica de la observación se realizó una inspección visual de las instalaciones del ITEC para posteriormente elaborar una tabla donde se especifican los dispositivos con los que se cuentan y tras realizar una medición se elaboró un plano detallado donde se muestran las distintas áreas de trabajo.

En el análisis de los datos, se realizó una serie de acciones para la compresión de la información recopilada, las tareas que se llevaron a cabo fueron la elaboración de tablas y gráficas conforme a los datos obtenidos, los cuales se pueden observar en el capítulo cuatro.

Como resultado final se presenta este documento, donde se muestran los resultados obtenidos de la investigación que llevan a la validación de la hipótesis, concluyendo que la implementación de un Firewall basado en Software libre en la red local del ITEC tiene como consecuencia una mejoría del servicio de internet dentro de sus instalaciones, así como el mejor desempeño de los equipos dentro de la red local y que se cuente con mayor seguridad en ella.

### 3.2 Requerimientos

Se tomó una muestra de 15 usuarios de un total de 180 alumnos que representan el 8.3% de los asistentes al **ITEC** para realizar una encuesta con la que se pueda conocer su opinión del servicio de internet con que cuentan, de esta manera también recopilar información para posteriormente efectuar un análisis de los datos obtenidos y mediante ellos poder determinar la calidad de la navegación en las instalaciones, con lo cual sea posible establecer si es necesaria la instalación de un **Firewall** que mejore la seguridad en la red, por lo cual se realizaron las siguientes preguntas:

1. ¿Cómo considera usted que es el servicio de internet actual?
2. ¿Considera que está seguro mientras navega en internet?
3. ¿Cuáles son las páginas de internet que más visita?
4. ¿Sabe lo que es y para qué sirve un Firewall?
5. ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?
6. ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?
7. ¿Conoce usted herramientas para mejorar la velocidad de navegación?  
Si, ¿Cuáles conoce?  
No
8. ¿Considera que se debe de controlar la velocidad del internet?
9. ¿Conoce usted herramientas para mejorar la seguridad en una red?
10. ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

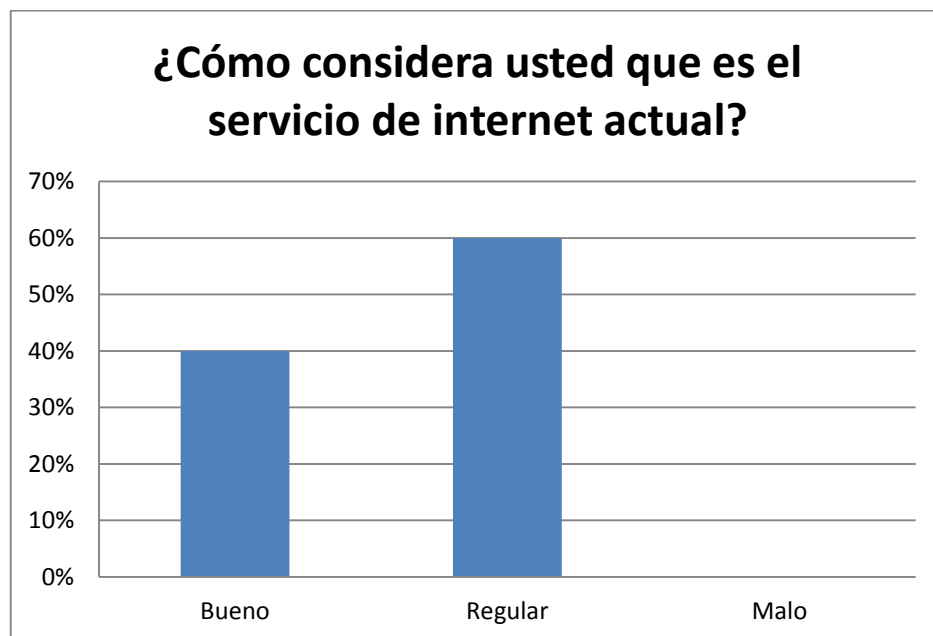
Véase los resultados en los anexos.

### 3.3 Análisis

Los resultados que se obtuvieron en las encuestas califican el servicio como bueno, sin embargo tomando en cuenta las observaciones hechas por los mismos usuarios es recomendable la instalación de un sistema de **Firewall** que realice las tareas de control del ancho de banda y filtrado web para el mejoramiento del servicio así como la seguridad en la navegación que se brinda en las instalaciones del **ITEC**. Ver anexo 1.

Una vez hecho el reconocimiento de las instalaciones se puede llegar a la conclusión de que además es necesario llevar a cabo la reestructuración del cableado de red con el que se cuenta en las instalaciones del **ITEC**, ya que dicho cableado se encuentra en un gran estado de deterioro, como lo son las cubiertas rotas, cableado expuesto, conectores rotos, etc.

A continuación, se muestra una de las gráficas mediante las cuales se realizaron los análisis. Para ver el resto de ellas véase el anexo 3.



### 3.3.1 Ubicación geográfica

Los Estados Unidos Mexicanos, están ubicados en la parte meridional de América del Norte, la ciudad capital es la Ciudad de México, está compuesta por 32 entidades federativas, el territorio nacional tiene una superficie de 1,964,375 km<sup>2</sup>, limita al norte con los Estados Unidos de América mientras que al sur tiene frontera con Guatemala y Belice. Ver la figura 18.

#### 3.3.1.1 Macro localización

Figura 17. Mapa de la república mexicana con división política.



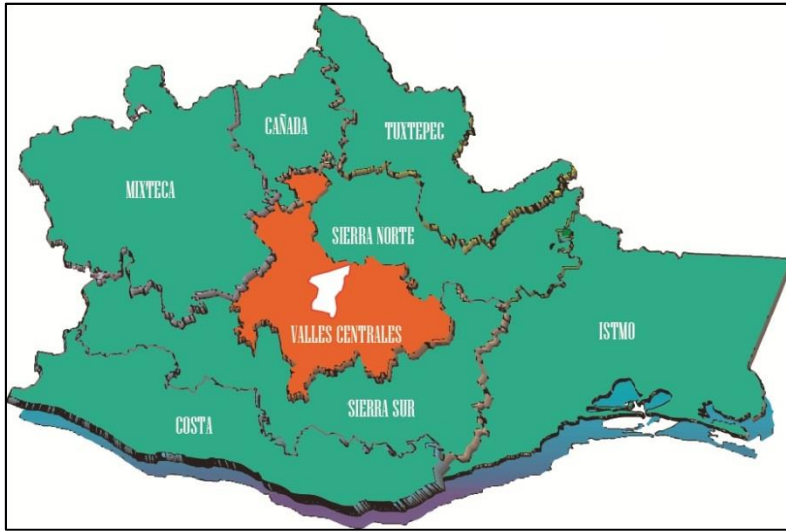
Fuente: [es.wikipedia.org/wiki/México](http://es.wikipedia.org/wiki/México)

#### 3.3.1.2 Micro localización

El Estado de Oaxaca se ubica al sur del país, colinda con el Estado de Guerrero al oeste, con Puebla al noroeste, Veracruz al norte, Chiapas al este y hacia el sur posee casi 600 km de costa en el océano pacífico. Por su extensión es el quinto estado más grande del país, está conformado por 8 regiones: Costa, Cañada, Istmo, Mixteca, Papaloapan, Sierra norte, Sierra sur y Valles Centrales, siendo en esta última donde se ubica la ciudad capital de Oaxaca de Juárez.

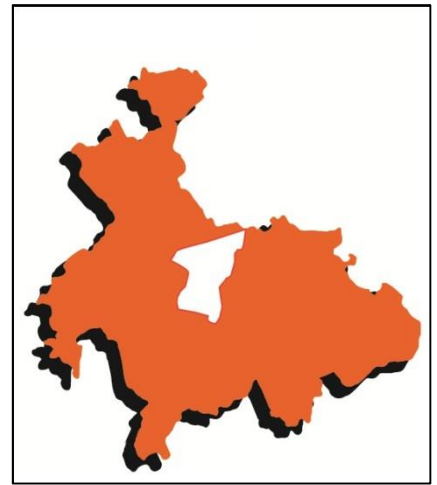
Las instalaciones del **ITEC** se encuentran ubicadas en la dirección de Bustamante # 312-A entre las calles Francisco Javier Mina y Aldama de la ciudad capital del Estado de Oaxaca, que corresponden a las coordenadas **17.057556 N, -96.725604 O**, a una altitud media de entre 1555 y 1557 metros sobre el nivel del mar. Ver la figura 19.

Figura 18. Mapa del Estado de Oaxaca por regiones.



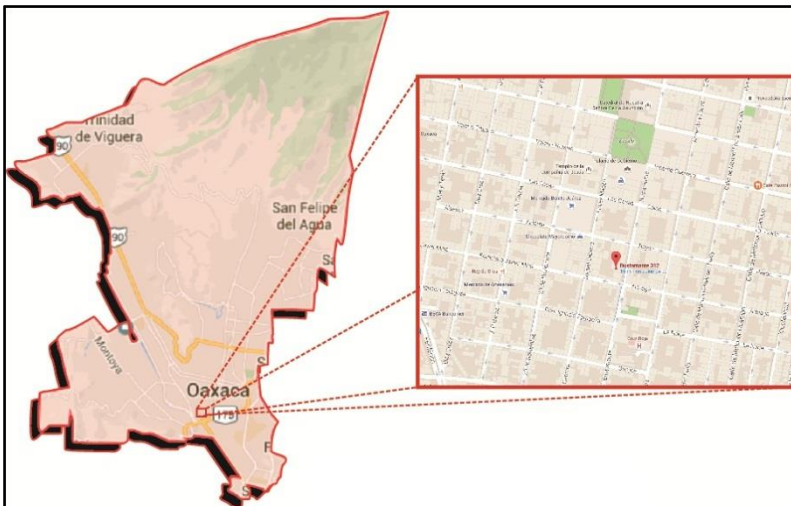
Fuente: Elaboración propia.

Figura 20. Región de Valles Centrales.



Fuente: Elaboración propia.

Figura 19. Ciudad de Oaxaca de Juárez.



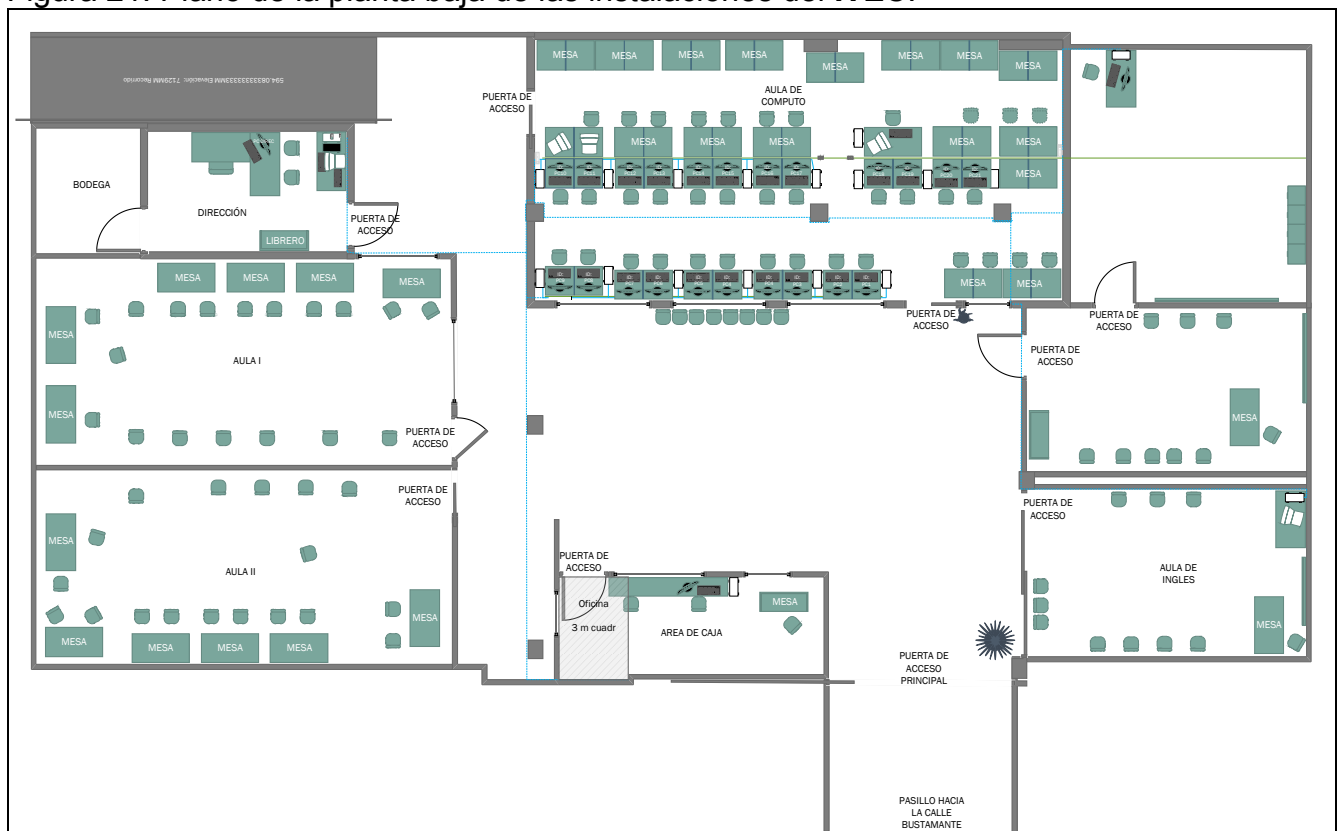
Fuente: Mapas de Google.

### 3.4 Desarrollo

La primera actividad que se llevó a cabo fue el reconocimiento de las instalaciones del ITEC que es donde se realizará la instalación del **Firewall**.

Las instalaciones de la institución están conformadas por 513m<sup>2</sup> de los cuales se encuentran 320m<sup>2</sup> asignados a las aulas, área administrativa, área de profesores, sala de cómputo, recepción y sala de espera, a continuación, se muestra el plano correspondiente a las instalaciones del ITEC.

Figura 21. Plano de la planta baja de las instalaciones del ITEC.



Fuente: Elaboración propia.



## Planta baja

La sala de cómputo tiene un área de 59m<sup>2</sup> en los cuales se encuentran distribuidas 21 computadoras también están instalados dos **Switch** de 16 puertos y uno de 24 puertos marca 3COM, estos se encuentran instalados en la pared mediante tornillos en las bases, hay 29 mesas y 37 sillas.

El cable de red utilizado en la instalación es par trenzado **UTP** categoría 5, los conectores son **RJ45** cat. 5e, y la norma utilizada es la **EIA/TIA 568 B**.

El espacio designado a los profesores tiene 72m<sup>2</sup> divididos en dos, en 26m<sup>2</sup> hay una mesa, una silla, una computadora con las mismas características con las que cuentan los equipos del centro de cómputo, una línea de lockers, este espacio también es utilizado para almacenar equipo y material sin utilizar, en los 20m<sup>2</sup> restantes hay una mesa, nueve sillas, un mueble para equipo de video y un pizarrón.

El aula de inglés mide 20m<sup>2</sup> donde hay una computadora con iguales características a los equipos del centro de cómputo, una mesa, doce sillas, un mueble para equipo de video y un pizarrón.

El área de recepción mide 11m<sup>2</sup> tiene una computadora, un escritorio con una silla, una repisa que se utiliza para almacenar material de trabajo, así como la caja donde se realizan los cobros de las colegiaturas.

La sala de espera tiene 52m<sup>2</sup> en donde hay 8 sillas y cuatro macetas con plantas decorativas.

El área administrativa o dirección cubre 10m<sup>2</sup> tiene un escritorio en "L", una mesa, dos computadoras, un teléfono, un modem, una impresora HP LaserJet P1102w, un **Switch**, un router inalámbrico, un regulador, un librero, una bodega contigua de 6m<sup>2</sup> donde se almacena equipo de papelería y limpieza.

La dirección es el espacio más adecuado para la instalación del **Firewall** debido a que es un área aislada.

A continuación, se muestra la tabla 6 con las características de los dispositivos que se encuentran en las instalaciones del **ITEC** así como su ubicación.

Tabla 5. Características de los dispositivos que se encuentran en el ITEC. 1 de 3

EQUIPO	CARACTERÍSTICAS	UBICACIÓN
PC1	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC2	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC3	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC4	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC5	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC6	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC7	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC8	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC9	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC10	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC11	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC12	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo

Tabla 6. Características de los dispositivos que se encuentran en el ITEC. 2 de 3

PC13	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC14	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC15	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC16	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC17	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC18	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC19	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC20	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
PC21	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audífonos	Sala de computo
Regulador	ISB sola basic Microvolt 2000	Dirección
Regulador	ISB sola basic Microvolt 2000	Dirección
Regulador	ISB sola basic Microvolt 2000	Dirección
PC_Docentes	Sistema operativo: Windows 7 SP1, Procesador: Intel (R) Atom (M), 1.66 GHz 1.67 GHz, Disco duro: 300 GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar	Sala de computo
Switch	Modelo 3Com OfficeConnect 16 Port 10/100M Switch with Auto MDIX 3C16792-US	Sala de cómputo
Switch	modelo 3Com OfficeConnect 16 Port 10/100M Switch with Auto MDIX 3C16792-US	Sala de cómputo
Switch	3Com de 24 Port, modelo 2016 N/S: 0400 / LMZQ6I0057815	Sala de cómputo
Switch	Marca Encore de 8 puertos	Dirección
Router Wi-Fi	Linksys WRT54G2 con 4 puertos Ethernet	Dirección
Modem	Technicolor modeloTG582n	Dirección

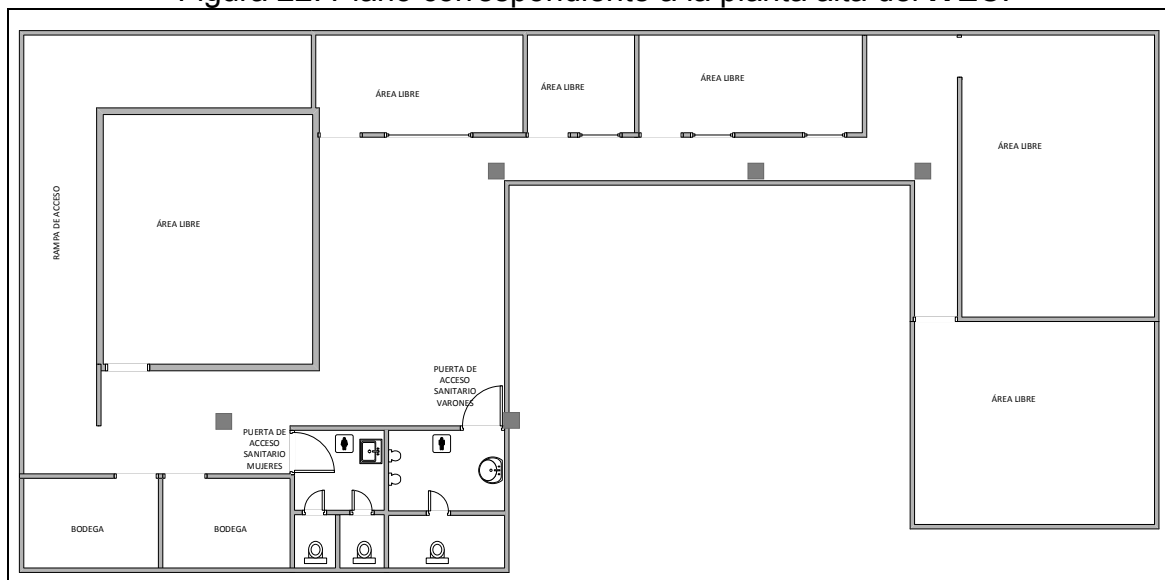
Tabla 7. Características de los dispositivos que se encuentran en el ITEC. 3 de 3

PC	Sistema operativo: IPCop v2.1.8 para i486, Procesador Intel(R) Celeron(R) a 1.70 GHz, Disco duro de 40GB, Memoria RAM de 512 MB, unidad de 3 1/2, unidad lectora de DVD, una tarjeta PCI adicional	Dirección
PC	Sistema operativo: Windows 7 SP1, Procesador: Intel (R) Atom(TM), 1.66 GHz 1.67 GHz, Disco duro: 300 GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar	Sala de docentes
PC	Sistema operativo: Windows 7 SP1, Procesador: Intel (R) Celeron(TM) 1.80 GHz 1.80 GHz, Disco duro: 160 GB, Memoria RAM: 2 GB, Pantalla LCD de 18", Teclado y mouse estándar	Recepción
PC	Sistema operativo: Windows XP SP3, Procesador: Intel(R) Atom(TM) CPU D410 1.66GHz 1.66GHz, RAM: 1GB, Disco duro: 120 GB	Dirección
PC	Sistema operativo: Windows 7 SP1, Procesador: Intel (R) Atom(TM), 1.66 GHz 1.67 GHz, Disco duro: 120 GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar	Dirección
Impresora laser	HP LaserJetP1102w	Dirección
Regulador	ISB sola basic Microvolt 2000	Dirección
PC	Sistema operativo: Windows XP SP1, Procesador: Intel (R) Celeron(R) 1.8 GHz, Disco duro: 40GB, Memoria RAM: 1 GB, Pantalla LCD de 15", Teclado y mouse estándar, Audifonos	Aula de inglés

Fuente: Elaboración propia

En la segunda planta se encuentran dos bodegas de 6m<sup>2</sup> cada una, los sanitarios que cubren 6m<sup>2</sup> de espacio para el de damas y 8m<sup>2</sup> para el de caballeros.

Figura 22. Plano correspondiente a la planta alta del ITEC.



Fuente: Elaboración propia.

Tras la observación de las instalaciones se determinó que el cableado de la red se encontraba en mal estado ya que tenía recubrimientos rotos y estaba a la vista de los usuarios, en la dirección existían cables excedentes que no tenían utilidad.

También tras el análisis de las necesidades en la red local se propone una herramienta que puede ser instalada en la misma para cubrir sus necesidades de seguridad y mejor aprovechamiento de la velocidad de navegación es un **Firewall**, pero actualmente estas soluciones enfocadas a empresas son muy costosas, lo cual representa una problemática más ya que el presupuesto de la institución no es el suficiente para poder costear una de estas alternativas, a continuación se muestra una tabla comparativa de algunos de los **Firewall's** en el mercado y una alternativa de bajo costo la cual puedes ser la adecuada para dar solución a sus necesidades:

Tabla 8. Comparativa de equipos firewall

TABLA COMPARATIVA DE EQUIPOS FIREWALL					
CATEGORÍA	WatchGuard XTM 25 & 1-Y Security Bundle WG025031 <sup>1</sup>	Firewall Watchguard Firebox T50 3yr Sec Bundle 45 Usuarios <sup>2</sup>	Dell SonicW ALL TZ Series <sup>3</sup>	Palo Alto Networks PA-3020 <sup>4</sup>	IPCop
Costo	\$ 14,059.15 MXN	\$33,392.00 MXN	\$1,398.25 US	\$ 35,870 US	\$1000.00 MXN
Manejo de VPN's	X	X	X	X	X
WI-FI					
DHCP	X	X	X	X	X
Filtrado WEB	X	X	X	X	X
Conexión WAN	X	X	X	X	X
Administración basada en WEB	X	X	X	X	X
Control de ancho de banda	X	X	X	X	X
Antivirus	X	X	X	X	
Antispam	X	X		X	X
VoIP	X	X	X	X	
Descifrado SSL y SSH	X	X	X	X	X

Las características son estandarizadas ya que se pueden configurar dependiendo si son admitidas en los equipos\*

Fuente: Elaboración propia.

En la tabla comparativa de los equipos **Firewall** se pueden apreciar características muy generales con las que cuentan cada uno, así como el costo de cada uno de ellos. Como se puede ver, la opción del **Firewall IPCop** es potente y versátil además de ser la más económica, por estas razones ha sido la elección a considerar.

## 3.5 Implementación

### 3.5.1 Restructuración del cableado

Para poder realizar la instalación del sistema de **firewall** primero se llevaron a cabo las tareas de reestructuración de la red cableada que se encontraba en la institución, ya que esta estaba en muy malas condiciones y no cumplía con las normas y estándares.

Las primeras actividades que realizaron fueron la identificación del cableado que se encontraba sin funcionamiento, también se identificaron las áreas donde dicho cable se encontraba desprotegido y a la vista de los usuarios, ya que este debería de estar dentro de canaletas y fuera de la apreciación de las personas, una vez realizada esta tarea se llevó a cabo la remoción del cableado que se encontraba en malas condiciones, roto o sin utilizar.

Se hizo la instalación de canaletas en las zonas de la dirección, pasillos y centro de cómputo para la correcta colocación del cable de red.

El cable que se utilizó para la reestructuración de la red fue par trenzado **UTP** de categoría 5e, así como conectores RJ45 cat. 5e

### 3.5.2 instalación y configuración

Para la instalación del sistema de **Firewall IPCop** en un equipo de cómputo es necesario cumplir con algunos requisitos.

- Procesador i486 o superior
- 2 tarjetas de red
- 512 Mb de memoria RAM o superior
- Disco duro de 4 Gb o superior
- Monitor y teclado (Solo para la instalación)
- Unidad de CD-ROM
- Un router (alámbrico o inalámbrico)
- **Switch** (Dependiendo de la cantidad de equipos en la red)

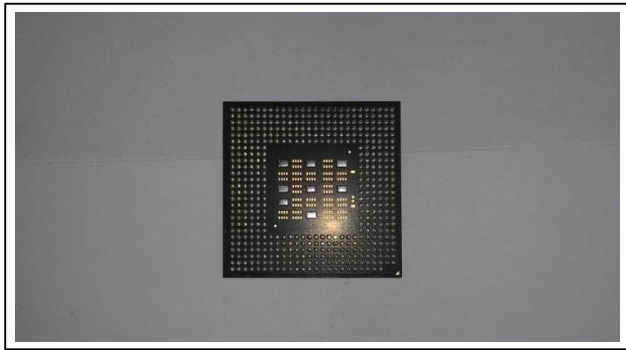


Figura 23. Procesador.



Figura 24. Tarjeta de red Ethernet.



Figura 25. Disco duro Samsung.



Figura 26. Tarjeta de memoria RAM Kingston.



Figura 27. Switch alámbrico 3COM.

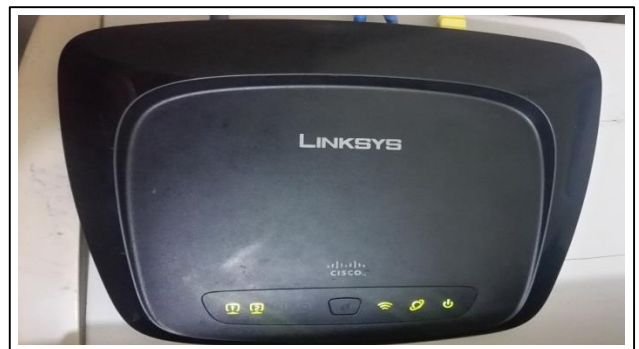


Figura 28. Router Linksys Inalámbrico/alámbrico.

Como sistema se utilizará el ya mencionado Software **IPCop**, el cual está basado en **Software libre**, al realizar la instalación tendremos un gran avance en la implementación de este **Firewall**.

Lo primero que hay que realizar es instalar las dos tarjetas en el equipo, para esto se utilizará la tarjeta de red integrada en el equipo y una tarjeta **PCI** que se instaló en una de las ranuras de expansión de la tarjeta madre del **PC** (Figura 29).



A continuación se tiene que realizar la obtención el sistema de **Firewall**, para ello hay que dirigirse a la página oficial de **IPCop** (Figura 30) mediante el siguiente link: <http://www.IPCop.org>

Actualmente la versión más estable se encuentra en la versión **2.1.8**.

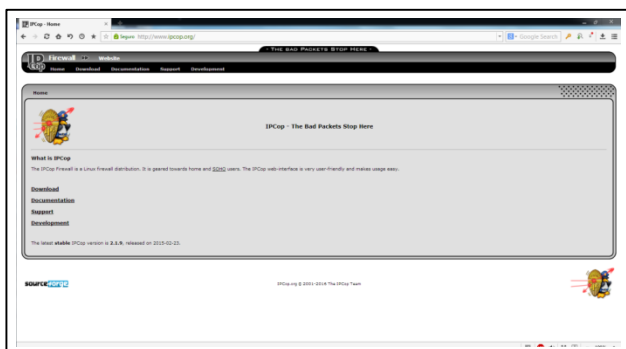


Figura 29. Página del sistema IPCop.



Figura 30. Tarjetas de red Instaladas.

La pantalla inicial del **Firewall IPCop**. Ver figura 31.

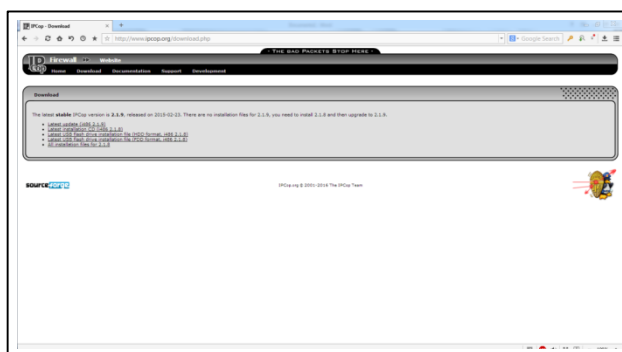


Figura 31. Sector descargas del sitio web de IPCop.

Ubicación donde se alojara la imagen **ISO** descargada. Ver figura 32.

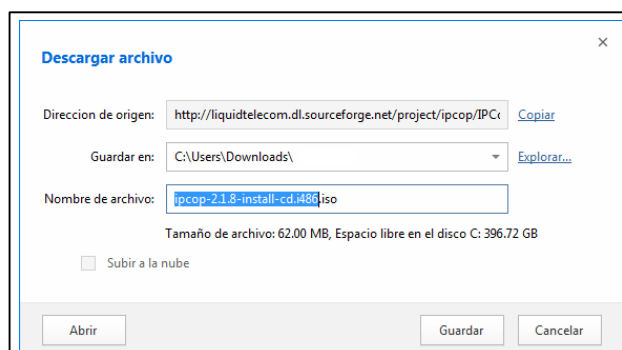


Figura 32. Pantalla de guardado de la descarga.

Una vez descargada la imagen **ISO** del **IPCop**, hay que grabarla en un **CD**. Ver figura 33.

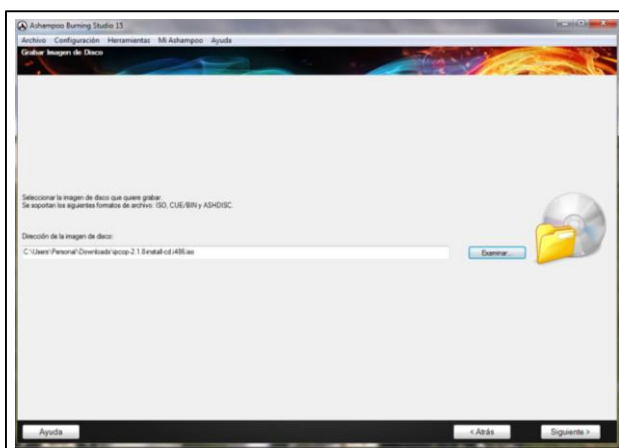


Figura 33. Pantalla de la aplicación para grabación.

Para iniciar con la instalación se deben conectar debidamente los componentes al gabinete y este a su vez a la corriente eléctrica, encenderlo, asegurarse de que el equipo inicie el sistema desde la unidad de **CD-ROM**, posteriormente se inserta el **CD**.

La primera pantalla que la computadora muestra es donde se aprecia el estado del equipo y sus componentes detectados. Ver figura 34.



Figura 34. Pantalla inicial de encendido.

Posteriormente la computadora muestra la pantalla donde espera una instrucción para continuar ya que se han detectado los archivos de arranque en la unidad de **CD-ROM**, las opciones son:

**Press RETURN to boot IPCop 2.1.8 default installation.**

**Press F1 for help and further information, TAB for boot target list.** Ver figura 35.

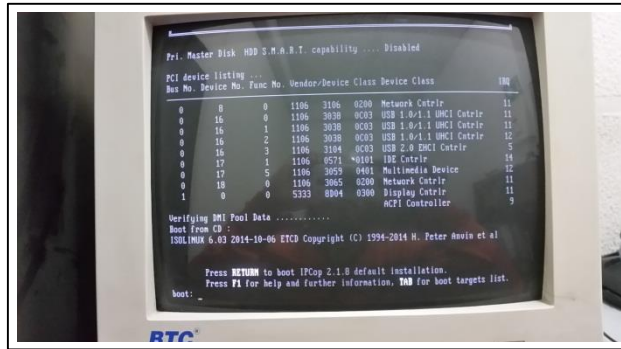


Figura 35. Selección de arranque.

Hay que presionar la tecla **ENTER** para realizar la primera opción.

La primera pantalla del sistema de instalación del **Firewall** muestra la opción para elegir el idioma de la instalación, por fines prácticos se seleccionará el idioma **Español Latino**, para el desplazamiento por el sistema de instalación se utilizan las teclas del cursor y la tecla **ENTER** o **ESPACIO** para confirmar las selecciones. Ver figura 36.

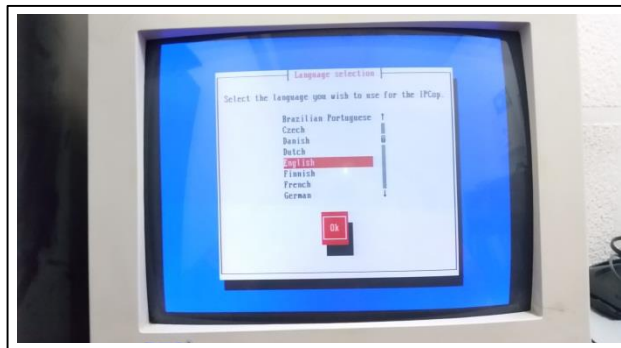


Figura 36. Selección de idioma de instalación.

Ahora se mostrará una pantalla de bienvenida. Ver figura 37.

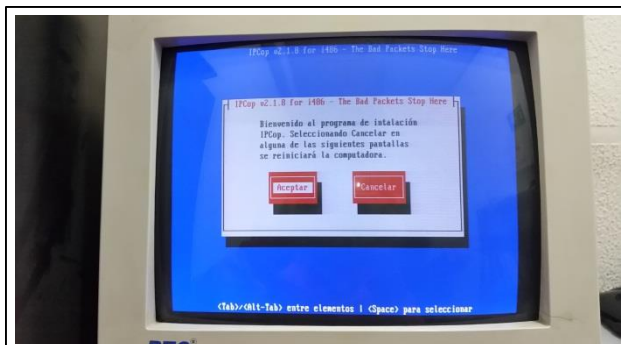


Figura 37. Pantalla de bienvenida a la instalación.

Para proseguir con la instalación hay que elegir la opción **aceptar** para continuar.

Posteriormente hay que seleccionar la configuración del teclado, para elegir español hay que desplazarse con las teclas del cursor hasta encontrar la opción **es** y seleccionarla. Ver figura 38.



Figura 38. Selección de idioma del teclado.

Posteriormente podrá ver la pantalla donde se tiene que elegir la zona horaria, de igual manera hay que desplazarse hasta encontrar la que seleccionará, en este caso será **America/Mexico\_City** y posteriormente hay que presionar el botón **aceptar**. Ver figura 39.



Figura 39. Selección de la zona horaria.

En la siguiente pantalla hay que configurar la fecha y la hora, al concluir se presiona el botón **aceptar**. Ver figura 40.



Figura 40. Configuración de la fecha y hora.

Ahora el sistema comenzará a buscar el origen de los ficheros para la instalación, y montará la unidad de **CD-ROM** para continuar con el proceso. Ver figura 41.



Figura 41. Pantalla de búsqueda de los ficheros.

Una vez que detecta el origen de los archivos que se van a instalar, el sistema realiza una búsqueda de la unidad.

Hay que seleccionar el Disco duro en el cual se llevará acabo la instalación de la lista que se muestra. Ver figura 42.



Figura 42. Selección del disco duro para la instalación.

Una vez seleccionado hay que presionar **aceptar** para continuar.

En este momento el sistema de instalación mostrará un mensaje para confirmar la instalación de los archivos ya que este paso dará formato al disco duro y se borrará toda la información. Ver figura 43.



Figura 43. Configuración o cancelación de la instalación.

Posteriormente hay que seleccionar la opción **Disco duro** para comenzar con el proceso de copia de archivos en el disco duro del equipo.

En la siguiente pantalla se pueden apreciar las tres opciones que nos ofrece en este paso el sistema de instalación. Ver figura 44.



Figura 44. Confirmación de la unidad seleccionada.

Se iniciará con el formateo, creación del sistema de archivos y el particionado del disco de forma automática, por ello el sistema muestra una pantalla con la leyenda **“Creando sistema de archivos. Esto puede tardar un tiempo”**. Ver figura 45.

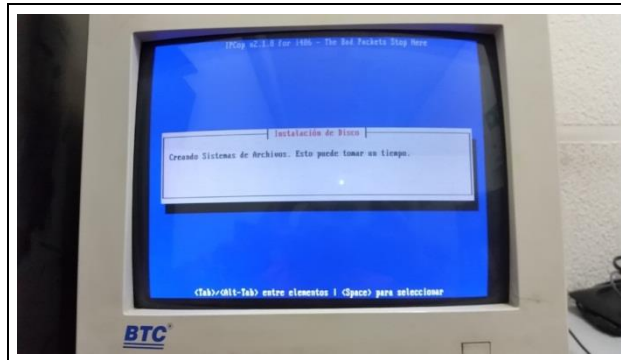


Figura 45. Creación del sistema de archivos.

El sistema instalará los archivos necesarios mostrando un recuadro con el avance de este proceso. Ver figura 46.

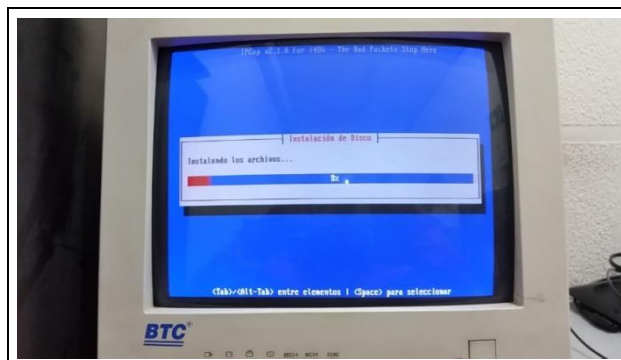


Figura 46. Avance del copiado de archivos.

Para concluir con la instalación y hacer las configuraciones básicas del **Firewall** hay esperar a que termine este proceso. Ver figura 47.



Figura 47. Conclusión del copiado de archivos.

Una vez terminada esta instalación el sistema muestra una pantalla en la cual se puede restaurar algún respaldo con el que se cuente del **Firewall**, debido a que no se tiene ninguna instalación del sistema de forma previa basta con seleccionar la opción de saltar y presionar **ENTER** o la barra espaciadora. Ver figura 48.



Figura 48. Pantalla de selección de Back up.

Posteriormente se muestra la pantalla en la que el sistema indica que se ha concluido con la instalación del **Firewall** y arroja la información que hay que tener en cuenta tal como la dirección **IP** mediante la cual se podrá tener acceso la administración del **Firewall** desde cualquier punto de la red, dicha **IP** puede ser cambiada posteriormente durante la configuración. Ver figura 49.





Figura 49. Pantalla final de la instalación.

Hay que seleccionar el cuadro que muestra la frase **¡Felicidades!** Para concluir con este proceso.

Por ahora se ha concluido la instalación del **Firewall**, a partir de este punto se describen los pasos para las configuraciones básicas del mismo. El primero de estos pasos para realizar la configuración del Firewall es asignar un nombre para el **Host** o el equipo, por defecto se asigna **IPCop**, este puede ser cambiado por el que se desee. Una vez asignado el nombre del **Host** hay que presionar el botón aceptar. Ver figura 50.



Figura 50. Asignación del nombre del host.

Ahora se tiene que asignar el nombre del dominio, por fines prácticos para esta instalación se ha dejado el nombre que está asignado por defecto que es **“localdomain”**, se selecciona la opción aceptar para proseguir. Ver figura 51.



Figura 51. Asignación del nombre del dominio.

El siguiente paso es muy importante ya que este sistema de **Firewall** diferencia las conexiones por color.

**RED -> INTERNET**

**GREEN ->RED LOCAL**

**BLUE -> WIRELESS**

**ORANGE -> DMZ**

Para esta configuración será de la siguiente manera:

**GREEN + RED**

Ya que se cuenta con una conexión mediante un modem por el cual se recibe el servicio de **internet**, el cual entrará a la interfaz **RED** del **Firewall**, una vez filtrado el tráfico por el **cortafuegos** se conectará a la interfaz **GREEN** un **router**, mediante el cual se proporcionará conexión mediante **wireless** y a su vez de forma cableada a los **Switch** que hay en la red local.

En esta versión la primera de las interfaces a configurar es la **RED** (roja).

Para la interfaz **RED**, se seleccionará la opción de **DHCP** para que el **modem** sea quien asigne la **IP** de esta tarjeta de forma automática ya que mediante esta es por la cual el trafico ingresara al **Firewall**; para hacer eso hay que desplazarse con las teclas del cursor hasta la opción **DHCP** presionar la tecla **ENTER** o la **barra espaciadora**,

posteriormente hay que presionar la opción “**aceptar**” para continuar con la configuración.

En la pantalla siguiente se realiza la elección para la configuración de esta interfaz, donde se aprecian las siguientes: **Módem analógico**, **Módem GSM/3G**, **ISDN**, **PPPoE**, **PPTP**, **Estático** y **DHCP**. Ver figura 52.



Figura 52. Selección de la función de la interfaz RED.

Ahora el sistema arrojará una pantalla donde se tiene que realizar la asignación de las tarjetas a las interfaces antes mencionadas, ya que se cuenta con dos tarjetas en esta pantalla solamente se ve esta cantidad de tarjetas.

En esta pantalla es donde se puede asignar la interfaz **RED** o **GREEN** a las tarjetas, se selecciona una de ellas con las teclas del cursor y solo se presiona la opción seleccionar para continuar. Ver figura 53.



Figura 53. Selección de tarjetas para las interfaces.

Se ha seleccionado la primera en la lista para asignar la interfaz **verde** o **GREEN**. Ver figura 54.

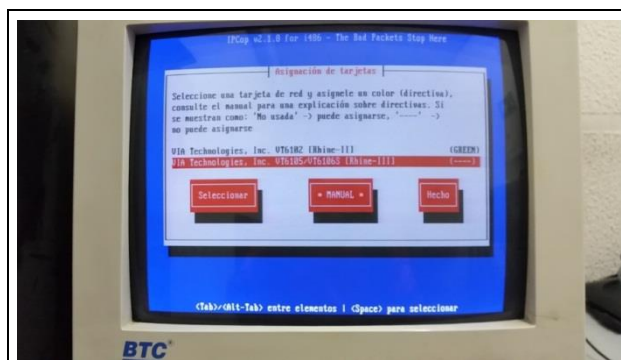


Figura 54. Selección de tarjeta para la interfaz GREEN.

Posteriormente se selecciona la segunda de las tarjetas para asignar la interfaz **roja** o **RED**. Ver figura 55.

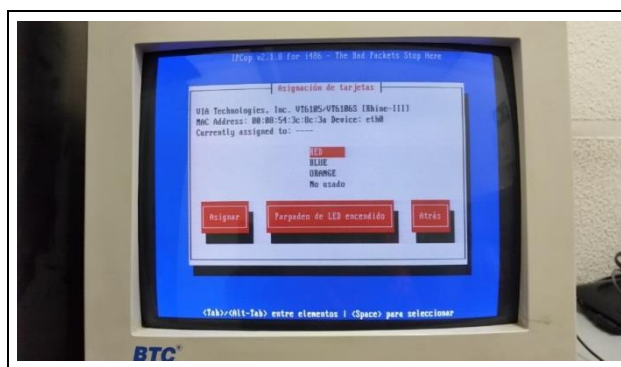


Figura 55. Asignación de la interfaz RED.

Una vez que se hayan designado las interfaces a las tarjetas, se selecciona la opción marcada con la palabra **Hecho**. Ver figura 56.



Figura 56. Confirmación de la selección de interfaces.

Una vez concluido este paso se comenzará con la configuración de la interfaz **GREEN** la cual inicia con la asignación de la **IP** mediante la cual se tendrá el flujo de datos filtrado.

Esta interfaz ya cuenta con una **IP** asignada por defecto, la cual es la que se mostró al finalizar con el proceso de la instalación dicha dirección es: **192.168.1.1** y se puede ver en la figura 57, en este paso se cambiará dicha **IP** para evitar confusiones posteriores y se asignará la **IP: 192.168.2.1** con la máscara de subred: **255.255.255.0** que se encuentra asignada por defecto, se selecciona la opción **aceptar** para proseguir con la configuración.

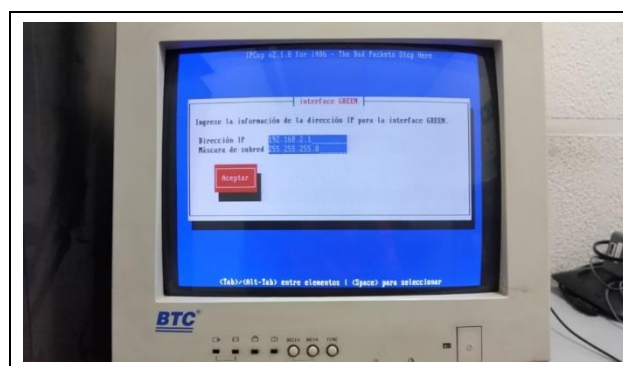


Figura 57. Configuración de la dirección IP.

A continuación se asigna el nombre de **host** para usar como cliente **DHCP** en la interfaz **RED**, para fines prácticos se quedará el que está por defecto y se seleccionará **aceptar** para continuar. Ver figura 58.



Figura 58. Asignación del nombre del host.

El siguiente paso es muy importante ya que si se realiza la configuración errónea podría haber problemas para tener comunicación con el **Firewall**.

El siguiente paso es la configuración del **DNS** y la puerta de enlace, por defecto el **Firewall IPCop** ya tiene configurada la opción de puerta de enlace como la dirección **192.168.1.254** la cual es la dirección **IP** reservada para el modem, pero no es mostrada en esta pantalla, si se realiza la instalación de este **Firewall** en una máquina virtual si es necesario cambiar esta configuración, así como la introducción de los **DNS** primario y secundario por lo cual en este paso se quedará en blanco y se seleccionará **aceptar**, si se selecciona la opción **saltar** la configuración terminará y habría que iniciar con la configuración de nueva cuenta. Ver figura 59.

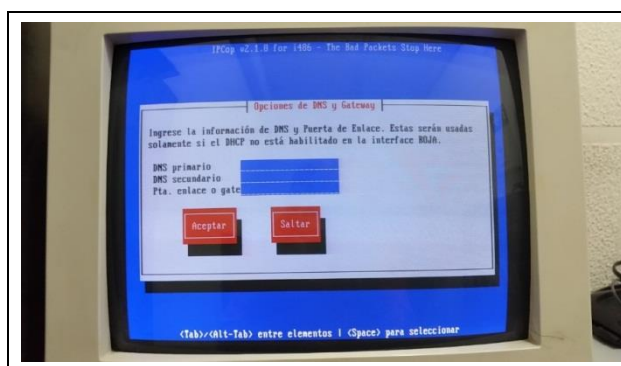


Figura 59. Pantalla de configuración de los DNS.

Se selecciona la opción **aceptar** para continuar con la configuración, posteriormente se presenta la configuración del **DHCP**, para ello hay que marcar la casilla de activado he introducir la dirección **IP** inicial, el rango de **IP's** si se desea ya que este paso reconoce la **IP** que se ha asignado y coloca como inicial la **IP** siguiente a la que se ha configurado anteriormente para la interfaz **GREEN**, Hay que seleccionar la opción **aceptar** para continuar. Ver figura 60.



Figura 60. Activación del DHCP y asignación de la IP.

A continuación se realizará la configuración de las contraseñas para los usuarios, la sesión del usuario “**root**” la cual se usará para realizar configuraciones posteriores en el **Firewall**, en el modo consola ya sea de forma física en el equipo o desde una conexión con otro equipo, una vez configurada la contraseña para este usuario hay que seleccionar la opción **aceptar**. Ver figura 61.



Figura 61. Asignación de la contraseña del usuario “root”.

Es momento de que asignar la contraseña para el usuario “**admin**” la cual servirá para iniciar sesión desde un navegador web en cualquier otro equipo de la red local. Ver figura 62.



Figura 62. Asignación de la contraseña del usuario “admin”.

Una vez configurada la contraseña para el usuario hay que seleccionar la opción **aceptar**.

Posteriormente se mostrará la pantalla donde se introducirá la contraseña para realizar respaldos. Ver figura 63.



Figura 63. Asignación de contraseña para respaldos.

Al finalizar el sistema mostrará otra pantalla más donde presenta la leyenda **¡Felicidades!** Para indicar que se ha terminado con esta parte del proceso, para proseguir hay que seleccionar la opción **aceptar**. Ver figura 64.





Figura 64. Pantalla final de la instalación.

Al terminar se puede apreciar el proceso de reinicio del sistema, el cual da inicio con la detención de los procesos. Ver figura 65.

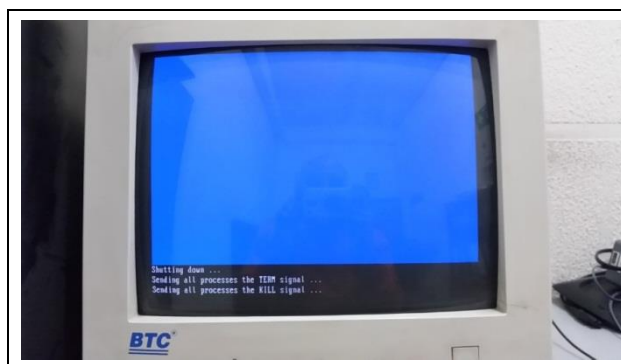


Figura 65. Reinicio del sistema.

Al reiniciar el equipo del Firewall muestra cinco opciones: **IPCop**, **IPCop (ACPI disabled)**, **IPCop (verbose booting)**, **Memory Test**, **Rescue** de las cuales hay que seleccionar la primera en la lista “**IPCop**” o esperar a que el conteo termine para iniciar de forma automática. Ver figura 66.



Figura 66. Pantalla de inicio del Firewall.

Una vez que el sistema inicia; el equipo mostrará el desarrollo del proceso de arranque del **Firewall** en el cual se puede apreciar si existe algún problema, de ser este el caso se podría apreciar una leyenda de **ERROR** en color **rojo**, si ha iniciado de forma correcta cada uno de los procesos y servicios del sistema mostrará en cada uno de ellos la palabra **DONE** de color **verde**.

Desarrollo del proceso de arranque del sistema de Firewall. Ver Imágenes 67 y 68.



Figura 67. Inicio de procesos del Firewall.



Figura 68. Sistema Firewall iniciado.

Ya que ha iniciado el **Firewall** se aprecia la opción de realizar el **login** a este, para ello hay que teclear el usuario **“root”** (sin las comillas), presionar **Enter** y posteriormente introducir la contraseña para este usuario y pulsar de nuevo **Enter**.

Pantalla donde el usuario puede iniciar sesión mediante la cuenta **“root”**. Ver figura 69.



Figura 69. Solicitud de inicio de sesión.

Siendo la siguiente pantalla la primera que indica que se ha iniciado sesión en el **Firewall**, a partir de este punto se pueden realizar las configuraciones desde línea de comandos, o desde el navegador de internet de alguna de las computadoras en la red local. Ver figura 70.



Figura 70. Inicio de sesión con el usuario “root”.

Para tener acceso al **Firewall** desde el navegador de alguna computadora de la red local, se debe conectar la tarjeta de red asignada a la interfaz **RED** al **modem** y la tarjeta de la interfaz **GREEN** al **router**, el cual a su vez estará conectado a un **Switch** que servirá para conectar las computadoras a la red con el tráfico filtrado.

Ahora se mostrará el proceso de configuración del **Firewall**, debido a que solo se requiere realizar el control del ancho de banda y el filtrado web, este documento se enfocará solamente en estos dos aspectos.

A continuación se explicarán los pasos para llevar a cabo la instalación de complementos que nos ayudarán a cumplir con este objetivo, se mostrará la forma más sencilla cumplir estos cometidos que es por medio de aplicaciones de escritorio para el entorno del sistema operativo **Windows**, con la finalidad de que este documento sirva como ayuda para las personas que no cuentan con conocimientos avanzados de cómputo, se utilizarán las siguientes:

Figura 71. Programa **WinSCP**.



Fuente: [winscp.net](http://winscp.net)

**WinSCP** permite tener acceso seguro al **Firewall** mediante una conexión **SSH** (Secure Shell), para esto también hay que realizar la habilitación de este servicio en el equipo donde está instalado el cortafuegos.

Figura 72. Programa **PUTTY**.



Fuente: [putty.org/](http://putty.org/)

**PUTTY**, proporciona una consola de comandos de **Linux** con la que se puede realizar la ejecución de instrucciones en el cortafuego desde el entorno de **Windows** sin necesidad de tener acceso al equipo de forma física.

La herramienta que se instalará primero en el equipo con **Windows** es **WinSCP** para ello hay que ejecutar el archivo **EXE** de la aplicación y seguir los pasos del instalador. En el caso de instalarlo en **Windows 7** o posterior, hay que dar autorización para que el programa realice cambios en el equipo. Ver figura 73.

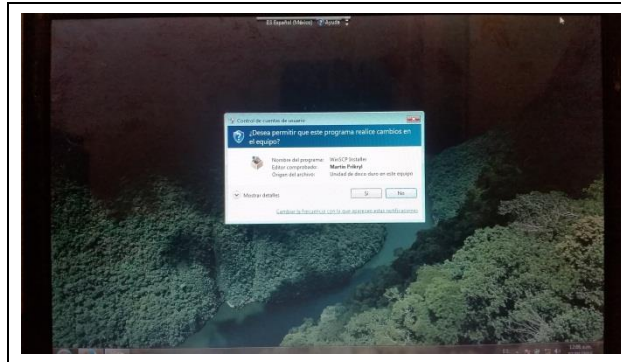


Figura 73. Autorización para el programa WinSCP.

Tras otorgar permisos aparecerá la pantalla inicial del instalador en la cual se tiene que hacer la selección del idioma con el que se va a realizar la instalación, en este caso se encuentra seleccionado por defecto el español, para proseguir con la instalación basta con hacer clic sobre el botón **aceptar**. Ver figura 74.

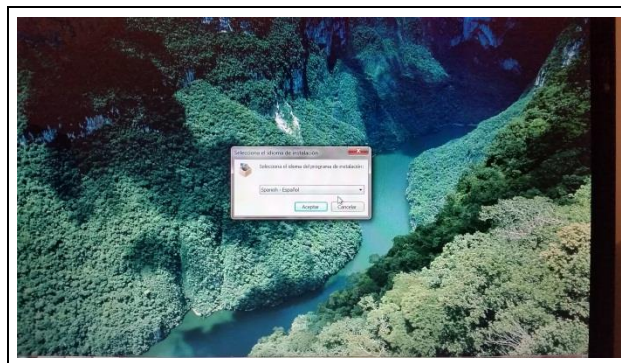


Figura 74. Instalador del programa WinSCP.

Después aparecerá una pantalla de bienvenida al asistente de la instalación, para continuar con el proceso de instalación hay que hacer clic en el botón **siguiente**. Ver figura 75.

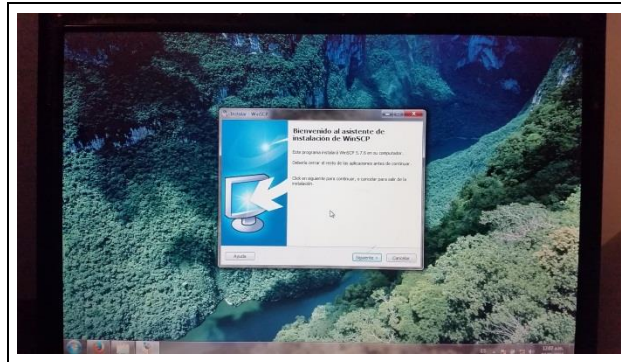


Figura 75. Bienvenida al asistente de instalación.

La pantalla siguiente corresponde al consentimiento de la licencia de esta aplicación, se puede realizar la lectura del contenido, pero hay que destacar que esta aplicación es de uso libre ya que se encuentra bajo una **licencia pública GNU**, para proseguir solo hay que hacer clic en el botón **aceptar**. Ver figura 76.

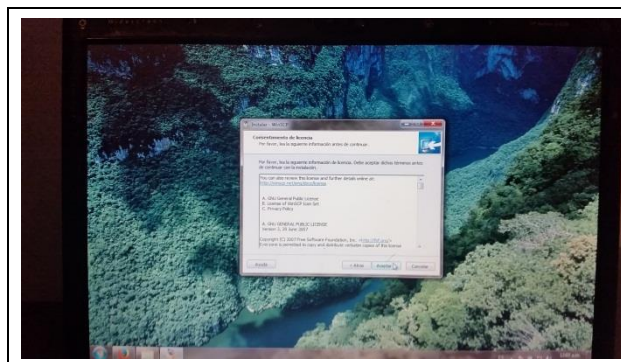


Figura 76. Pantalla de aceptación de licencias.

El siguiente paso es elegir el tipo de la instalación que sea más conveniente, se mostrarán dos opciones **Típica** y **Personalizada**, hay que elegir la opción **Típica** ya que para las acciones que se van a realizar no es necesario hacer alguna otra configuración especial. Ver figura 77.

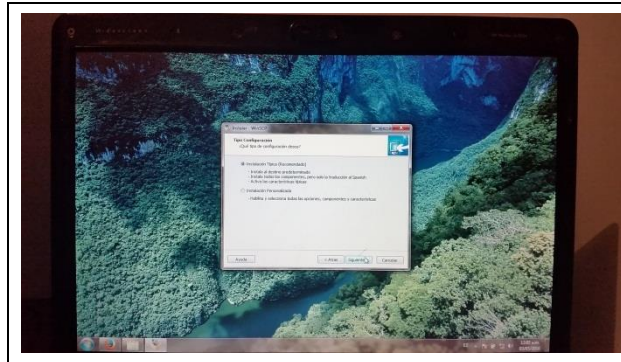


Figura 77. Selección del tipo de instalación.

En el siguiente paso se mostrará una pantalla donde se puede elegir el tipo de interfaz con la cual se desee trabajar, la opción **Commander** mostrará una pantalla con dos paneles, un panel izquierdo para los archivos locales, el panel derecho para los directorios del equipo remoto, y la interfaz **Explorador** en la cual solo se mostrará una ventana con los directorios remotos, en este caso hay que elegir la interfaz **Commander** debido a que es más amigable con los usuarios e intuitiva. Ver figura 78.

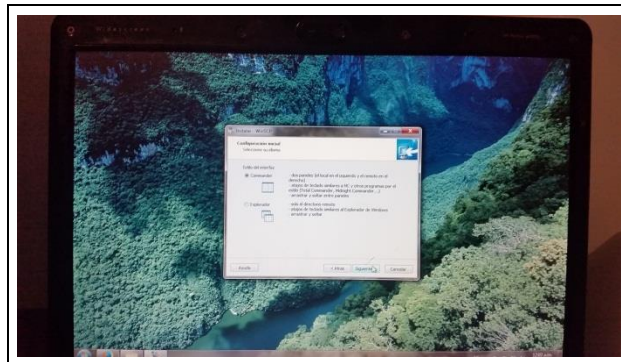


Figura 78. Selección de la interfaz para la aplicación.

Tras dar clic en el botón siguiente aparecerá otra pantalla con un informe de las configuraciones de la instalación, solamente basta con hacer clic en el botón **instalar** para que se inicie esta fase. Ver figura 79.

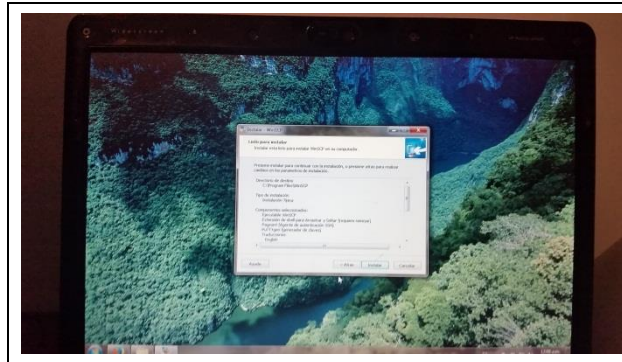


Figura 79. Informe de las configuraciones.

En este paso se mostrará el progreso de la instalación. Ver figura 80.

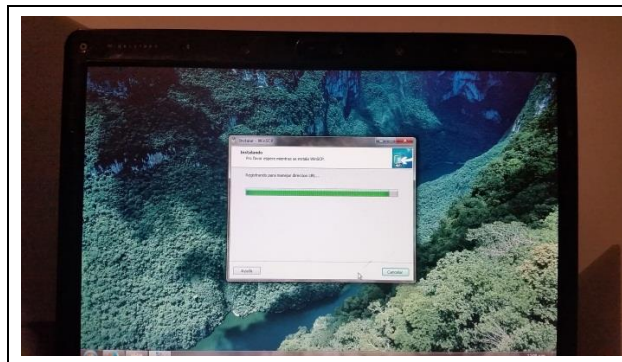


Figura 80. Barra de estado de la instalación.

Al concluir la instalación aparecerá la pantalla final donde se aprecia que se ha completado la instalación del **WinSCP** y presentará la opción de realizar una donación, también se señalan dos opciones marcadas las cuales son **Iniciar WinSCP** y **Abrir página de inicio**, hay que desmarcar la segunda y hacer clic en el botón **Finalizar**. Ver figura 81.

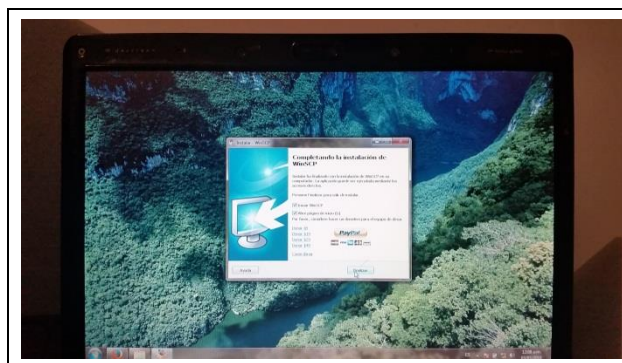


Figura 81. Final de la instalación del WinSCP.



Al ejecutar la aplicación de **WinSCP** se presenta la pantalla principal, en esta se puede apreciar una interfaz sencilla y muy intuitiva, también se muestra los tipos de conexiones que se pueden realizar en este caso es **SFTP (SSH File Transfer Protocol)**, una caja de texto donde se hay que introducir la **IP** o el nombre del servidor, el usuario, la contraseña y el puerto por el cual se llevará a cabo la comunicación cada vez que sea necesario. Ver figura 82.

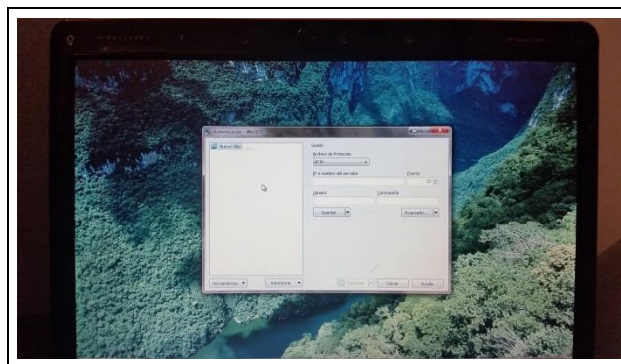


Figura 82. Pantalla inicial del programa WinSCP.

Ahora hay que activar la conexión por **SSH** en el **Firewall**, para ello tienen que acceder al cortafuegos mediante el navegador web del equipo con **Windows**.

La siguiente acción a realizar es abrir el navegador web con el cual se realizará el acceso, introducir la **IP** que corresponde a la interfaz **GREEN** (verde) en la barra de direcciones, posteriormente será solicitado el usuario y la contraseña, se deberá de ingresar el usuario **admin** y el **Password** asignado durante la instalación. Ver figura 83.

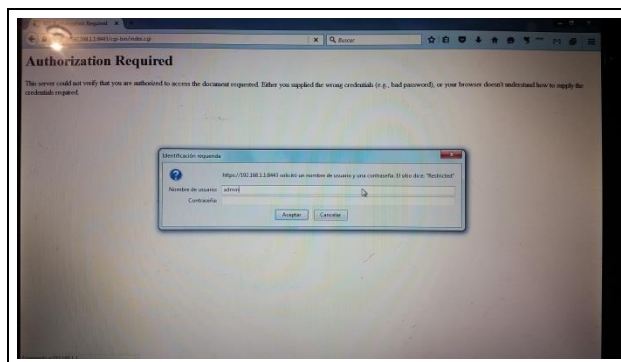


Figura 83. Inicio de sesión con usuario admin.

Ahora se mostrará la pantalla de inicio del **Firewall** donde se puede ver el estado del mismo y una barra de menús, de instalar algún complemento se mostrará dentro de esa barra, de acuerdo a las necesidades que se tengan se podrán configurar las características que se deseen. Ver figura 84.

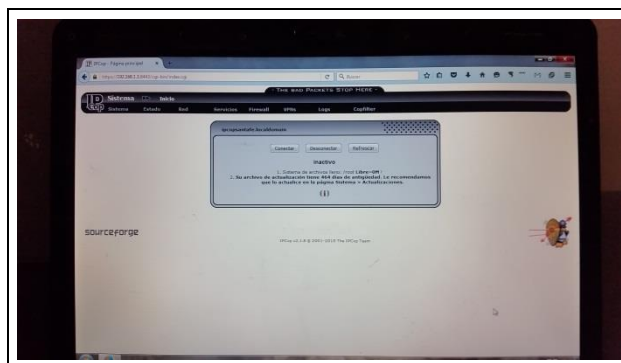


Figura 84. Pantalla principal del Firewall.

La configuración que se tiene que realizar en este momento es la activación del acceso **SSH**, para esto hay que dirigirse al menú "**Sistema/ Acceso SSH**". Ver figura 85.

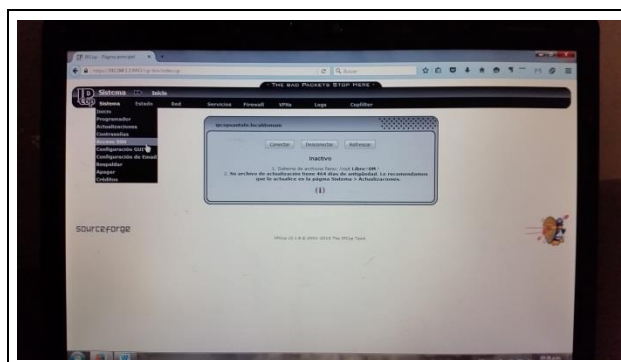


Figura 85. Acceso SSH en el menú Sistema.

Sucesivo a esto se puede ver la pantalla propia del submenú **Acceso SSH** donde se realiza la activación de este servicio, haciendo clic en la casilla de **activación** y así permitir conexiones remotas. Ver figura 86.

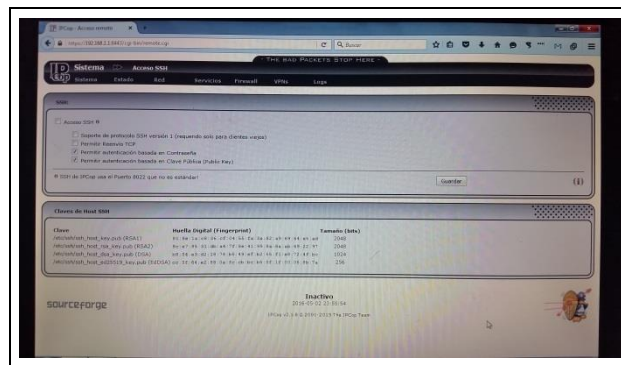


Figura 86. Pantalla principal del menú Acceso SSH.

A continuación se muestra la casilla de **Acceso SSH** activada una vez hecho esto hay que dirigirse a la parte inferior de la pantalla para hacer clic en el botón **guardar** y de esta manera poder realizar las conexiones con este método. Ver figura 87.

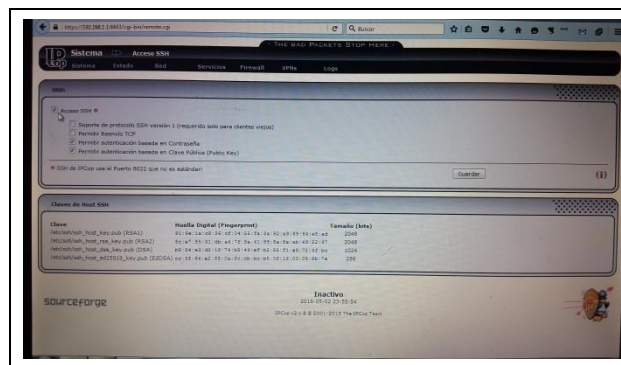


Figura 87. Activación del servicio SSH.

Ahora ya se puede realizar la instalación de **Addon's** (agregados) o complementos mediante la aplicación **WinSCP**, en este momento se muestra la pantalla de la aplicación en la cual hay que introducir los datos de acceso, posteriormente se tiene que hacer clic en el botón **Conectar**. Ver figura 88.

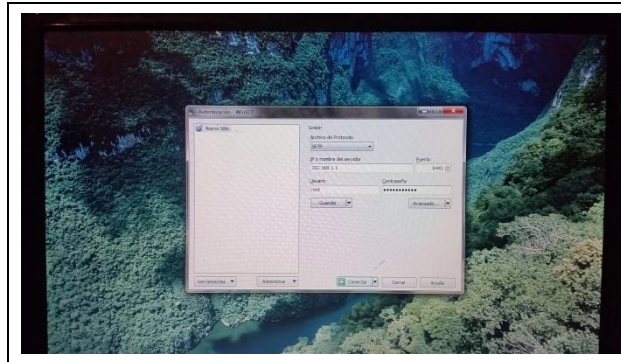


Figura 88. WinSCP con parámetros para conexión.

Después el sistema muestra la pantalla donde se puede ver el proceso de la conexión. Ver figura 89.

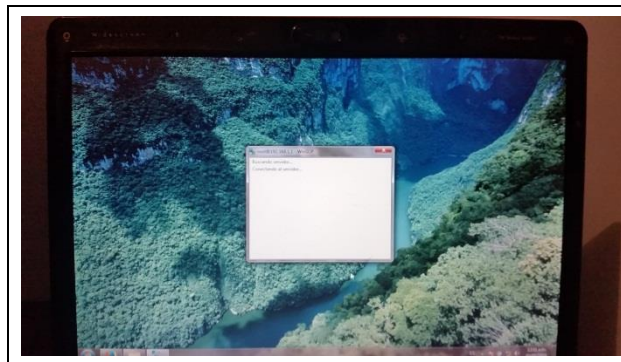


Figura 89. Inicio de la conexión con el WinSCP.

Al terminar esto se mostrará la pantalla de la interfaz que se eligió durante el proceso de instalación de **WinSCP** donde se puede navegar en los archivos locales en el panel izquierdo y en los directorios del **Firewall** en el panel derecho. Ver figura 90.

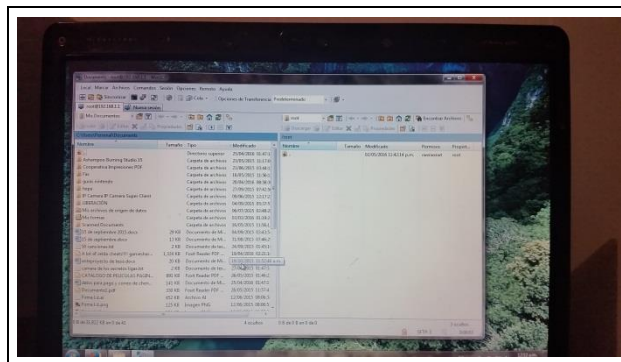


Figura 90. Pantalla principal del programa WinSCP.

Enseguida se puede realizar la instalación de complementos con esta herramienta, mediante el **WinSCP** se pueden copiar los complementos desde el **PC** al **Firewall**, aquí se ejemplificará la instalación de uno de estos complementos.

El complemento que se instalará es el **copfilter** en su versión **2.1.93beta1**, que es un módulo donde se pueden configurar más opciones en el **Firewall** como **filtrado POP3**, **filtrado SMTP**, **filtrado HAVP**, **filtrado C-ICAP**, **filtrado FTP**, **Antispam**, **Antivirus**, etc., esta instalación es para ejemplificar el modo en el cual se pueden agregar complementos.

En el panel izquierdo hay que ubicar el **copfilter** en la computadora, el cual se transferirá al **Firewall** arrastrándolo con el ratón al panel derecho en el directorio **“root”**. Ver figura 91.

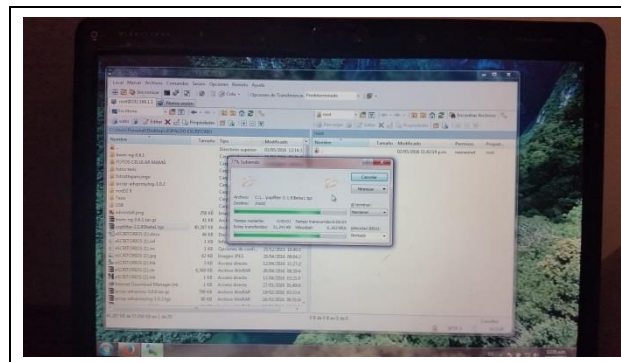


Figura 91. Copiado de los ficheros al Firewall.

En la siguiente pantalla se puede apreciar que el archivo se encuentra en el **Firewall**, con esto se puede realizar la extracción de este complemento y posteriormente la instalación del mismo. Ver figura 92.

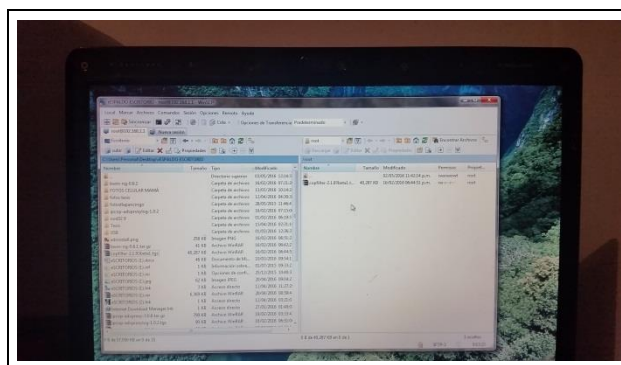


Figura 92. Directorio de los archivos en el firewall.

Para extraer este archivo sin tener que hacerlo desde el equipo donde se encuentra instalado el **Firewall** pueden hacerlo desde una conexión **SSH**, en la aplicación de **WinSCP** hay que hacer clic derecho sobre el archivo comprimido, en el menú contextual se tiene que elegir la opción de “**Comandos propios**” y después en la opción “**UnTar/GZip**”, para posteriormente elegir la ruta donde se extraerá, en este caso se quedará como está para que se extraiga en el mismo directorio. Ver figura 93.

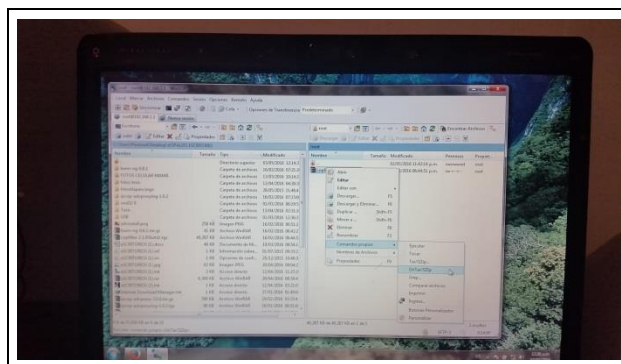


Figura 93. Extracción de archivos firewall con WinSCP.

Nota: La extracción de los archivos también se puede realizar mediante comandos de **Linux** pero esto se explicara de forma posterior.

En la siguiente pantalla se puede observar que el archivo ya se encuentra descomprimido y muestra el directorio “**copfilter-2.1.93beta1**” en el cual se encuentran los archivos para su instalación. Ver figura 94.

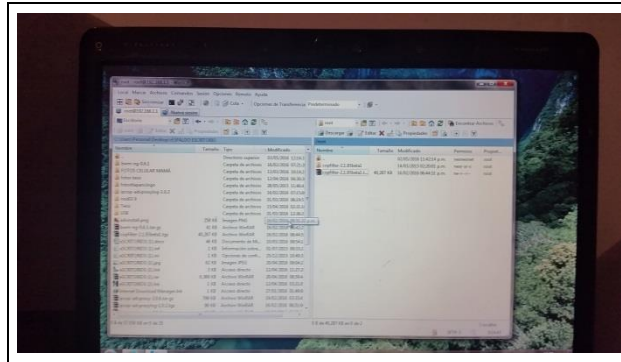


Figura 94. Ficheros descomprimidos en Firewall.

Para la instalación de este complemento es necesaria la utilización de la línea de comandos de **Linux** pero no es necesario que se dirijan al **Firewall** de forma física, es en este momento en el que se explicará la utilización de la herramienta **PUTTY** con la cual se puede realizar la instalación del **copfilter**.

La versión de **PUTTY** que se usará es una versión portable, al ejecutar la aplicación se muestra la pantalla inicial de dicha herramienta, en la cual se pueden apreciar parámetros similares a los de **WinSCP** donde hay que colocar la **IP** o nombre del **Host**, el puerto por el cual se realizará la conexión, en este caso se utilizará el puerto **8022**, hay que marcar la casilla de tipo de conexión **SSH** para posteriormente hacer clic en el botón “**Open**” y realizar la conexión. Ver figura 95.

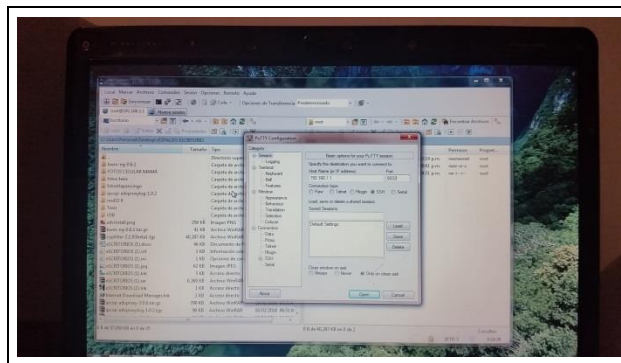


Figura 95. Pantalla principal del programa PUTTY.

Una vez realizada la conexión se mostrará la consola de comandos en la cual hay que entrar con los datos del usuario “**root**” tal y como si se trabajara en el **Firewall** de forma física. Ver figura 96.

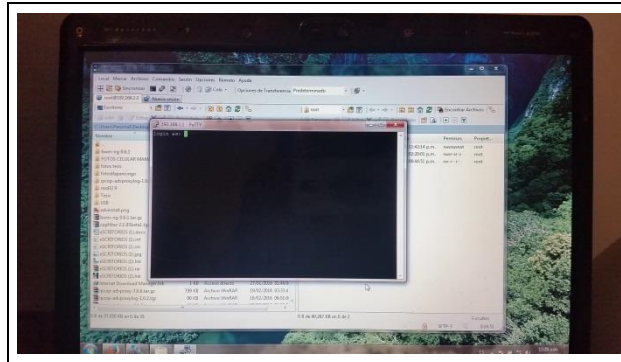


Figura 96. Pantalla de la consola de comandos.

En esta consola de comandos hay que introducir el usuario “**root**” al igual que su clave, una vez hecho esto se mostrará en la pantalla que se ha iniciado sesión, ahora para ver archivos que se encuentran en este directorio se utilizara el comando:

**# ls**

Este comando de **Linux** es el equivalente a **# dir** de **MS-DoS**, al ejecutarlo se podrá apreciar que se encuentran dos elementos, uno es el archivo comprimido **copfilter-2.1.93beta1.tgz** con letras blancas y el otro elemento es **copfilter-2.1.93beta1** con letras azules que indica que es una carpeta. Ver figura 97.

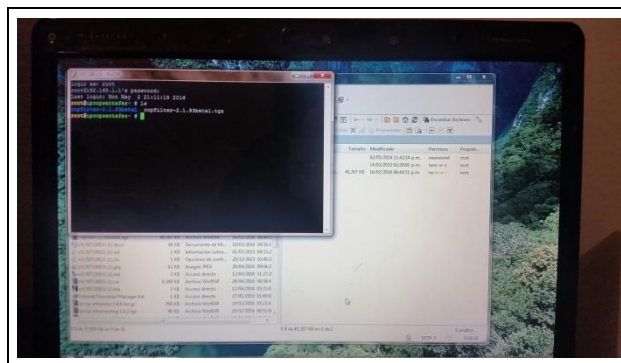


Figura 97. Utilización del comando # ls en PUTTY.

Para poder entrar en la carpeta se ejecuta la siguiente línea:

**# cd copfilter-2.1.93beta1** Ver figura 98.



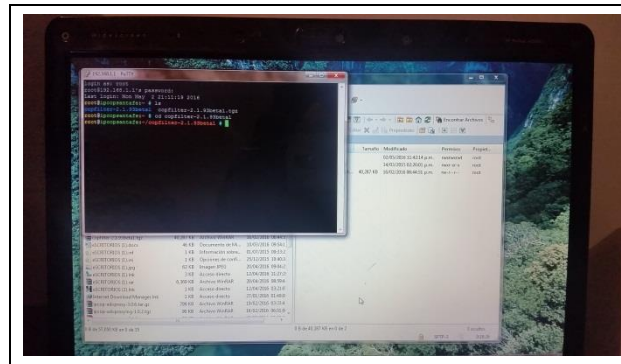


Figura 98. Utilización del comando # cd en PUTTY.

Una vez más hay que escribir el comando # ls para ver los archivos que se encuentran en este directorio, hecho esto se puede apreciar que dentro de esta carpeta se encuentran dos archivos uno llamado **copfilter-2.1.93beta1\_install.xz** y otro llamado **install**, se puede deducir este último es el archivo que se utilizará para la instalación del **copfilter**. Ver figura 99.

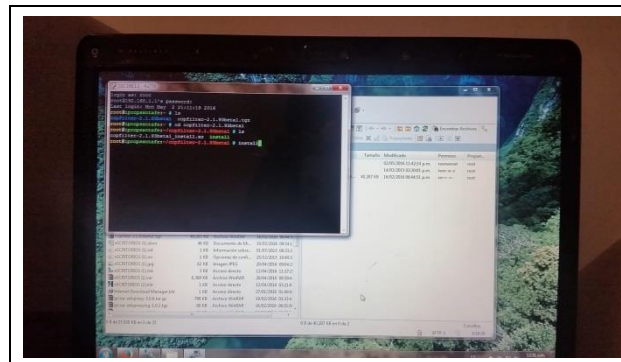


Figura 99. Instalación del copfilter desde PUTTY.

Ahora para ejecutar la instalación hay que hacerlo mediante la ejecución del siguiente comando:

**# ./install**

En la siguiente pantalla se puede apreciar que al ejecutar esta línea comenzara con el proceso de instalación de este complemento. Ver figura 100.

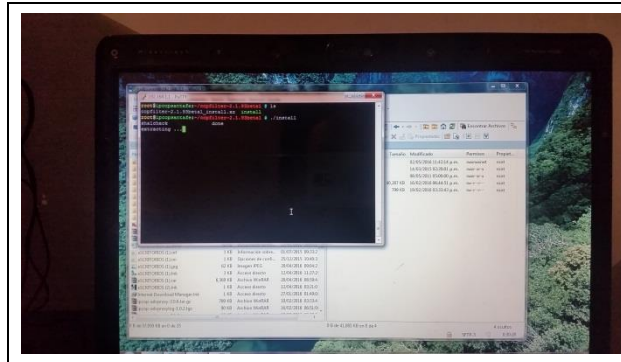


Figura 100. Proceso de instalación del copfilter.

Ahora se puede apreciar que antes de que concluya la instalación muestra un mensaje de advertencia para confirmar la instalación o cancelarla. Ver figura 101.

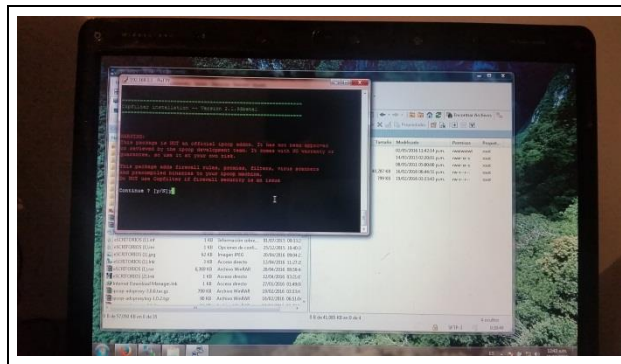


Figura 101. Mensaje de confirmación para la instalación.

En la parte inferior de este mensaje se muestra una pregunta para saber si se desea continuar o no, para continuar hay que presionar la tecla **Y** de lo contrario será la letra **N**.

En esta pantalla se puede apreciar el final del proceso de instalación, el cual fue exitoso, una vez instalado este complemento. Ver figura 102.

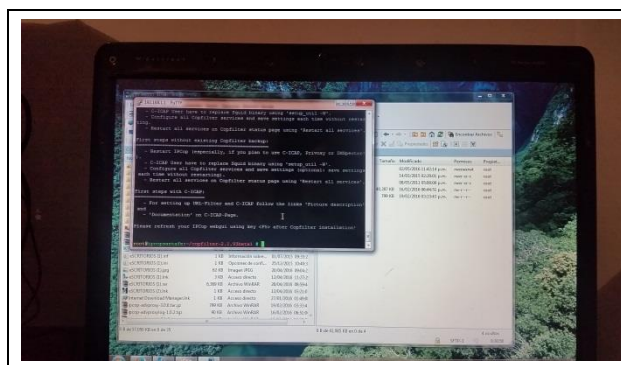


Figura 102. Final de la instalación del copfilter.

Para cerciorarse de que el proceso concluyo correctamente hay que entrar desde el navegador web en esta pantalla se puede apreciar que se encuentra un nuevo menú en la parte derecha de la barra de menús. Ver figura 103.

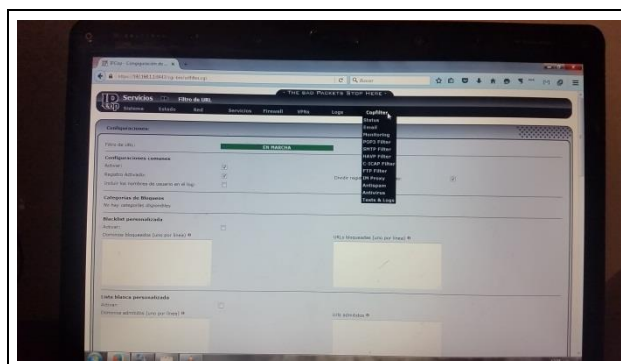


Figura 103. Ubicación del copfilter en el firewall.

Ahora que ya se ha instalado se puede proseguir con las configuraciones que se deben realizar, la primera será el filtrado de contenido web.

Para comenzar con la configuración de filtrado de contenido hay que dirigirse al menú **Servicios/Proxy** como se puede apreciar en la figura 104.

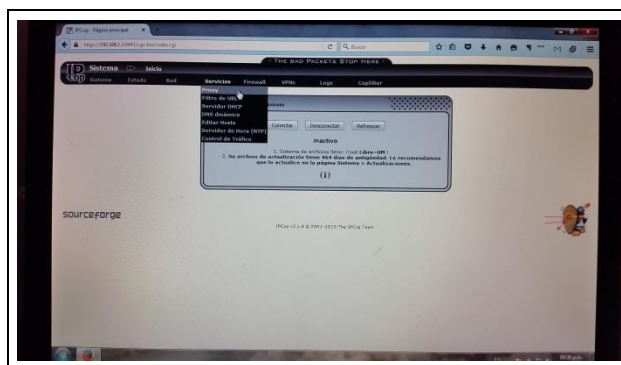


Figura 104. Acceso al submenú Servicios/ Proxy.

En la figura 105. Se puede ver la pantalla principal del apartado del submenú **Proxy** en el cual habrá que activar la casilla de **Redirectores** que se encuentra en la parte inferior de este apartado, una vez marcada la casilla hay que hacer clic en el botón **guardar** para salvar esta configuración, (los **Redirectores** trabajan con el **Proxy** para filtrar y re direccionar el trafico web basado en reglas que pueden incluir listas negras, listas blancas, franjas horarias, etc.).

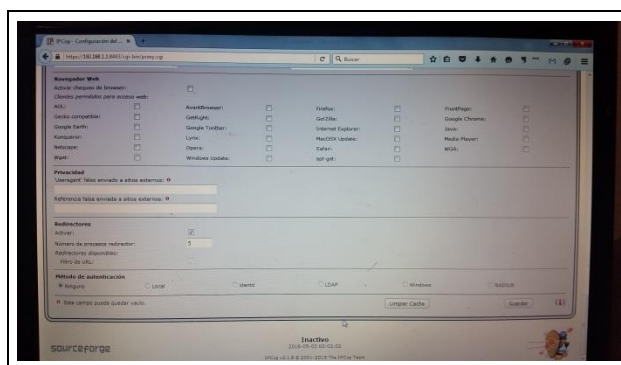


Figura 105. Pantalla principal del submenú Proxy.

Una vez realizado esto hay que habilitar el filtrado web para ello hay que dirigirse al menú **Servicios/Filtro URL**, tal como se muestra en la figura 106.

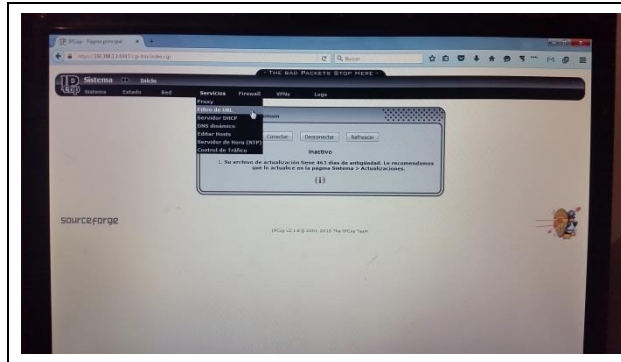


Figura 106. Acceso al menú Filtro URL.

En este apartado se encontrarán con una leyenda que dice **PARADO** en un rectángulo de color rojo, así como una serie de casillas desactivadas en la figura 107 se observan estas, para activarlas solo hay que hacer clic en ellas.

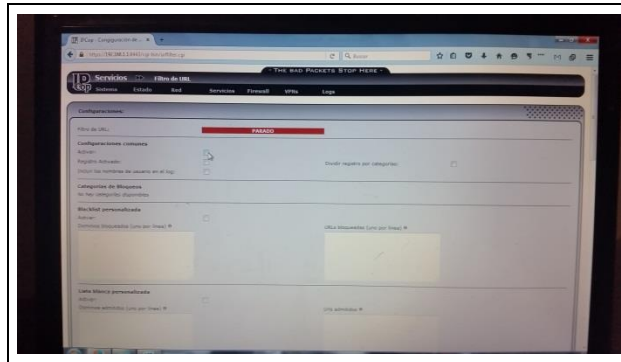


Figura 107. Pantalla principal del menú Filtro URL.

En la figura 108 se muestran las casillas activadas, más abajo se puede ver cajas de texto donde se pueden introducir las páginas o direcciones IP que se deseen bloquear.

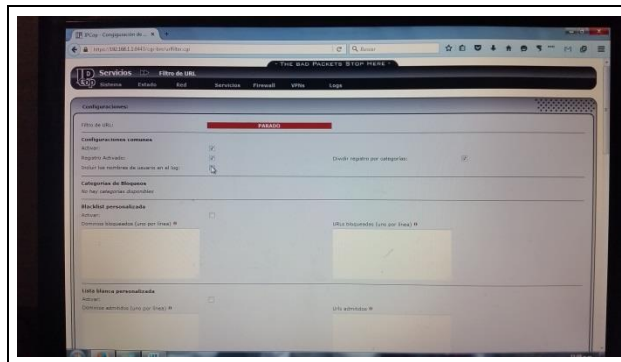


Figura 108. Activación de los servicios del Filtro URL.

A continuación en la figura 109 se puede ver la parte baja de este apartado en el cual hay que hacer clic en el botón guardar para que estas configuraciones surtan efecto.

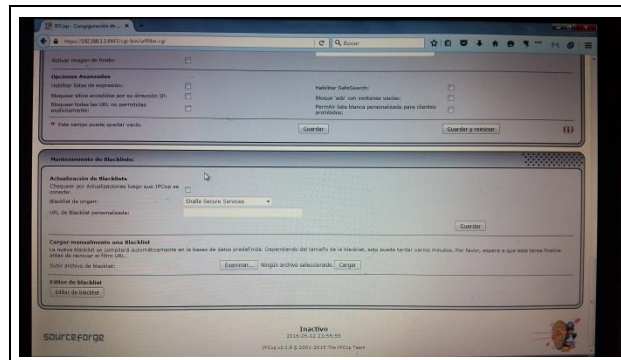


Figura 109. Botón guardar y reiniciar del Filtro URL.

Tras guardar los parámetros el servicio del **Firewall** se reiniciará y posteriormente el cartel de **PARADO** cambiará a **EN MARCHA** en un rectángulo de color verde tal como se muestra en la figura 110.

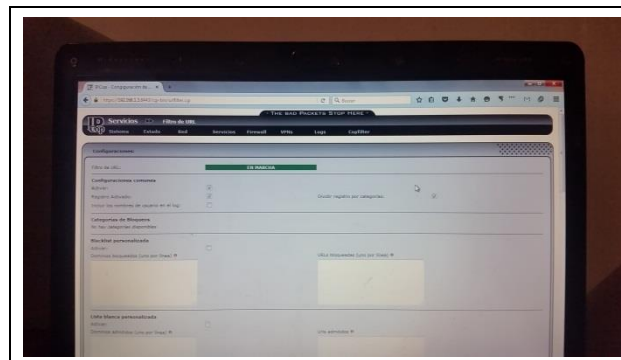


Figura 110. Inicio satisfactorio del filtro URL.

Con esto estará activado el **Filtrado URL** pero para complementar las tareas de este panel hay que instalar una **BLACK LIST** o **lista negra** en la cual se encuentran almacenados de forma categórica los contenidos que comúnmente son bloqueados, esto ayuda a que el contenido se filtre de una manera menos compleja, en la figura 111 se muestra la pantalla de la página <http://urlblacklist.com/?sec=download>. Donde se pueden descargar estas **BLACK LIST**, también se pueden crear estas, pero para hacerlo de la forma más sencilla posible es recomendable descargarlas.

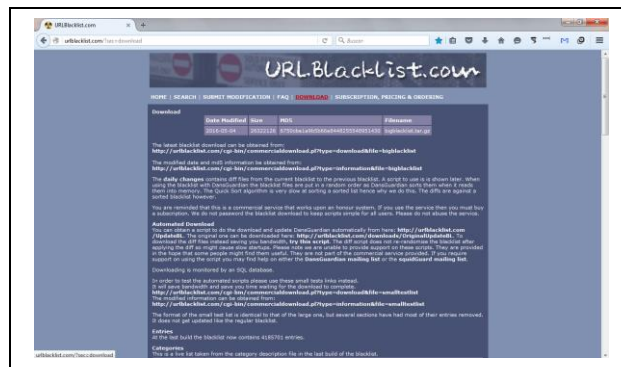


Figura 111. Pantalla de la página: urlblacklist.com

Una vez descargada la **BLACK LIST** más actual se tendrá un archivo comprimido en formato **.tar.gz** el cual se utilizará para agregarlo al **Firewall**.

En la figura 112 se aprecia la parte baja del apartado **Filtro URL** en el cual es donde se realiza la instalación de la **BLACK LIST**.

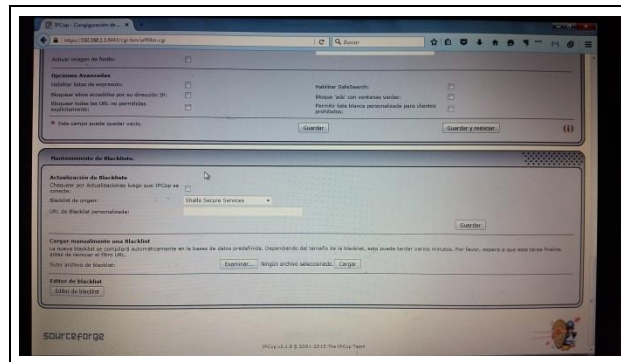


Figura 112. Sección de instalación de listas negras.

Para agregar la **BLACK LIST** solamente basta con hacer clic en el botón **Examinar** para localizar el archivo que se descargó de la página antes mencionada tal como se muestra en la figura 113 y seleccionarlo, para posteriormente hacer clic en el botón **Cargar**.

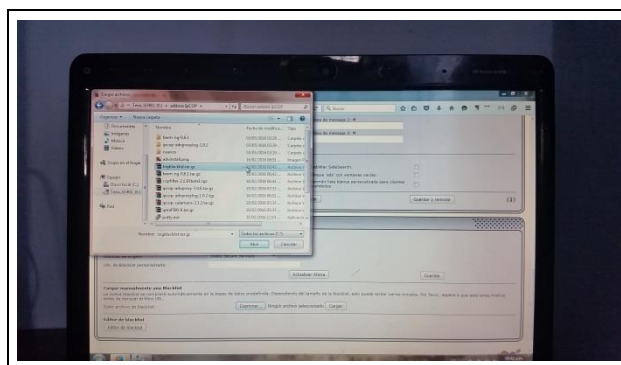


Figura 113. Selección del archivo de la Black List.

Una vez que se ha terminado de cargar la **BLACK LIST** se mostrará un mensaje en la parte superior de la pantalla indicando que la **BLACK LIST** ha sido cargada con éxito y en la parte inferior aparecerá un nuevo módulo el cual se llama **Categorías de bloqueos** que se muestra en la figura 114 donde se pueden ver las distintas categorías del contenido a filtrar de forma alfabética y donde se pueden marcar las que se quieran bloquear.

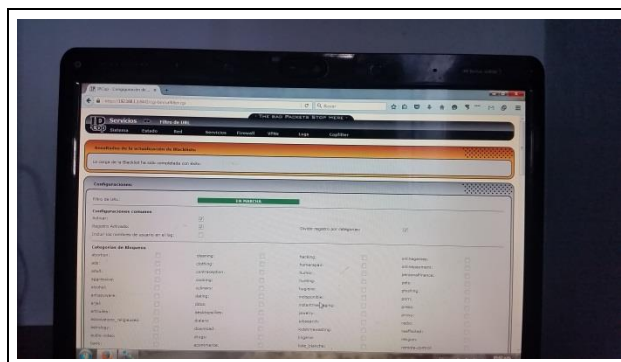


Figura 114. Correcta instalación de la Black List.

Posteriormente de marcar las categorías que se desean bloquear se pueden ingresar direcciones **IP** o dominios dentro de las cajas de texto con las que cuenta este apartado, como se muestra en la figura 115 para que estas listas tengan efecto hay que marcar la casilla de **activación**, al terminar estas configuraciones hay que guardar los cambios realizados y reiniciar el **Proxy** para que surtan efecto, esto se puede hacer haciendo clic en el botón **guardar y reiniciar** que se encuentra en la parte inferior de esta sección.



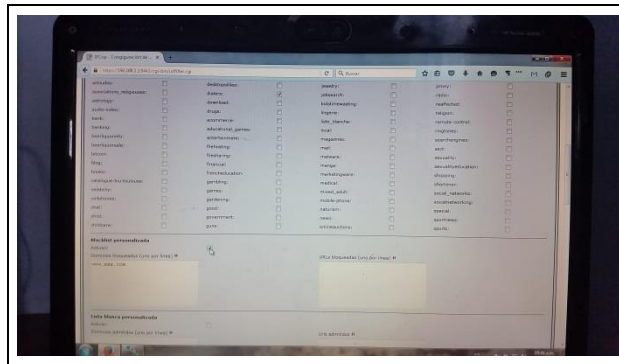


Figura 115. Contenido wep separado por categorías.

Con esto queda configurado el filtro de contenido, pero depende de las necesidades de los usuarios la configuración de este apartado, para el bloqueo de páginas con conexiones seguras (**HTTPS**) como **Facebook** o **Youtube** si fuera necesario solo hay que introducir una línea de comandos en la consola del **Firewall** ya sea directamente en el o desde **PUTTY** en el caso de **Facebook** la línea es la siguiente:

```
# iptables -I FORWARD -p tcp --dport 443 -m string --string www.facebook.com -  
-algo bm -j DROP
```

Y en el caso de Youtube sería la siguiente:

```
# iptables -I FORWARD -p tcp --dport 443 -m string --string www.youtube.com --  
algo bm -j DROP
```

Una vez que se ha guardado y reiniciado el servicio se puede constatar que se esté ejecutando el bloqueo, en la figura 116 se muestra el mensaje de bloqueo que presenta el **Firewall** cuando se intenta entrar a una página que se encuentra bloqueada.

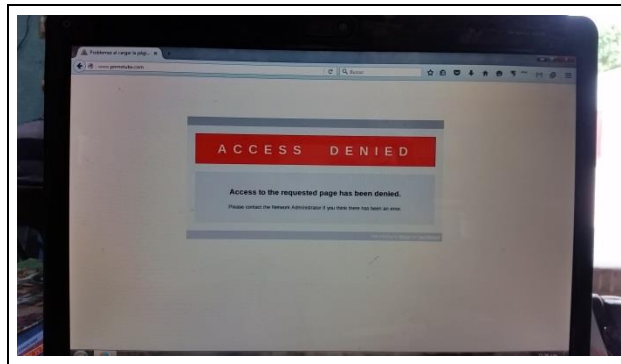


Figura 116. Página bloqueada por el Firewall.

Tras concluir con la configuración del bloqueo de contenido hay que configurar el control de ancho de banda para ello tendrán que seguir los siguientes pasos.

Ahora hay que configurar del control del ancho de banda, para esto es necesario dirigirse al menú “**Servicios/Control de Tráfico**”, donde se mostraran tres apartados los cuales son: **Configuraciones**, **Agregar servicio**, **Servicios de control de tráfico**, en el apartado de “**Configuraciones**” se encuentra una casilla de activación habilitarla solo basta con hacer clic en ella. Ver figura Imagen 117.

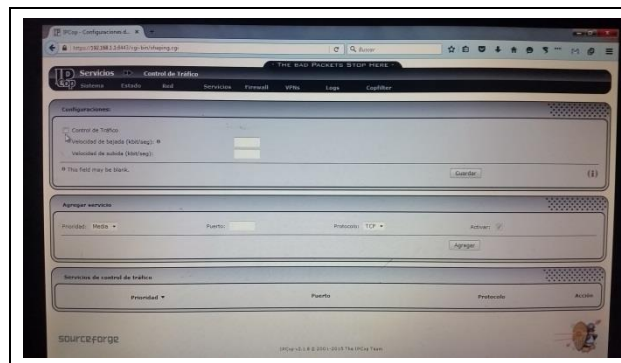


Figura 117. Apartado de control de tráfico del Firewall.

A continuación hay que asignar la velocidad de bajada y de subida del tráfico en las cajas de texto ubicadas en el apartado de “**Configuraciones**”, con lo cual se delimitará su uso, de esta manera todos los equipos de la red solamente utilizaran esa misma velocidad, una vez realizado este paso hay que guardar la configuración. En el menú “**Servicios/proxy**” se puede llevar a cabo la delimitación de las descargas, así como los momentos en los que se pueden hacer las descargas ya sea por hora o día,

también se pueden configurar los límites de transferencias tales como el tamaño máximo de los archivos que se pueden descargar y la velocidad máxima de los archivos que se pueden subir al internet. Ver figura 118.

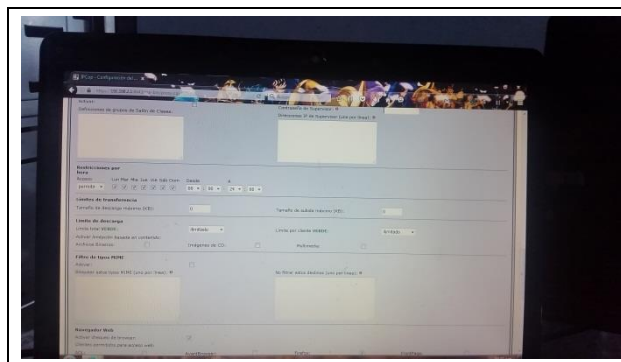


Figura 118. Configuración de rangos de subida y bajada.

## **CAPITULO IV. RESULTADOS**

## 4.1 Cableado estructurado.

Se instalaron canaletas en las áreas de la dirección y el pasillo en la figura 119 y 120 se pueden apreciar las canaletas instaladas en estos dos sitios.



Figura 119. Canaletas en la dirección.



Figura 120. Canaletas fuera de la dirección.

El cable de red que se encontraba en malas condiciones o sin utilizar fue removido de las áreas donde se encontraba. Ver figura 121.



Figura 121. Cable de red.

Se instalaron canaletas en el centro de cómputo para colocar de forma correcta el cable de red que comunica a los **Switch** que se encuentran instalados en dicha área de la escuela. Ver figura 122 y 123.

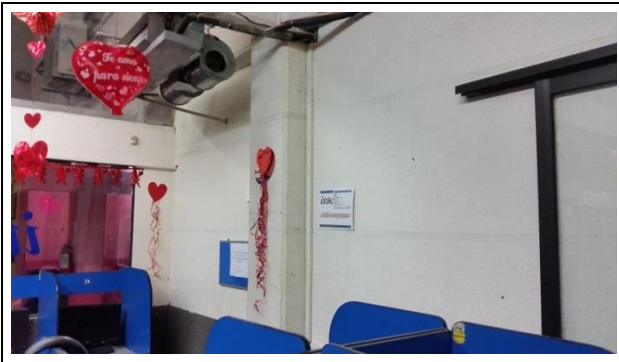


Figura 122. Canaletas del centro de cómputo. Figura 123. Canaleta del centro de cómputo.

Una vez instaladas las canaletas en la dirección, pasillos y centro de cómputo se realizó la instalación del cable de red cat. 5e. Con estas acciones se llevó a cabo el mejoramiento del cableado en las instalaciones.

## 4.2 Firewall.

El equipo de cómputo que se utilizó para la instalación del **Firewall** fue instalado en la dirección de la escuela, junto a uno de los equipos de cómputo con el que se realizan tareas de administración debido a que no se contaba con otro espacio, aunque es más recomendable colocarlo de forma aislada por motivos de seguridad. Ver figura 124.



Figura 124. Firewall IPCop en la dirección del ITEC.

### 4.3 Análisis de resultados.

Se realizó una encuesta a un grupo de 10 alumnos que se encontraban en las instalaciones del **ITEC** para saber cuál era su opinión del servicio tras la instalación del **Firewall** en la red y de esta manera poder analizar los resultados; las preguntas que se realizaron son las siguientes:

1 ¿Qué opina del actual servicio de internet?

Malo                      Regular                      Bueno

2 ¿Sabe lo que es un Firewall?

Si                      No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo                      Regular                      Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es?

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala                      Regular                      Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor                      Igual                      Mejor                      No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son?

No ¿Por qué?

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué?

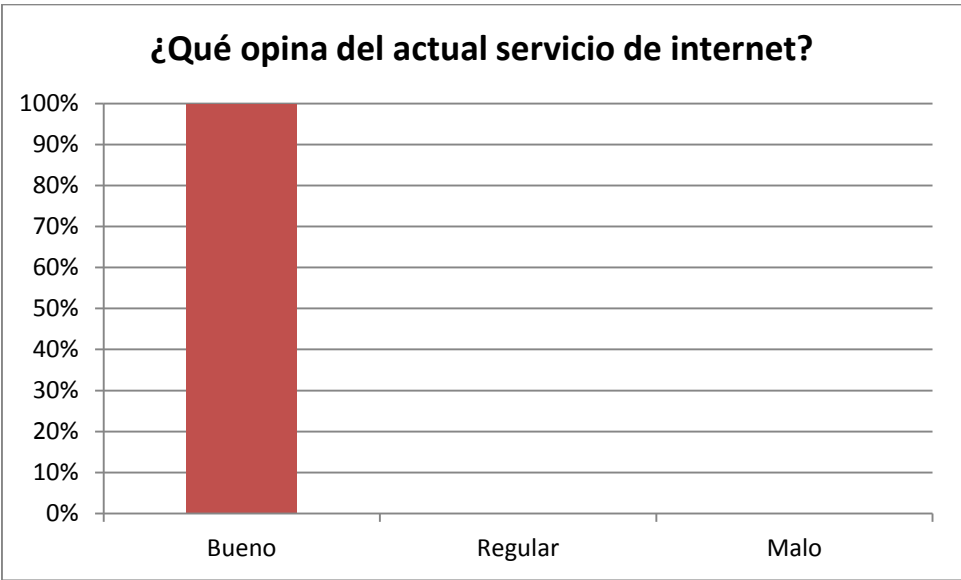
No, ¿Por qué?

Véase las respuestas en la sesión de anexos.

Con los resultados obtenidos de las encuestas se realizó un análisis con el cual se pudo corroborar que el servicio de internet en las instalaciones de la escuela mejoró considerablemente ya que los usuarios percataban un cambio en la velocidad con la que se podía navegar, también se referían con comentarios favorables respecto a la seguridad en la navegación ya que al encontrarse con el bloqueo de páginas potencialmente peligrosas consideraban que pueden navegar de forma más segura. Además se realizó el análisis y la comparación de las respuestas obtenidas de esta encuesta con las respuestas del sondeo anterior, de dicho análisis se realizaron una serie de gráficas con las cuales se puede observar los niveles de comparación. Véase el anexo 2.

En los resultados de esta última encuesta los usuarios califican el servicio de mejor manera que en la anterior y consideran que la posibilidad de que ahora se les permita navegar en sus dispositivos móviles les parece una mejora en el servicio que se les ofrece actualmente. También se preguntó si recomendarían el uso de este sistema a dicho cuestionamiento su contestación fue afirmativa.

A continuación se muestra una de las gráficas mediante las cuales se realizaron los análisis de las respuestas a esta última encuesta. Para ver el resto de ellas véase el anexo 2.





## CONCLUSIONES

Tras la mejora del cableado estructurado en las áreas del centro de cómputo, dirección, pasillos, es posible apreciar los cambios de manera inmediata en la eficiencia de la conexión y el aspecto debido a que el cable con el que se contaba anteriormente se podía ver por los pasillos, con el recubrimiento exterior roto en secciones, con conectores dañados, por lo que se considera que se realizaron las tareas adecuadas al colocar las canaletas, remover los cables excedentes y en mal estado.

Posterior a la instalación, configuración del **Firewall** para poder llevar a cabo las tareas del control del ancho de banda y el filtrado web en la red local del **ITEC**, se realizó una encuesta a un grupo de alumnos mediante la cual se pudieron analizar sus respuestas y de esta manera llegar a la conclusión de que el servicio de internet con el cual se trabajaba mejoró considerablemente, los usuarios y los encargados de la institución piensan que al llevar a cabo estas tareas se sienten más seguros al realizar una conexión desde los equipos de cómputo de la institución como desde sus dispositivos personales puesto que anteriormente por las carencias de los métodos de seguridad no proporcionaban este servicio, esto les parece una gran mejora.

Con esto se puede comprobar que la hipótesis se cumple debido a que los resultados obtenidos del análisis de los resultados que se obtuvieron son satisfactorios, los usuarios se sienten más seguros al navegar puesto que el contenido potencialmente peligroso es bloqueado con efectividad, por consecuencia la seguridad tiene un aumento considerable, el ancho de banda es mejor aprovechado debido a que delimitar el tráfico entrante y saliente se puede administrar de mejor manera, también al contar con memoria caché el firewall propicia que la navegación se más rápida porqué las peticiones a las páginas más consultadas ya no se hace directamente a la red sino al Firewall.

Con esto se puede concluir que la hipótesis se comprueba de forma satisfactoria ya que se demuestra que un sistema de firewall de bajo costo para controlar el ancho de banda y restringir el contenido web como parte de una solución para **MPyME's** es muy factible y recomendable.

## **ANEXOS**

## ANEXO 1. ENCUESTAS

Nombre: Belén Ángeles Martínez Mejía

Edad: 14 años

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Está bien pero a veces cuando estamos muchos en las computadoras se pone lento**

2 ¿Considera que está seguro mientras navega en internet?

**R: Si, por que entro a las páginas que el maestro nos dice y cuando seguimos sus instrucciones no tengo problemas**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube, Facebook y la Wikipedia**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: Las páginas para adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que está muy bien por qué a veces en algunas páginas nos aparecen ventanas de páginas para adultos**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si porque a veces todos estamos viendo youtube y se pone lento el internet**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: mejor y de esa manera no nos preocuparíamos de las páginas para adultos o estaríamos más seguros cuando estemos usando el internet**

**Nombre: Rodolfo Héctor Beltrán Solís**

**Edad: 12 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: que está muy bien**

2 ¿Considera que está seguro mientras navega en internet?

**R: Si, por que el profe nos ayuda**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Wikipedia, youtube, Facebook y el google**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: las páginas para los adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que estaría muy bien para que no se puedan ver cosas que no son buenas y que puedan meterle virus a las computadoras**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?  
Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si, porque así podríamos usar el internet todos**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Que sea mejor y estemos más seguros al usar las computadoras**

**Nombre: José Mario Hernández García**

**Edad: 39 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Regular, no a considero mala, pero podría ser mejor**

2 ¿Considera que está seguro mientras navega en internet?

**R: mientras visitemos las páginas que nos recomienda el profesor durante la clase sí, pero cuando usamos las computadoras después de terminar nuestras prácticas, a veces no quiero entrar a páginas porque pueden tener virus**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube, Wikipedia, Facebook y Hotmail**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No, no sé qué es eso**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: principalmente las páginas pornográficas, porque aquí toman clase niños pequeños y no me parecen adecuado que ellos pudiesen verlas**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: Que está muy bien porque así podemos estar más tranquilos de las páginas que visitan los niños que toman clase, y también nosotros estaríamos más seguros de no contagiar un virus en las computadoras**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si, por que algunas veces algunos ven YouTube y se pone lento el internet**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Que sea más seguro porque si se instala el internet va a ser más seguro, no veríamos las ventanas que aparecen de páginas para adultos**

**Nombre: María León Aguilar**

**Edad: 17 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Esta bien pero en ocasiones se pone lento cuando hay muchos usando las computadoras**

2 ¿Considera que está seguro mientras navega en internet?

**R: si por que no entro a páginas que no se nos recomienden**

3 ¿Cuáles son las páginas de internet que más visita?

**R: youtube, Facebook, Gmail, Hotmail, miniclips**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: Las páginas XXX y las de violencia**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: estaría muy bien porque así no nos preocuparíamos tanto por las paginas xxx**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si creo que así podríamos usar mejor el internet**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No ninguna**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Espero que sea más rápida y con más seguridad que ahora**

**Nombre: Leticia Castro Navarro**

**Edad: 42 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Se encuentra muy bien, pero considero que podría mejorar**

2 ¿Considera que está seguro mientras navega en internet?

**R: considerando si porque solo utilizo las páginas que nos indica nuestro profesor**

3 ¿Cuáles son las páginas de internet que más visita?

**R: youtube, Facebook, Wikipedia y Hotmail**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: Las páginas para adultos y aquellas páginas donde se promueve la violencia**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que sería excelente utilizan las te porque hay niños que usan las computadoras y no siempre se puede estar pendiente de ellos**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si eso significa que podemos usar de forma más rápida y con más seguridad el internet se debería de instalar, cualquier cosa que ayude a que los jóvenes puedan usar las computadoras de una forma más segura es muy buena**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: espero que pueda ser más rápida y más segura**

**Nombre: Ruth Santos Ortega**

**Edad: 40 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Muy bueno**

2 ¿Considera que está seguro mientras navega en internet?

**R: Si, siempre tenemos la ayuda de nuestros profesores**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube y Facebook**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: los que son para adultos porque aquí reciben clases niños menores y podrían ver esas páginas**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: muy bien, para que los niños no puedan ver cosas que no deban**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si nos ayuda a que el internet este más rápido considero que si**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: mejor de cómo es ahora**



**Nombre: Erick Torres Romero**

**Edad: 13 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: la mayor parte del tiempo es muy bueno**

2 ¿Considera que está seguro mientras navega en internet?

**R: una vez me salió una página que decía que tenía virus así que no creo que sea siempre seguro**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube, Facebook, Wikipedia y Hotmail**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

R: las paginas para adultos y las que tienen virus

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

R: Que estaría muy bien para no entrar a páginas con virus

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: si sirve para que este mejor el internet si**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Espero que sea mucho mejor y que no tengamos que preocuparnos tanto**

**Nombre: Sofía Gómez Gómez**

**Edad: 17 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Que está muy bien**

2 ¿Considera que está seguro mientras navega en internet?

**R: Si**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Facebook, youtube, Gmail y wikipedia**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: Las páginas para adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que serviría de mucho para no poder entrar a páginas para adultos o con virus**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si sirve para que este más rápido es mucho mejor**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Espero que sea más segura y mucho más raída**

**Nombre: Claudia Hernández Mora**

**Edad: 22 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: en ocasiones esta, rápido en ocasiones está lento pero en general está bien**

2 ¿Considera que está seguro mientras navega en internet?

**R: No del todo, sé que existen páginas donde se pueden robar los datos**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube, Facebook y mail**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: las páginas donde hay cosas para adultos, páginas donde hay virus y donde puedan robar nuestra información**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: Que estaría muy bien porque hay jóvenes más pequeños que podrían entrar a páginas inadecuadas para ellos**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si, así podría estar mejor el internet**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: pues que sea más seguro y más rápido**

**Nombre: Luis Enrique Lozano Garrido**

**Edad: 22 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: que se encuentra muy bien**

2 ¿Considera que está seguro mientras navega en internet?

**R: No del todo pero si le hacemos caso al profesor nos sentimos más seguros**

3 ¿Cuáles son las páginas de internet que más visita?

**R: youtube, Facebook y Hotmail**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: los contenidos para adultos por qué hay páginas que no son recomendadas para los más jóvenes**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que hace mucha falta y que sería algo muy importante para estar más seguro**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si, por que podría estar más rápido**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: espero que sea más segura y más rápida**

**Nombre: Hesiquio José García Cruz**

**Edad: 43 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Considero que está bien**

2 ¿Considera que está seguro mientras navega en internet?

**R: No es su totalidad por que hay páginas con las que pueden infectar con virus las computadoras**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Hotmail**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: Las paginas para adultos y las páginas donde podemos bajar virus**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: Que estaría excelente porque así podríamos estar más seguros**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si ayuda a hacer que el internet este mas raído considero que si**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Espero que sea mucho más rápida y sea más segura**

**Nombre: Juan Pablo García Rodríguez**

**Edad: 13 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: que está bien**

2 ¿Considera que está seguro mientras navega en internet?

**R: No completamente no se puede estar siempre seguro**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Facebook y youtube**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: Las páginas para adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: Que ayudaría mucho para que usemos las computadoras con más seguridad**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si, para que el internet sea más rápido**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: que el internet sea más rápido y más seguro**

**Nombre: David Ortiz García**

**Edad: 13 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Considero que el servicio del internet está regular**

2 ¿Considera que está seguro mientras navega en internet?

**R: Si, por que en las computadoras tenemos antivirus**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Wikipedia, Youtube y Facebook**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: las paginas para adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que hace falta, porque hay páginas con cosas que no deberíamos ver**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si porque así estaría más rápido el internet**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Pues que sea más segura, para que no se puedan abrir páginas para adultos**

**Nombre: María Martínez Gómez**

**Edad: 23 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: que está bien pero podría ser mejor tal vez más rápido**

2 ¿Considera que está seguro mientras navega en internet?

**R: En ocasiones aparecen ventanas con mensajes de páginas que no abrimos así que creo que no en su totalidad**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube y Facebook**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: las páginas para adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que podríamos estar más seguros cuando usemos el internet, ya que no todas las paginas son seguras**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: si por qué a veces está un poco lento pero la mayor parte del tiempo está bien**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Esperaría que fuera más segura**



**Nombre: Héctor Hernández Hernández**

**Edad: 13 años**

1 ¿Cómo considera usted que es el servicio de internet actual?

**R: Esta bien pero podría mejorar**

2 ¿Considera que está seguro mientras navega en internet?

**R: si, por que tenemos ayuda de nuestro profesor**

3 ¿Cuáles son las páginas de internet que más visita?

**R: Youtube y Facebook**

4 ¿Sabe lo que es y para qué sirve un Firewall?

**R: No**

5 ¿Qué tipo de contenidos cree usted que debe de ser bloqueados?

**R: las páginas para los adultos**

6 ¿Qué opina de la instalación de un servicio que realice el filtro de contenido que usted consulta en Internet?

**R: que estaría muy bien para que no haya tanto problema**

7 ¿Conoce usted herramientas para mejorar la velocidad de navegación?

Si, ¿Cuáles conoce?

**R: No**

8 ¿Considera que se debe de controlar la velocidad del internet?

**R: Si por que es mejor para que el internet este más rápido**

9 ¿Conoce usted herramientas para mejorar la seguridad en una red?

**R: No**

10 ¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?

**R: Esperaría que fuera más seguro**

**Nombre: Ariadna Lucia Ruiz**

**Edad: 27**

**1 ¿Qué opina del actual servicio de internet?**

Malo

Regular

Bueno

**2 ¿Sabe lo que es un Firewall?**

SI

No

**3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?**

Malo

Regular

Bueno

**4 ¿Ha notado algún cambio en la navegación actual?**

Si, ¿Cuáles es? Pues esta un más rápido cuando entro a algunas páginas y ya no aparecen ventanas con imágenes para adultos

**No**

**5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?**

Mala

Regular

Buena

**6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?**

Peor

Igual

Mejor

No noto cambios

**7 ¿Considera usted que se deban hacer cambios a la red actual?**

Si, ¿Cuáles son?

No ¿Por qué? No, porque ahora ya está mejor, antes en algunas páginas aparecían imágenes para adultos y ahora no se ven o no se pueden entrar a esas páginas.

**8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?**

Si, ¿Por qué? Si, por que está muy bien que no se puedan ver páginas con violencia.

**No, ¿Por qué?**

**Nombre: Dulce Karina Juárez**

**Edad: 19 años**

**1 ¿Qué opina del actual servicio de internet?**

Malo

Regular

Bueno

**2 ¿Sabe lo que es un Firewall?**

SI

No

**3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?**

Malo

Regular

Bueno

**4 ¿Ha notado algún cambio en la navegación actual?**

Si, ¿Cuáles es? Se puede entrar más rápido en algunas páginas

No

**5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?**

Mala

Regular

Buena

**6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?**

Peor

Igual

Mejor

No noto cambios

**7 ¿Considera usted que se deban hacer cambios a la red actual?**

Si, ¿Cuáles son?

**No ¿Por qué? No, creo que esta mejor que antes el internet**

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué?, si porque ya es más seguro usar el internet y podrían evitar los virus y páginas para adultos y violentas

No, ¿Por qué?

Nombre: Ángel García Ramírez

Edad: 62

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Que ya no aparecen ventanas con mensajes de premios o de que tenemos virus cuando abrimos alguna página

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son?

No ¿Por qué? No porque ya está muy bien y es más seguro

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Claro porque es más seguro así y se pueden evitar páginas inapropiadas

No, ¿Por qué?

Nombre: Ubaldo Mejía Solano

Edad: 34

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Ya no aparecen las ventanas emergentes y se bloquean las ventanas de contenido inapropiado

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son?

No ¿Por qué? No, porque está muy bien ahora que está más segura

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Claro porque es más segura la red con este servicio y no se pueden entrar a páginas que son para adultos aquí está muy bien porque hay niños que podrían entrar a ellas pero con ese sistema no es posible

No, ¿Por qué?

Nombre: José Mario Hernández García

Edad: 39 años

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Para entrar a algunas páginas esta mejor porque es más rápido

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son? ahora está mejor que antes pero creo que podría ser muchísimo más rápido

No ¿Por qué?

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Si, ahora ya las ventanas emergentes que solían aparecer antes ya no aparecen, y tras hacer una prueba con el profesor de entrar a una página para adultos no se pudo entrar y eso está muy bien porque es más seguro

No, ¿Por qué?

Nombre: Leticia Castro Navarro

Edad: 42 años

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Ya no se puede entrar a páginas que promueven la violencia y que tienen imágenes para adultos

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son?

No ¿Por qué? Está muy bien ahora, antes era un poco más

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Sí, porque de esta manera se pueden evitar que se vean páginas que no son adecuadas

No, ¿Por qué?

Nombre: Esther Sánchez Hipólito

Edad: 12

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Podemos entrar a las páginas un poco más rápido que antes

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son?

No ¿Por qué? El internet ya está un poquito más rápido pero creo que podría ser mucho más rápido

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Creo que sí para que su internet este un poquito más rápido

No, ¿Por qué?



Nombre: José María Pérez Cruz

Edad: 25

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Si, que ahora podemos entrar un poco más rápido a algunas páginas y que se han bloqueado las páginas para adultos

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son? Pues en google se pueden hacer algunas búsquedas de páginas inapropiadas, aunque no las abre, podría ser posible que no se hagan las búsquedas, porque hay otras que simplemente no carga la búsqueda, creo que es lo único

No ¿Por qué?

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Si lo recomendaría porque me parece que es una buena ayuda para que los que usen el internet están más seguros y tranquilos con lo que ven en el internet

No, ¿Por qué?

Nombre: Elizabeth Silva Huerta

Edad: 18 años

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Pues para entrar al youtube está un poco más rápido y ya nos dan permiso de entrar al internet con nuestro teléfono cuando salimos de clase y eso está mejor y ya no se aparecen ventanas con cosas que nosotros no abrimos

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son? Hay páginas donde se podían descargar juegos y ahora ya no, creo que nos debería dejar creo que es lo único malo porque antes si se podía aunque a veces se abrían ventanas que nosotros no habíamos abierto

No ¿Por qué?

8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Si, por que ya es más seguro con esa forma de seguridad y es un poquito más rápido, creo que está muy bien

No, ¿Por qué?

Nombre: Yajaira Salgado Martínez

Edad: 23

1 ¿Qué opina del actual servicio de internet?

Malo

Regular

Bueno

2 ¿Sabe lo que es un Firewall?

SI

No

3 ¿Qué opina del servicio que controla el ancho de banda y el filtrado de contenido web que se instaló?

Malo

Regular

Bueno

4 ¿Ha notado algún cambio en la navegación actual?

Si, ¿Cuáles es? Que es un poco más rápido y más seguro porque ya no hay ventanas emergentes con contenido que no abrimos y ya no se pueden abrir algunas páginas que podrían tener virus

No

5 ¿Cómo es la seguridad en la navegación ahora que se instaló un sistema que filtra el contenido web?

Mala

Regular

Buena

6 ¿Con respecto al servicio de internet anterior a la instalación del Firewall, como considera que esta el servicio?

Peor

Igual

Mejor

No noto cambios

7 ¿Considera usted que se deban hacer cambios a la red actual?

Si, ¿Cuáles son? Pues antes se podía uno bajar música y ahora algunas páginas donde podíamos bajarla ya no se abren pero en general está bien creo que solo eso, que nos dejaran bajar música

No ¿Por qué?

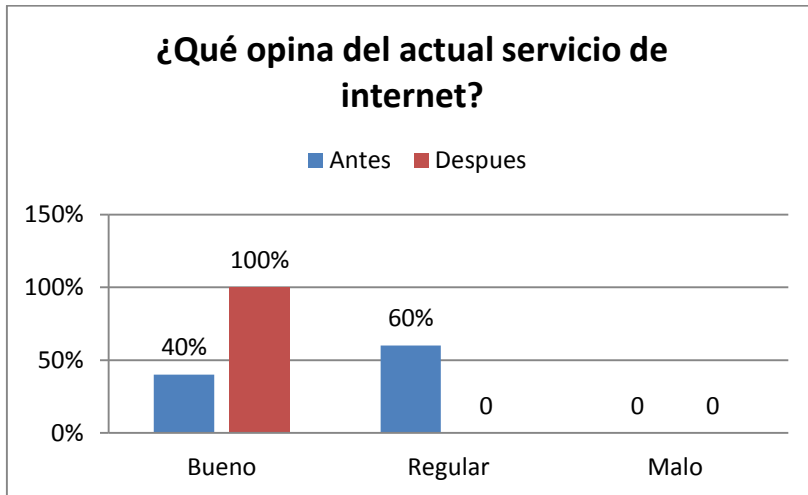
8 ¿Recomendaría usted el sistema de control de ancho de banda filtrado web que está instalado actualmente en la red del ITEC a otros pequeños y medianos empresarios?

Si, ¿Por qué? Si, por que se pueden evitar virus y podrían controlar lo que se ven en el internet

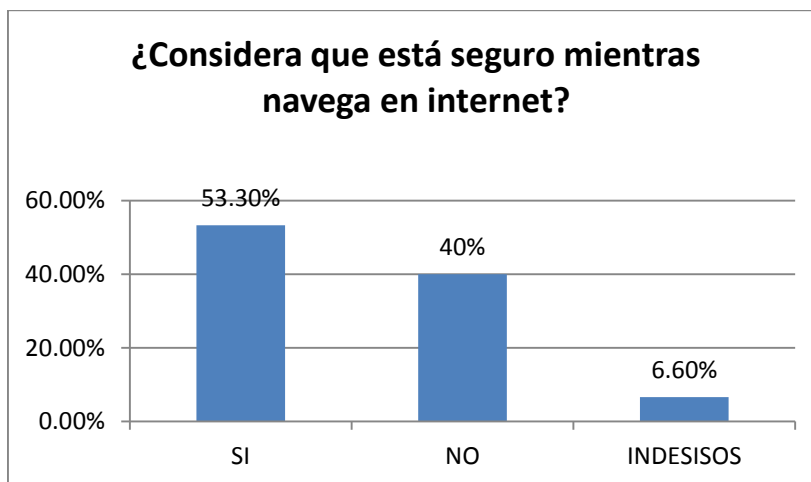
No, ¿Por qué?

## ANEXO 2. GRÁFICAS

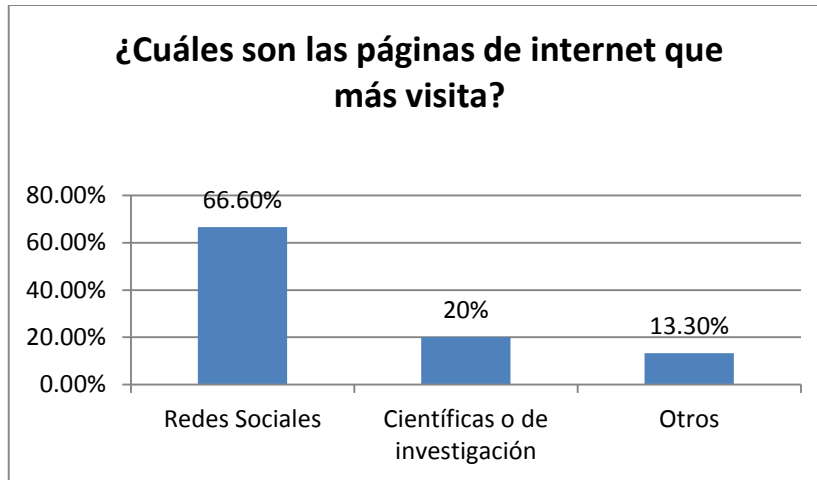
Pregunta No. 1			
	Bueno	Regular	Malo
Antes	40 %	60 %	0
Después	100 %	0	0



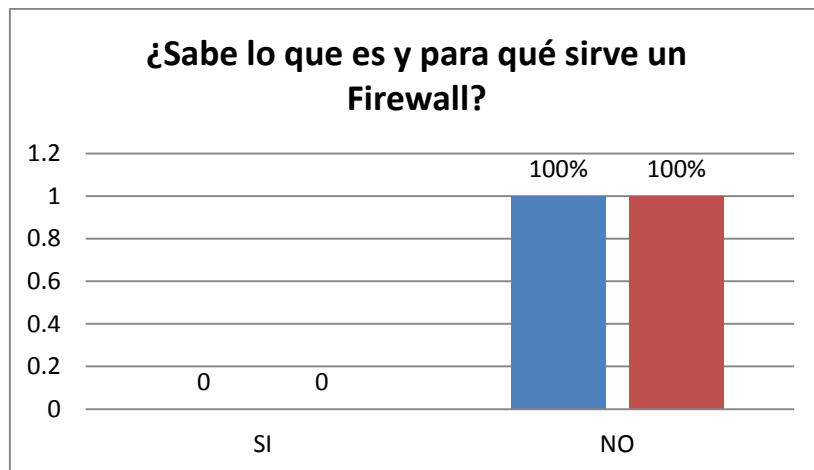
Pregunta No. 2		
Si	No	Indecisos
53.3 %	40 %	6.6 %



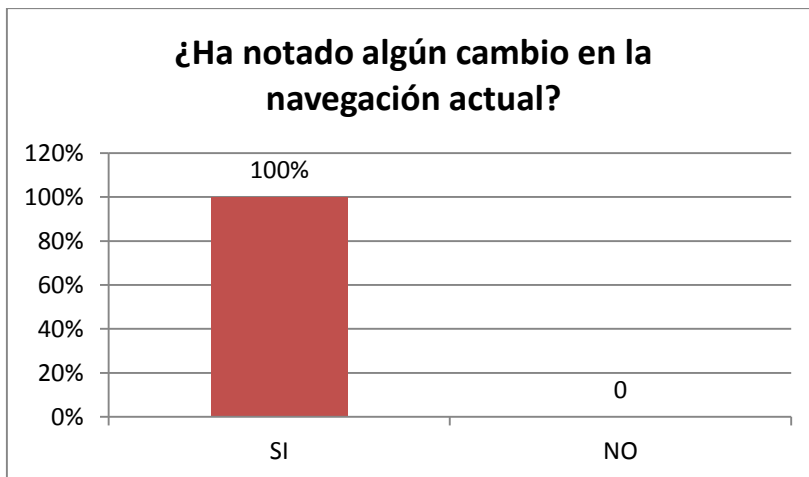
Pregunta No. 3		
Redes Sociales	Científicas o de investigación	Otros
66.6 %	20 %	13.3 %



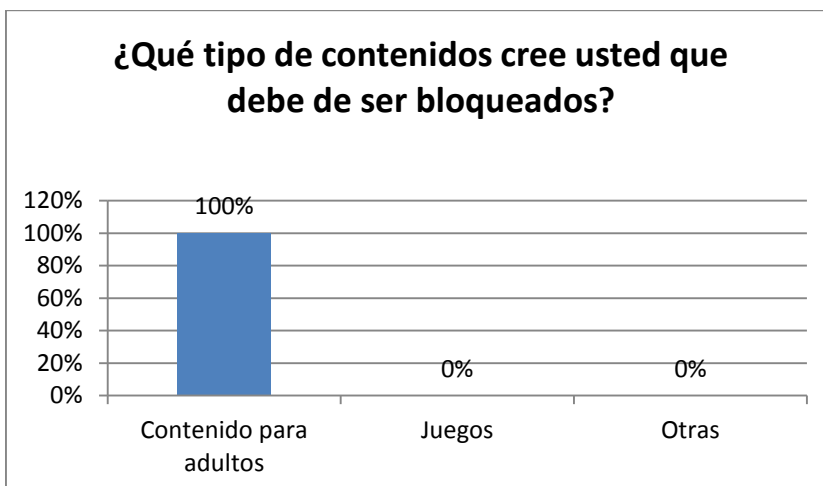
Comparación de la pregunta 4 del antes y la pregunta 2 del después		
	SI	NO
Antes	0	100 %
Después	0	100 %



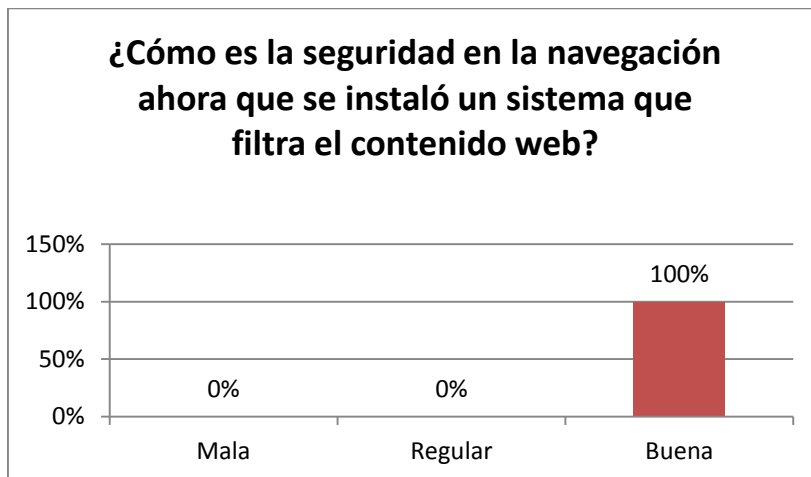
Pregunta No. 4	
SI	NO
100 %	0



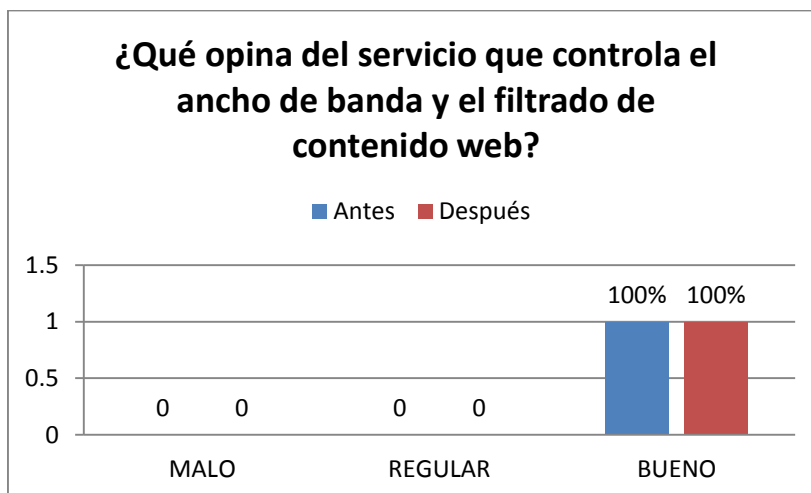
Pregunta No. 5		
Contenido para adultos	Juegos	Otras
100 %	0	0



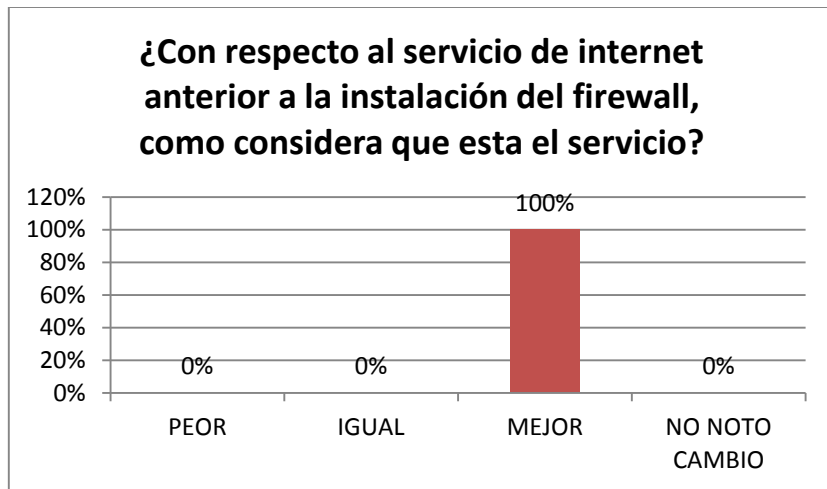
Pregunta No. 5		
MALA	REGULAR	BUENA
0	0	100 %



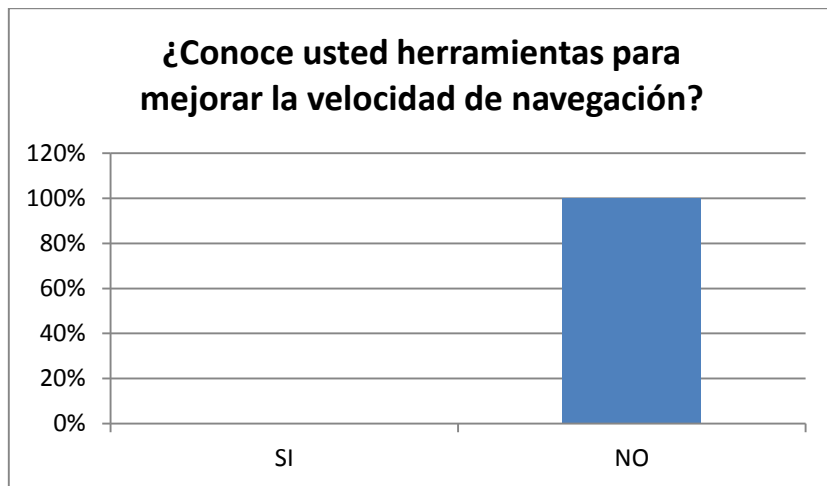
Comparación de la pregunta 6 del antes y la pregunta 3 del después		
Es bueno	Es malo	Indiferencia
15	0	0
10	0	0



Pregunta No. 6			
PEOR	IGUAL	MEJOR	NO NOTO CAMBIO
0	0	100 %	0

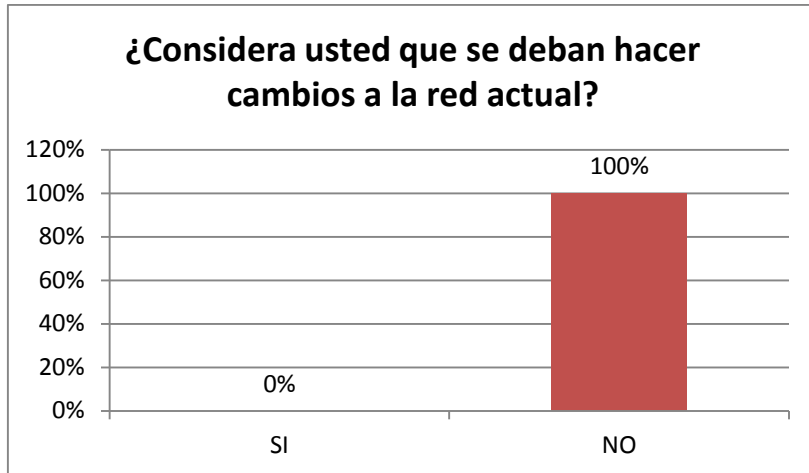


Pregunta No. 7	
SI	NO
0	100 %

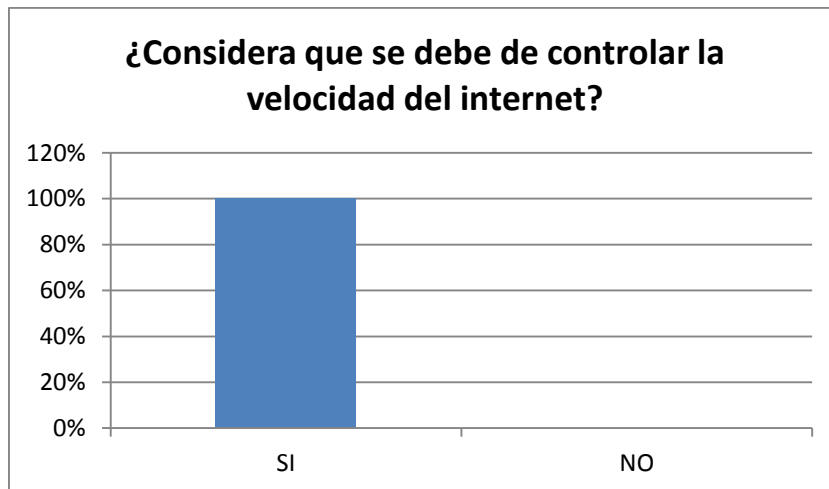




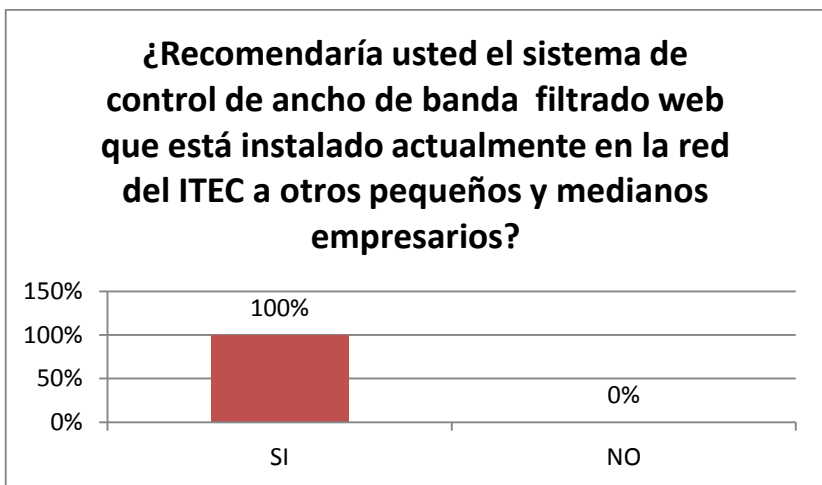
Pregunta No. 7	
SI	NO
0	100 %



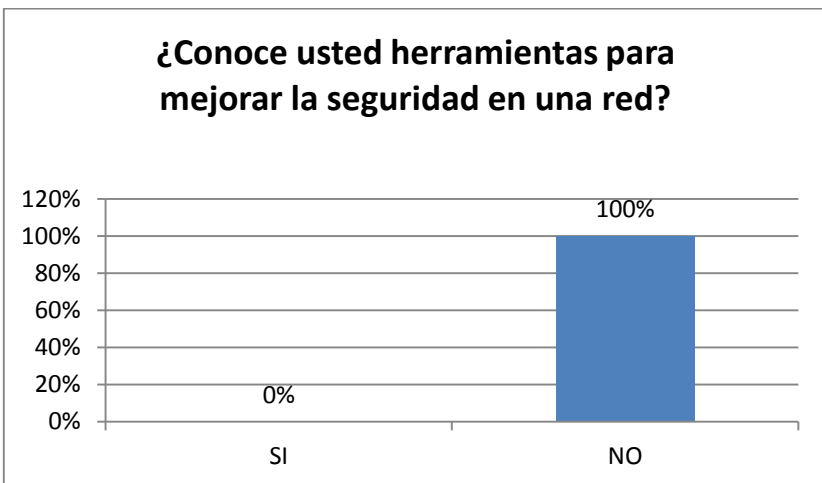
Pregunta No. 8	
SI	NO
100 %	0



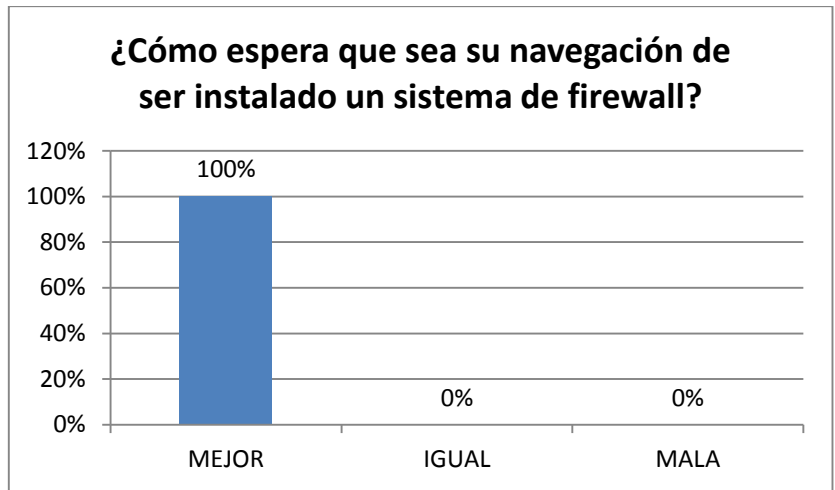
Pregunta No. 8	
SI	NO
100 %	0



Pregunta No. 9	
SI	NO
0	100 %



Pregunta No. 10		
¿Cómo espera que sea su navegación de ser instalado un sistema de Firewall?		
MEJOR	IGUAL	MALA
100 %	0	0



### ANEXO 3. EVIDENCIAS

Comparativa del antes y después de las tareas de mejoramiento del cableado estructurado.

Fotografías tomadas antes de la restructuración del cableado estructurado:

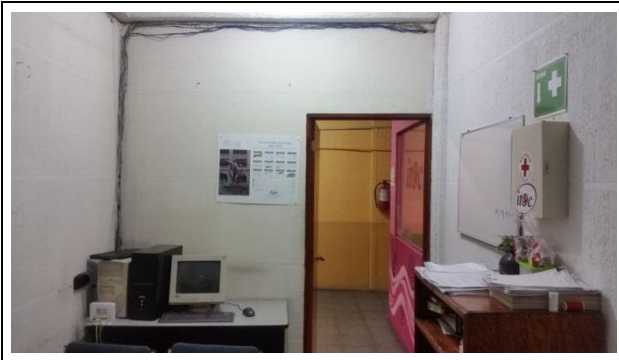


Figura 125. Cable de red en la dirección.



Figura 126. Instalación telefónica y eléctrica.



Figura 127. Cable de red en los pasillos.



Figura 128. Cable de red en los pasillos.

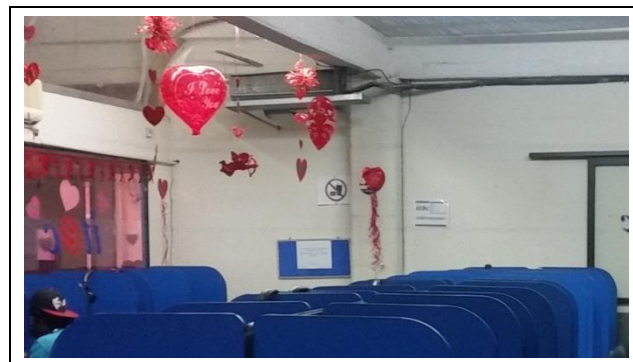


Figura 129. Cable de red en el centro de cómputo.

Fotografías tomadas tras la mejora del cableado estructurado:



Figura 130. Canaletas del centro de cómputo.

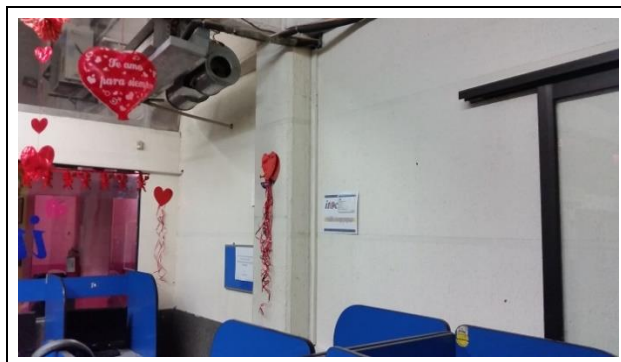


Figura 131. Canaletas en la dirección.



Figura 132. Canaletas en los pasillos.



Figura 133. Canaletas en los pasillos.

## GLOSARIO DE TÉRMINOS.

### A

#### **ADSL**

Acrónimo del inglés Asymmetric Digital Subscriber Line que consiste en la transmisión analógica de datos digitales por medio de una línea telefónica convencional, 22

#### **AIEE**

Siglas para definir al Instituto Americano de Ingenieros Eléctricos, 19

#### **AP**

Acrónimo en inglés para Punto de Acceso, estos son dispositivos que permiten el acceso a una red mediante Wi-Fi, 25

Acrónimo en inglés para Punto de Acceso, estos son dispositivos que permiten el acceso a una red mediante Wi-Fi, 21, 24, 25

### B

#### **BLE**

Bluetooth de Baja Energía, 29

#### **Bridge**

Dispositivo de red que realiza la conexión entre dos redes haciendo la función de un puente, 24

### C

#### **Caracteres ASCII**

Es el Código Estándar Estadounidense para Intercambio de Información, es un código de caracteres basado en el alfabeto latino, 24

#### **Cifrado AES**

Es un esquema de cifrado por bloques adoptado como estándar de cifrado por el gobierno de los Estados Unidos, 25

### E

#### **EAP**

Es un entorno de autenticación usado habitualmente en redes LAN inalámbricas y puede ser utilizado para autenticación en redes cableadas, 25

#### **Encriptación RC4**

Es el sistema de cifrado de flujo más utilizado en algunos de los protocolos más populares como TLS/SSL y WEP, 24

### F

#### **Firewall**

Sistema cortafuegos ya sea basado en Software o aplicación, su función es la de actuar como una barrera entre dos redes., VI, 2, 4, 5, 7, 8, 44, 45, 46, 47, 58, 62, 63, 67, 71, 72, 73, 75, 80, 81, 82, 85, 86, 87, 89, 90, 91, 96, 97, 99, 100, 101, 102, 108, 109, 111,

112, 116, 117, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 154

Sistema cortafuegos ya sea basado en Software o aplicación, su función es la de actuar como una barrera entre dos redes., 66

#### **Fraggle Attack**

Tipo de ataque DoS que implica el envío de una gran cantidad de tráfico falso a la dirección de difusión de un router en una red., 56

#### **Full-duplex**

Modo de transmisión y recepción de datos en dos direcciones, ambas al mismo tiempo, 19

## **H**

#### **Hackers**

es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo., 45, 57

#### **Half-duplex**

Modo de transmisión y recepción de datos en dos direcciones pero en una dirección a la vez, 19, 33

#### **Hardware**

Es el conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático, 25, 27, 30, 34, 44, 45, 49, 50, 51

## **I**

#### **ICMP Ping Flood**

Tipo de ataque Dos que consiste en saturar una línea de comunicación con un número excesivo de paquetes., 56

#### **IEEE**

Siglas para definir al Instituto de Ingenieros Eléctricos y Electrónicos, VI, 19, 24, 25, 26, 27, 28

#### **IP**

Siglas para Protocolo de Internet, 18, 34, 35, 36, 37, 38, 45, 47, 48, 80, 82, 85, 86, 96, 102, 108, 111

#### **IPX**

Siglas para Protocolo de Intercambio de Internet, 18

#### **IRE**

Siglas para definir al Instituto de Ingenieros de Radio, 20

#### **ISO**

Siglas para Organización Internacional de Estandarización, 17, 73, 74

## **L**

#### **LAN**

Siglas en inglés para Red de Área Local, 10, 11, 12, 20, 25, 32, 44, 45, 58

## **L**

### **LLC**

Siglas para referirse a la capa de enlace de datos del modelo OSI, 19

## **M**

### **MAC**

Siglas para definir el Control de Acceso al Medio, 19, 29, 30

### **MAN**

Siglas en inglés para Red de Área Metropolitana, 10, 11

### **Man-in-the-Middle**

Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado, 24

### **Modelo OSI**

Modelo de Interconexión de Sistemas Abiertos, donde se indican las 7 capas de red, 17

### **MPyME's**

Siglas para Micro, Pequeñas y Medianas Empresas, 1, 4

## **N**

### **Netbooks**

Es una categoría de computadora portátil, de bajo costo y dimensiones reducidas, 20

### **No-breaks**

Es un aparato que te regula el voltaje y además de que cuando se vaya el suministro de luz tu pc sigue trabajando por un periodo mínimo., 50

### **Notebooks**

También llamada Computadora portátil o laptop, 20, 23

## **P**

### **PAN**

Siglas en inglés para Red de Área Personal, 10

### **PC**

Siglas de Computadora Personal, 23, 40, 69, 70, 72, 100

### **PCI**

Siglas de Interconexión de Componentes Periféricos, 23, 69, 72

### **PCMCIA**

Acrónimo de Asociación Internacional de Tarjetas de Memorias para Computadoras Personales, 23

### **PDA's**

Asistentes Digitales personales, 26



**Portabilidad**

Es la capacidad que tienen los equipos inalámbricos para moverse sin perder la conexión de una red, 20

**Proxy**

Un proxy, o servidor proxy, en una red informática, es un servidor (programa o dispositivo), que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor., 45, 47, 48, 57, 58, 106, 111

**R****Repetidores**

Dispositivos de red que se encargan de repetir una señal para poder seguir transmitiendo el flujo de datos en una red, 13, 14, 16

**Rogue AP**

Es un Punto de Acceso que tiene por objetivo que los usuarios se conecten a él para, capturar su tráfico y con ello, sus credenciales, 24

**Router**

Es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes, 22, 30, 69, 72, 163

**S****Sistemas DSS**

Sistema de Soporte de Decisiones, 25

**Sitios web**

Un sitio web es un conjunto de páginas web desarrolladas en código html, relacionadas a un dominio de Internet el cual se puede visualizar en la World Wide Web (www) mediante los navegadores web., 46, 60

**Smurf Attack**

Tipo de ataque Dos que se basa en el uso de servidores de difusión con el objetivo de paralizar una red., 56

**Software**

Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas., 2, 6, 8, 34, 37, 39, 44, 45, 49, 50, 51, 58, 59, 60, 72

**Software libre**

Es el aquel Software que respeta las libertades del usuario para ejecutar, copiar, distribuir, estudiar, modificar y mejorarlo, 2, 6, 8, 58, 59, 72

**SYN Flood Attacks**

Es una forma de ataque de denegación de servicio en el que un atacante envía una secuencia de solicitudes SYN a un sistema de destino en un intento de consumir suficientes recursos de servidor para hacer que el sistema deje de responder al tráfico legítimo., 56

**T****Topología**

Forma física o lógica de interconectar y transmitir datos en una red, 12, 13, 14, 15, 16, 38, 40

**Topología bus**

Es una red donde se utiliza un solo cable que recorre desde un extremo al otro la red, 13

#### **Tramas**

Son series de bits, organizados en forma cíclica, que transportan información y que permiten en la recepción extraer esta información, 15, 19, 25, 30

## **U**

#### **URL**

Es una sigla del idioma inglés correspondiente a Uniform Resource Locator (Localizador Uniforme de Recursos). Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados., 60, 107, 109

## **W**

#### **WAN**

Siglas en inglés para Red de Área Amplia, 5, 10, 12

#### **Wardriving**

Se le llama wardriving a la búsqueda de redes inalámbricas desde un vehículo en movimiento, 24

#### **WEP**

Acrónimo de Wired Equivalent Privacy o Privacidad equivalente a Cableado y es el método utilizado para asegurar la privacidad en el estándar IEEE 802.11 o Wi-Fi, 24

#### **Wi-Fi**

Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, 21, 24, 25, 26, 29, 69

#### **Wireless**

Término utilizado para describir las telecomunicaciones en las cuales las ondas electromagnéticas llevan la señal y se comparte la información, 25, 82

#### **WLAN**

Acrónimo para Red de Área Local Inalámbrica, 25, 26

#### **WPA**

Acrónimo de Acceso Wi-Fi Protegido, es un sistema para proteger las redes inalámbricas, 24, 25

## REFERENCIAS BIBLIOGRÁFICAS.

Bornhager, M. (2012). Router and Routing Basics. En Cisco Systems Networking Academy.

Hallberg, B. A. (2014). Networking A Beginner's Guide (6° ed.). United States of America: McGraw-Hill.

Stallings, W. (2010). Comunicaciones y Redes de Computadores (7° ed.). Madrid: Pearson.

Stallings, W. (2011). Network Security Essentials: Applications And Standards (4 ed.). New York: Prentice Hall.

Tanenbaum, A. S., & J. Wetherall, D. (2012). Redes de computadoras. México: Pearson Educación.

Salvetti, D. (2011). Redes Wireless (2011 ed.). Buenos Aires: Fox Andina.

## REFERENCIAS VIRTUALES.

ORACLE. (2010). <http://www.oracle.com>. Recuperado el 4 de 12 de 2015, de <https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0re/index.html>

(s.f.). Obtenido de IEEE Advancing Technology for Humanity SECCION MEXICO: [http://www.ieee.org.mx/IEEE/IEEE\\_Seccion\\_Mexico\\_-\\_Historia.html](http://www.ieee.org.mx/IEEE/IEEE_Seccion_Mexico_-_Historia.html)

Free Software Foundation, I. (05 de 09 de 2015). <http://www.gnu.org>. Recuperado el 17 de 12 de 2015, de <http://www.gnu.org/philosophy/free-sw.es.html>

HP TECH SOLUTIONS. (28 de 12 de 2015). Obtenido de [http://www.actiweb.es/hptechsolutions/antenas\\_wifi.html](http://www.actiweb.es/hptechsolutions/antenas_wifi.html)

INEGI. (2014). <http://www.inegi.org.mx>. Recuperado el 4 de 12 de 2015

kaspersky Latam. (5 de 2 de 2016). Obtenido de <http://latam.kaspersky.com/mx/internet-security-center/definitions/web-filter>

kerchak. (16 de 2 de 2016). Obtenido de <http://kerchak.com/ventajas-de-la-tecnologia-bluetooth/>

Larousse. (28 de 12 de 2015). Obtenido de <http://www.larousse.mx/resultados/>

Microsoft. (20 de 1 de 2016). <http://windows.microsoft.com>. Obtenido de <http://windows.microsoft.com/es-xl/windows/what-is-firewall#1TC=windows-7>

Seguridad Wireless. (16 de 2 de 2016). Obtenido de <http://www.seguridadwireless.net/hwagm/modificacion-equipo-wifi.html>

Tienda Oficial Linksys. (15 de 2 de 2016). Obtenido de <http://www.linksys.com/>

UNAM. (s.f.). <http://redyseguridad.fi-p.unam.mx>. Recuperado el 13 de 12 de 2015, de <http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html>