ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ

MANUEL FÉLIX LÓPEZ

CARRERA DE INFORMÁTICA

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA

TEMA:

SERVIDOR PARA AUTENTICACIÓN EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR

AUTORES:

MARÍA GABRIELA PAZMIÑO PALMA
JOSÉ LUIS PINARGOTE SANTANA

TUTOR:

ING. RAMON JOFFRE MOREIRA PICO, MGTR

CALCETA, NOVIEMBRE 2016

DERECHO DE AUTORÍA

Pazmiño Palma María Gabriela y Pinargote Santana José Luis, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

.....	.....
MARÍA G. PAZMIÑO PALMA	JOSÉ L. PINARGOTE SANTANA

CERTIFICACIÓN DEL TUTOR

Ramón Joffre Moreira Pico certifica haber tutelado la tesis SERVIDOR PARA AUTENTICACIÓN EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR, que ha sido desarrollada por María Gabriela Pazmiño Palma y José Luis Pinargote Santana, previa la obtención del título de Ingeniero en Informática, de acuerdo al REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

.....

ING. RAMÓN JOFFRE MOREIRA PICO, MGTR

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han APROBADO la tesis SERVIDOR PARA AUTENTICACIÓN EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR, que ha sido propuesta, desarrollada y sustentada por María Gabriela Pazmiño Palma y José Luis Pinargote Santana , previa la obtención del título de Ingeniero en Informática, de acuerdo al REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

..... **.....**

ING. MARLON R. NAVIA MENDOZA, MGTR
MIEMBRO

ING. ORLANDO ÁYALA PUYAS, MGTR
MIEMBRO

.....

ING. DANIEL A. MERA MARTINEZ, MGTR
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, que nos abrió las puertas y ofrecernos la oportunidad de ser profesionales de calidad.

A la Ing. Jessica Morales por brindarnos sus conocimientos impartidos en clases.

Al tutor Ing.Mg. Joffre Moreira por guiarnos y brindarnos su apoyo en el desarrollo de nuestra tesis.

A nuestros familiares que siempre han estado presentes a lo largo de nuestra vida estudiantil.

Los autores

DEDICATORIA

A Dios por estar presente en mi camino y darme fortaleza para seguir adelante en mis estudios Universitarios.

A mis padres por brindarme su apoyo incondicional durante todo mi proceso de estudio y guiarme en los buenos y malos momentos.

A mi esposo por apoyarme a seguir con mis estudios universitarios y estar ahí siempre en cualquier situación que se me presente.

A mis suegros por ayudarme durante este proceso de desarrollo de tesis acogiéndome como una hija.

A mis hermanos ya que sin su apoyo incondicional y ejemplo de perseverancia no hubiera podido alcanzar las metas propuestas a lo largo de este duro trayecto como lo es el estudio universitario.

A mis familiares en general que me apoyaron moralmente para que pueda seguir adelante.

.....
MARÍA G. PAZMIÑO PALMA

DEDICATORIA

A Dios por darme la fortaleza y sabiduría necesaria para cumplir con mis objetivos y culminar mis estudios universitarios satisfactoriamente.

A mis padres por estar siempre apoyándome en cada momento de mi vida y guiarme por un buen camino.

A todos mis familiares por compartir grandes momentos y estar en solidaridad en los momentos de dificultad.

.....
JOSÉ L. PINARGOTE SANTANA

CONTENIDO GENERAL

CARÁTULA i
DERECHO DE AUTORÍA ii
CERTIFICACIÓN DEL TUTOR iii
APROBACIÓN DEL TRIBUNAL iv
AGRADECIMIENTO v
DEDICATORIA vi
DEDICATORIA vii
CONTENIDO GENERAL viii
CONTENIDO DE CUADROS Y FIGURAS xii
FIGURAS: xii
CUADROS: xiii
RESUMEN xiv
PALABRAS CLAVES xiv
ABSTRACT xv
KEY WORDS xv
CAPÍTULO I. ANTECEDENTES 1
1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA 1
1.2. JUSTIFICACIÓN 2
1.3. OBJETIVOS 4
1.3.1. OBJETIVO GENERAL 4
1.3.2. OBJETIVOS ESPECÍFICOS 4
1.4. IDEAS A DEFENDER 4
CAPÍTULO II. MARCO TEÓRICO 5
2.1. REDES DE INFORMÁTICAS 5
2.1.1. CLASIFICACIÓN DE LAS REDES DE COMUNICACIÓN 5

2.1.1.1. REDES DE ÁREA PERSONAL 5
2.1.1.2. REDES DE ÁREA LOCAL 6
2.1.1.3. REDES DE ÁREA METROPOLITANA 6
2.1.1.4. REDES DE ÁREA AMPLIA 7
2.1.2. MEDIO TRANSMISIÓN DE LAS REDES 7
2.1.2.1. GUIADOS 8
2.1.2.1.1. PAR TRENZADO 8
2.1.2.1.2. COAXIAL 10
2.1.2.1.3. FIBRA ÓPTICA 10
2.1.2.2. NO GUIADOS 11
2.1.2.2.1. ONDAS DE RADIOS 12
2.1.2.2.2. MICROONDAS 12
2.1.2.2.3. INFRARROJO 12
2.1.3. TOPOLOGÍAS DE RED 13
2.1.3.1. TOPOLOGÍA FÍSICA 13
2.1.3.2. TOPOLOGÍA LÓGICA 15
2.2. SISTEMAS OPERATIVOS 15
2.2.1. DISTRIBUCIONES DE LINUX 16
2.2.1.1. DEBIAN 17
2.2.1.2. UBUNTU 17
2.2.1.3. LINUX MINT 18
2.2.1.4. KALI LINUX 18
2.2.1.5. FEDORA 18
2.2.1.6. RED HAT ENTERPRISE LINUX 18
2.2.1.7. OPENSUSE 19
2.2.1.8. CENTOS 19
2.2.1.9. ARCH LINUX 19

2.2.2. DISTRIBUCIONES FREEBSD 19
2.2.2.1. PFSENSE 20
2.3. SEGURIDAD INFORMÁTICA 20
2.3.1. CRIPTOGRAFÍA 21
2.3.1.1. ALGORITMO DE CLAVE SIMÉTRICA 21
2.3.1.2. ALGORITMO DE CLAVE ASIMÉTRICA 22
2.3.2. HERRAMIENTAS DE SEGURIDAD 24
2.3.2.1. SNIFFER 24
2.3.2.1.1. TIPOS DE SNIFFERS 24
2.3.2.2. NMAP 26
2.3.3. SERVIDOR RADIUS 26
2.3.3.1. FASES DEL SERVIDOR RADIUS 27
2.3.3.1.1. FASE DE AUTENTICACIÓN 27
2.3.3.1.2. FASE DE AUTORIZACIÓN 28
2.3.3.1.3. FASE DE AUDITORÍA 28
2.3.3.2. AUTENTICACIÓN BASADA EN PUERTO 802.1X 29
2.3.3.3. AUTENTIFICACIÓN HOTSPOT 30
2.4. METODOLOGÍA PPDIOO 30
2.4.1. PREPARAR 31
2.4.2. PLANIFICAR 31
2.4.3. DISEÑAR 32
2.4.4. IMPLEMENTAR 32
2.4.5. OPERAR 32
2.4.6. OPTIMIZAR 33
CAPÍTULO III. DESARROLLO METODOLÓGICO 34
3.1. METODOLOGÍA PPDIOO 34
3.1.1. FASE DE PLANIFICACIÓN 34

3.1.2. FASE DE DISEÑO 35
3.1.3. FASE DE IMPLEMENTACIÓN 36
3.1.4. FASE DE OPERACIÓN 37
3.1.5. FASE DE OPTIMIZACIÓN 38
CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 40
RESULTADOS 40
DISCUSIÓN 55
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 56
CONCLUSIONES 56
RECOMENDACIONES 57
BIBLIOGRAFÍA 58
ANEXOS 64

CONTENIDO DE CUADROS Y FIGURAS

FIGURAS:

Figura: 02.01. Cables de par trenzado 9
Figura: 02.02. Topología de bus..... 13
Figura: 02.03. Topología anillo 14
Figura: 02.04. Topología estrella..... 14
Figura: 02.05. Proceso de autenticación y autorización del servidor RADIUS. 30
Figura: 03.01. Servicios instalados..... 36
Figura: 03.02. Servicios inicializados en el servidor. 37
Figura: 03.03. Interfaces de red levantadas. 37
Figura: 03.04. Recursos del servidor..... 38
Figura: 04.01. Diagrama de red del GAD Municipal del Cantón Bolívar..... 40
Figura: 04.02. Análisis del tráfico en general..... 41
Figura: 04.03. Análisis del tráfico TCP 42
Figura: 04.04. Análisis del tráfico HTTP, HTTPS 42
Figura: 04.05. Escaneo de la red informática del GAD Bolívar 43
Figura: 04.06. Escaneo de la red informática del GAD Bolívar con detalles de los puertos abiertos..... 43
Figura: 04.07. Test de velocidad del ancho de banda..... 44
Figura: 04.08. Topología del servidor RADIUS en la red privada. 45
Figura: 04.09. Diagrama de red propuesta para el servidor del control de acceso privado. 45
Figura: 04.10. Diagrama de red propuesta para el servidor del control de acceso público y biblioteca. 46
Figura: 04.11. Configuración DHCP. 46
Figura: 04.12. Usuarios para la autenticación RADIUS en la red privada del GAD Bolívar 47
Figura: 04.13. Lista de filtrado de páginas web 47
Figura: 04.14. Reglas de firewall 48
Figura: 04.15. Autenticación RADIUS por medio del portal cautivo (hostpot). 48
Figura: 04.16. Autenticación RADIUS, usuario incorrecto. 49
Figura: 04.17. Portal cautivo servidor de acceso público. 49

Figura: 04.18. Test de comprobación del servidor RADIUS. 50
Figura: 04.19. Filtro de navegación del proxy..... 50
Figura: 04.20. Control de ancho de banda LAN privada. 51
Figura: 04.21. Control de ancho de banda LAN público LAN biblioteca. 52
Figura: 04.22. Consumo de ancho de banda en la red privada. 52
Figura: 04.23. Consumo de ancho de banda en periodo semanal 53
Figura: 04.24. Test de velocidad, usuario de la red de acceso privado 53
Figura: 04.25. Test de velocidad, usuario de la red de acceso público 54

CUADROS:

Cuadro: 03.01. Característica de hardware de los servidores instalado. 36
Cuadro: 03.02. Distribución de ancho de banda del GAD Municipal del Cantón Bolívar. 39

RESUMEN

Este trabajo tuvo como objetivo implementar un método de autenticación que restrinja el acceso a usuarios no autorizados en la red inalámbrica y cableada del GAD Municipal del Cantón Bolívar, permitiendo fortalecer y mejorar el desempeño de la intranet, se organizaron los recursos existentes y controlando el flujo de información por cada equipo autenticado. Se utilizó el sistema operativo pfSense y los paquetes de instalación freeRADIUS, Squid y SquidGuard que fueron necesarios para gestionar los servicios de la LAN. La metodología que se usó es PPDIOO que es propuesta por Cisco, brindando un enfoque en el desarrollo, diseño e implementación de redes. El principal resultado muestra que al administrar los recursos adecuadamente en base a las prioridades y restricciones de navegación, se logra mejorar la disponibilidad del acceso a internet y evitar el congestionamiento.

PALABRAS CLAVES

Servidor RADIUS, estándar 802.1X, redes de comunicación, autenticación en redes.

ABSTRACT

This study aimed to implement an authentication method that restricts access to unauthorized wireless and wired network GAD Municipal Bolívar Canton users, allowing strengthen and improve the performance of the intranet, existing resources were organized and controlling flow authenticated information for each computer and smartphone. pfSense operating system and the installation packages FreeRADIUS, Squid and SquidGuard were necessary to manage LAN services. The methodology used is PPDIOO that is proposed by Cisco, providing a focus on the development, design and implementation of networks. The main result shows that to properly manage resources based on priorities and constraints navigation is achieved to improve the availability of internet access and avoid congestion.

KEY WORDS

RADIUS server, standard 802.1X, communication networks, authentication

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Las redes cableadas e inalámbricas son parte funcional de una empresa u organización, permitiendo la comunicación entre los dispositivos terminales e interconectándolos en la Internet. A simple vista es una gran ventaja, pero se convierte en una amenaza cuando no hay medidas de seguridad que protejan la información que fluye en la red interna o intranet, lo que sería perjudicial para toda entidad.

Varios son los riesgos que se pueden presentar en las redes cableadas e inalámbricas. Por ejemplo, se podría perpetrar un ataque por conexión cableada de un usuario no autorizado o por la ubicación de un punto AP (Access Point) interceptando la conexión en busca de información confidencial, utilizando métodos de ataques dirigidos que trasgredan a la organización.

En el GAD Municipal del Cantón Bolívar las redes inalámbricas por su naturaleza de cobertura tienen el riesgo de recibir ataques informáticos que podrían vulnerar las seguridades y acceder a información vital de dicha entidad, siendo objeto de posibles fraudes o espionajes corporativos.

Este problema se presenta en redes donde el número de usuarios es generalmente grande y se ve la necesidad de controlar el acceso por métodos de autenticación que permiten gestionar los recursos de la red existentes, para robustecer la seguridad de una organización. De acuerdo a esta problemática los autores del presente proyecto de tesis se plantean la siguiente interrogante:

¿De qué manera reforzar la seguridad y controlar el acceso de los usuarios en la red de computadoras del GAD Municipal del Cantón Bolívar?

1.2. JUSTIFICACIÓN

Toda organización o entidad implementa redes cableadas e inalámbricas para conectarse a la Internet, teniendo en cuenta las vulnerabilidades existente, se debe tomar medidas de seguridad que puedan prevenir ataques informáticos internos o externos que disminuyan los riesgos, protegiendo así la integridad, confiabilidad y disponibilidad de la información.

En el art. 8 de la Ley Orgánica de Educación Superior (LOES, 2010), literal f indica: “Fomentar y ejecutar programas de investigación de carácter científico, tecnológico y pedagógico que coadyuven al mejoramiento y protección del ambiente y promuevan el desarrollo sustentable nacional”. Por ende, el presente proyecto está orientado a brindar mayor seguridad en el proceso de autenticación y hacer un buen uso de los recursos de la red informática.

La Ley Orgánica de telecomunicaciones (LOT, 2015), en el art. 2, explica que esta ley se aplicará a todas las actividades de establecimiento, instalación y explotación de redes; de esta manera tal como expresa el art. 3, se podrá promover y fomentar la convergencia de redes, servicios y equipos. Por otro lado en el capítulo II art. 9 expresa que para el caso de redes inalámbricas se deberán cumplir las políticas y normas de precaución o prevención, para ello los gobiernos autónomos descentralizados, en su normativa local observarán y darán cumplimiento a las normas técnicas que emita la Agencia de Regulación y Control de las Telecomunicaciones así como a las políticas que emita el Ministerio sector de las Telecomunicaciones y de la Sociedad de la Información, favoreciendo el despliegue de las redes.

Es por esta razón que se desea contribuir al GAD Municipal del Cantón Bolívar con la implementación de un servidor que sea adaptable a las necesidades de la infraestructura de la red cableada e inalámbrica, el mismo que sea capaz de controlar el acceso de los usuarios en la intranet, autorizando el uso de los recursos de la LAN y WAN; a través de sistemas de autenticación brindando una solución enfocada a la seguridad de la organización.

El GAD Municipal del Cantón Bolívar, como institución pública, brinda la aceptación de que estudiantes realicen diferentes prácticas pre-profesionales, dando la oportunidad de que los autores de este trabajo apliquen los conocimientos y experiencias en el ámbito laboral y de forma unánime contribuir en la ejecución de proyectos tecnológicos que ayuden a mejorar los procesos en la entidad.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar servidor con autenticación en la red de comunicación de datos del GAD Municipal del Cantón Bolívar para mejorar el rendimiento de seguridad en la entidad.

1.3.2. OBJETIVOS ESPECÍFICOS

- Recolectar información de la red del GAD Municipal del Cantón Bolívar.
- Desarrollar un modelo de implementación del servidor RADIUS.
- Instalar el servidor RADIUS con la configuración adecuada.
- Comprobar el correcto funcionamiento de autenticación, autorización y acceso del servidor RADIUS.

1.4. IDEAS A DEFENDER

La implementación de un servidor RADIUS mejorará la seguridad y administración en la red cableada e inalámbrica del GAD Municipal del Cantón Bolívar.

CAPÍTULO II. MARCO TEÓRICO

2.1. REDES DE INFORMÁTICAS

Según Pérez y De los Cobos (2010) indica, que las redes informáticas son parte fundamental de la comunicación, una red se compone de un conjunto de nodos emisores receptores de información, conectados por enlaces que permiten la transmisión de datos unidireccional, bidireccional o multidireccional. Hoy en día las redes de computadoras son el conjunto de dispositivos terminales interconectados entre sí con el objetivo de compartir recursos (disco duro, impresoras, entre otros) y acceder a la información con la mayor velocidad posible.

Las redes de computadoras de alta velocidad son un tema que ha sido ampliamente estudiado y conseguido en la literatura durante las últimas dos décadas, constituyendo una opinión generalizada el hecho de que su comportamiento dinámico debe ser cuidadosamente atendido en los análisis de rendimiento y control. (Naveas y Urrutia, 2013).

2.1.1. CLASIFICACIÓN DE LAS REDES DE COMUNICACIÓN

2.1.1.1. REDES DE ÁREA PERSONAL

El alcance de red es más restringido, centrada en el usuario, designa una interconexión en un espacio local. Otros nombres de este tipo de red son; red individual y red doméstica (Dordoigne, 2011).

Los argumentos expuestos por Márquez (2011) demuestran que, en los últimos años, las redes inalámbricas se han desarrollado de una manera acelerada, esto ha animado en las instituciones un interés por su estudio debido a su creciente complejidad y su uso masivo en cualquier ámbito tecnológico para cumplir con sus necesidades como entidad.

2.1.1.2. REDES DE ÁREA LOCAL

Tanenbaum y Wetherall (2012) indica que las Local Area Network (LAN), o por su traducción al español Redes de Área Local, son el tipo de red más extendido, utilizándose primordialmente para el intercambio de datos y recursos entre las computadoras ubicadas en un espacio relativamente pequeño, como un edificio o un grupo de ellos, como por ejemplo instituciones educativas o gubernamentales y hasta en nuestra propia casa. Henríquez (2013) determina que este tipo de red se interconecta una serie de computadoras y dispositivos periféricos en un área de hasta 200 m., pudiendo llegar a 1 Km de distancia con el uso de repetidoras. Considera tanto el software como el hardware para la conexión de los dispositivos y el tratamiento de la información que transmite. Cuando se integran a esta red soluciones inalámbricas hablamos de una WLAN (Wireless LAN).

2.1.1.3. REDES DE ÁREA METROPOLITANA

MAN o Metropolitan Area Network, cuya traducción al castellano es Red de Área Metropolitana, es una red de datos diseñada específicamente para ser utilizada en ámbitos de ciudades o pueblos. La primera característica, hablando en términos de cobertura geográfica, es que las Redes de Área Metropolitana o MAN son más grandes que las redes de área local o LAN, pero menores en alcance geográfico que las redes de área amplia (WAN) (Tanenbaum y Wetherall, 2012).

De acuerdo a Henríquez (2013) dice que las redes de área metropolitana pueden ser privadas o públicas; permite la integración de voz, datos, video, streaming como funcionalidades estables. Su estructura de transmisión permite llegar a velocidades de hasta 75 Mbps con pares de cobre y hasta 10 Gbps en el caso de fibra óptica. Si bien se basa en la misma tecnología de una LAN.

2.1.1.4. REDES DE ÁREA AMPLIA

La llamada Red de Área Amplia, o WAN (Wide Area Network) como también se la conoce es básicamente una o más redes LAN interconectadas entre sí para poder abarcar mucho más territorio, incluso ciudades o continentes. Las redes WAN son mayormente utilizadas por grandes compañías para su propio uso, mientras que otras WAN son utilizadas por ISP para ofrecerle el servicio de Internet a su clientela. Las computadoras conectadas a través de una Red de Área Amplia o WAN generalmente se encuentran conectados a través de redes públicas tales como el sistema telefónico, sin embargo también pueden valerse de satélites y otros mecanismos (Tanenbaum y Wetherall, 2012).

Gómez (2012) menciona, que las redes de área amplia son redes informáticas que se extienden sobre un área geográfica extensa utilizando medios como: satélites, cables interoceánicos, Internet, fibras ópticas públicas, etc.

2.1.2. MEDIO TRANSMISIÓN DE LAS REDES

Los medios de transmisión son parte fundamental de las redes de computo están constituidos por los enlaces que interconectan los diferentes equipos de red a través de ellos transportan la información desde un punto a otro de la propia red (Herrera, 2011).

En lo planteado por Márquez (2011) define, que el rendimiento se puede medir de muchas formas, incluyendo el tiempo de tránsito y de respuesta. El tiempo de tránsito es la cantidad de tiempo necesario para que un mensaje viaje desde un dispositivo al siguiente por la nube. El rendimiento de una red depende de varios factores, incluyendo el número de usuarios, el tipo de medio de transmisión, la capacidad del hardware conectado y la eficiencia del software. El rendimiento se mide a menudo usando dos métricas: ancho de banda y latencia.

2.1.2.1. GUIADOS

De acuerdo a Rojo (2012) menciona, que los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de llevar diferentes tecnologías de nivel de enlace. La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto.

Ramírez (2012) indica que los medios guiados son aquellos que utilizan un medio sólido para la transmisión de datos. Los cables (medios guiados) transmiten impulsos eléctricos o lumínicos. Los bits se transforman en el adaptador de red y se convierten en señales eléctricas o lumínicas específicas que están determinadas por el protocolo que implemente esa red. Dentro de los medios guiados tienen 3 categorías: Par trenzado, coaxial y fibra óptica que se detallan a continuación:

2.1.2.1.1. PAR TRENZADO

Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital y su ancho de banda depende del calibre del alambre y de su longitud (Figura 02.01). Debido a su bajo costo y buen comportamiento, los pares trenzados son adecuados para una red local que tenga pocos nodos, un presupuesto limitado y una conectividad simple. En cambio, en distancias largas y a altas velocidades, el cable de par trenzado no garantiza una total integridad de los datos transmitidos (Amezaga, 2013)

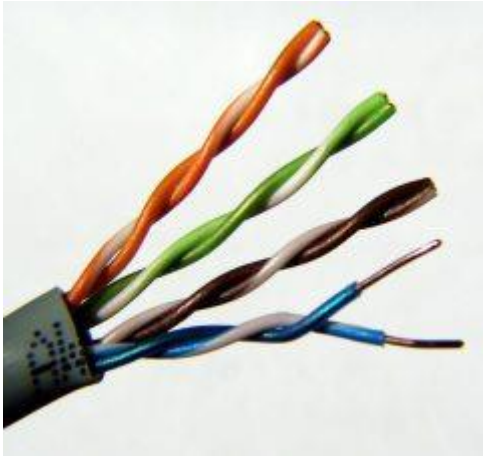


Figura: 02.01. Cables de par trenzado
Fuente: Amezaga (2013)

Ramírez (2012) manifiesta, que este cable consiste en pares de hilos trenzados y recubiertos de una capa aislante externa. Es de fácil instalación y ofrece cierta protección contra las interferencias externas. Puede estar apantallado (STP) o sin apantallar (UTP). Los conectores que se utilizan son los denominados RJ45.

En función de sus características se pueden clasificar en cuatro categorías:

- **Categoría 3. -** Se utiliza para transmitir datos con una velocidad de transmisión de hasta 10 Mbps hasta una longitud máxima de red de 500 m y una frecuencia superior de 16 MHz.

- **Categoría 5:** Se utiliza para transmitir datos con una velocidad de transmisión de hasta 100 Mbps hasta una longitud máxima de red de 700 m y una frecuencia superior de 100 MHz.

- **Categoría 6:** Se utiliza para transmitir datos con una velocidad de transmisión de hasta 1.000 Mbps y una frecuencia superior de 250 MHz. Es el más utilizado actualmente.

- **Categoría 7:** Es un estándar propuesto para transmitir datos con una velocidad de transmisión de hasta 1.000 Mbps y una frecuencia superior de 600 MHz. Su conector RJ45 será distinto a los utilizados actualmente.

2.1.2.1.2. COAXIAL

Ramírez (2012) manifiesta que el cable coaxial está formado por un hilo conductor central rodeado de un material aislante que, a su vez, está rodeado por una malla fina de hilos de cobre o aluminio o una malla fina cilíndrica. Todo ello está rodeado por un aislamiento que le sirve de protección para reducir las emisiones eléctricas. Se usa normalmente para datos y para los sistemas de antenas colectivas de televisión.

Los cables coaxiales para redes de datos usan frecuentemente conectores en T y terminadores. El terminador es necesario en las topologías de bus donde hay un cable principal que actúa de troncal con ramas a varios dispositivos pero que en sí misma no termina en un dispositivo, si el cable principal se deja sin terminar, cualquier señal que se transmita sobre él generará un eco que rebota hacia atrás e interfiere con la señal original. El terminador absorbe la onda al final del cable y elimina el eco de vuelta (Rojo, 2012).

2.1.2.1.3. FIBRA ÓPTICA

Amezaga (2013) define, que está siendo muy usada últimamente como medio de transmisión en las redes de telecomunicaciones debido a sus ventajas sobre el resto. Permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y muy superiores a las de cable convencional. Es un medio de transmisión muy bueno, ya que este cable es inmune a las interferencias electromagnéticas, también se utiliza para redes locales y para redes interurbanas, debido a la baja atenuación que tienen.

De acuerdo con Ramírez (2012) la fibra óptica está formado por fibras de vidrio (o plástico). Cada filamento tiene un núcleo central de fibra de vidrio con un alto

índice de refracción que está rodeado de una capa de material similar pero con un índice de refracción menor. De esa manera aísla las fibras y evita que se produzcan interferencias entre los elementos contiguos a la vez que protege el núcleo. Todo el conjunto está protegido por otras capas aislantes y absorbentes de luz. Los cables de fibra óptica pueden transmitir la luz de tres formas diferentes: Monomodo, Multimodo, Multimodo de índice Gradual.

- **Monomodo:** En este caso, la fibra es tan delgada que la luz se transmite en línea recta. El núcleo tiene un radio de 10 **μm** y la cubierta, de 125 **μm**.

- **Multimodo:** La luz se transmite por el interior del núcleo incidiendo sobre su superficie interna, como si se tratara de un espejo. Las pérdidas de luz en este caso también son prácticamente nulas. El núcleo tiene un diámetro de 100 **μm** y la cubierta, de 140 **μm**

- **Multimodo de índice gradual:** La luz se propaga por el núcleo mediante una refracción gradual. Esto se debe a que el núcleo se construye con un índice de refracción que va en aumento desde el centro a los extremos. Suele tener el mismo diámetro que las fibras multimodo.

2.1.2.2. NO GUIADOS

Según Dordoigne (2011) indica, que en los medios no guiados la tecnología de red inalámbrica aún no está lista para sustituir a los soportes limitados, debido, sobre todo, al pequeño ancho de banda, pero aun así es un buen complemento. Estas tecnologías se encuentran en todos los ámbitos de la red también permiten la movilidad de los usuarios, en el interior de las oficinas o lugares de trabajo o en el exterior. También conocidos como comunicación sin cable, transporta ondas electromagnéticas sin usar un conductor físico. En su lugar, las señales se radian a través del aire (o en unos pocos casos el agua) y, por lo tanto, están disponibles para cualquiera que tenga un dispositivo capaz de aceptarla.

Los medios no guiados se basan en la propagación de ondas electromagnéticas por el espacio. Una radiación electromagnética tiene una naturaleza dual, como onda y como corpúsculo, y su comportamiento dependerá de las características ondulatorias de la radiación, especialmente de la longitud de onda (Ramírez, 2012).

2.1.2.2.1. ONDAS DE RADIOS

Ramírez (2012) dice que son ondas electromagnéticas cuya longitud de onda es superior a los 30 cm. Son capaces de recorrer grandes distancias y pueden atravesar materiales sólidos, como paredes o edificios. Se propagan en todas las direcciones (ondas multidireccionales). Su mayor problema son las interferencias entre usuarios. Estas ondas son las que emplean las redes Wi-Fi, Home RF o Bluetooth. Son las más usadas, pero tienen apenas un rango de ancho de banda entre 3 Khz y los 300 Ghz. Son poco precisas y solo son usados por determinadas redes de datos o los infrarrojos.

2.1.2.2.2. MICROONDAS

Se basan en la transmisión de ondas electromagnéticas cuya longitud de onda varía entre 30 cm y un milímetro. Estas ondas viajan en línea recta, por lo que el emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Km de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles (Ramírez, 2012).

2.1.2.2.3. INFRARROJO

Son ondas electromagnéticas (longitud de onda entre 1 mm y 750 mm) direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia. Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología:

resultan muy cómodas para ordenadores portátiles. Sin embargo, no se consiguen altas velocidades de transmisión (Bernal, 2012).

2.1.3. TOPOLOGÍAS DE RED

Pech (2013) indica, que el objetivo de estas topologías es buscar la forma más económica y eficaz de conexión, para al mismo tiempo aumentar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión, permitir un mejor control de la red y lograr de forma eficiente el aumento del número de las estaciones de trabajo.

Por otro lado, Torres (2011) dice, que las redes de comunicación están construida mediante una topología física y una topología lógica que se explican a continuación:

2.1.3.1. TOPOLOGÍA FÍSICA

De acuerdo con Torres (2011) explica que una topología física se refiere a la distribución de los puntos finales y los cables conectados y según de Zayas y Sao (2002) Existen cuatro principales topologías físicas las cuales son las siguientes:

- **Bus:** Es la forma más simple, de dar servicio a todos y cada uno de los terminales. En caso de que un nodo falle, una parte de la red queda sin servicio. Suele emplearse cable coaxial, y el ejemplo más típico lo constituyen las redes Ethernet (Figura 02.02).

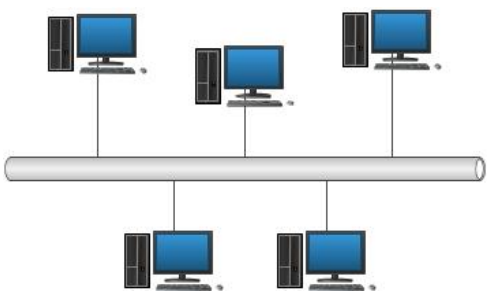


Figura: 02.02. Topología de bus

Fuente: Los Autores (2016).

- **Anillo:** Es una variante de la anterior, en la que el tendido se cierra sobre sí mismo, por lo que en caso de su rotura se puede acceder a las estaciones aisladas por el otro lado del anillo. En la práctica, la mayoría de las topologías en anillo (lógica) terminan en una estrella física. Pueden emplearse cables de pares, coaxiales o la fibra óptica, su ejemplo más significativo de utilización es en las redes Token Ring (Figura 02.03).

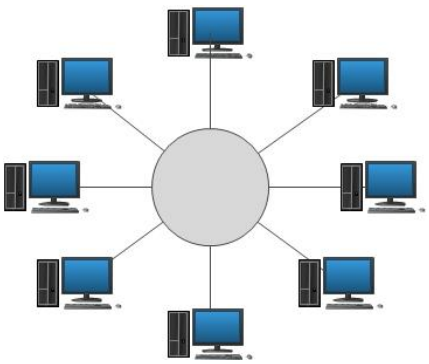


Figura: 02.03. Topología anillo

Fuente: Los Autores (2016).

- **Estrella:** Es aquella en la que un elemento central (Switch o hub) sirve de puente entre todas las terminales de la LAN, ella proporciona la conmutación entre todas. Aísla unos elementos del fallo de otros, pero presenta un punto crítico; el nodo central, que en caso de fallo deja la red sin servicio. El costo del cableado es elevado al requerir conexiones punto a punto para todos los elementos, aunque este se minimiza al emplear cable UTP (Figura 02.04).

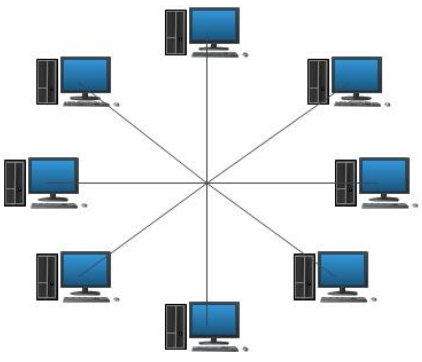


Figura: 02.04. Topología estrella

Fuente: Los Autores (2016).

- **Malla:** Es la topología que presenta un nivel mayor de seguridad. Los nodos de la red se unen entre sí, para formar una estructura en la que al menos existen dos rutas posibles por cada nodo; así en caso de fallo en una de ellas, la información se puede hacer circular por la otra. Resulta muy adecuada para cubrir, por ejemplo, un país completo. Puede resultar inicialmente más cara que las otras, pero si se cuida el diseño y se ajusta la capacidad de los enlaces, este incremento se recompensa con los beneficios.

2.1.3.2. TOPOLOGÍA LÓGICA

Díaz (sf) explica que es la forma de conseguir el funcionamiento de una topología física de una forma eficiente. Existen topologías lógicas definidas:

- **Topología anillo-estrella:** Implementa un anillo a través de una estrella física.

- **Topología bus-estrella:** Implementa una topología en bus a través de una estrella física.

2.2. SISTEMAS OPERATIVOS

Los sistemas operativos para computadoras son herramientas informáticas que controlan lo que el hardware hace, y facilitan el uso de otras aplicaciones y hardware por medio de una interfaz gráfica; es decir, las ventanas y los iconos que utilizamos para acceder a otros programas y a los dispositivos que conectamos a la máquina: cámaras digitales, impresoras, discos duros, entre muchos otros. Los sistemas operativos se han convertido en productos y productores culturales cargados ideológicamente, quizá unos más alternativos que otros, y que generan toda una mitología tanto alrededor del producto como del usuario (López, 2010)

Según Suárez (2012) menciona, que un sistema operativo es el corazón de una computadora, actúa como un conjunto de programas fundamentales que crean la interfaz relativamente uniforme para acceder a la amplia variedad de dispositivos (de entrada/salida, impresoras, cámaras digitales, componentes inalámbricos de la red que permiten la comunicación de las computadoras, etc.) con las que interactúa el usuario, el cual coordina, maneja y controla todos los recursos de una red de computadoras y proporciona la base sobre la cual pueden escribirse los programas de aplicación para lograr un buen rendimiento. El OS coordina la interacción entre el equipo y los programas que están en ejecución. Controla la asignación y utilización de los recursos de hardware tales como:

- Memoria
- Tiempos del CPU
- Espacios en el disco duro
- Dispositivos periféricos

En un entorno de red, los servidores asignan recursos a los clientes de la red y el sistema de red permiten que estos recursos sean coordinados y aprovechados correctamente en el sistema del cliente.

2.2.1. DISTRIBUCIONES DE LINUX

López (2010) fundamenta, que las distribuciones Linux crecen día tras día como fuertes competidores. Pero más que simples ambientes gráficos para el uso más amigable de un ordenador. Además, GNU/Linux, por su parte, no están exentas de una mitología muy clara y definida. Con una filosofía que apunta al bien social y a la comunidad, las distribuciones GNU/Linux, bajo licencia GPL, se presentan como la alternativa, la libertad en un mundo privativo, y son legitimadas por los mismo programadores de software en general que reconocen la estabilidad y las prestaciones de estos programas con la posibilidad de modificarlos y adecuarlos a las necesidades propias

Existe un gran número de distribuciones de los diferentes sistemas operativos Linux. Cada distribución cuenta con sus propias características y supone unas ventajas y unos inconvenientes a los usuarios convencionales. Por ello una de las principales dudas de los usuarios antes de instalar Linux en sus equipos es qué distribución elegir y cuál se adapta mejor a sus conocimientos y a su hardware (Velasco, 2015).

2.2.1.1. DEBIAN

Velasco (2015) se refiere que es una de las distribuciones más puras en cuanto a capacidad de personalización. Esta distribución viene con muy pocos paquetes instalados (los necesarios, principalmente), lo que permite una mayor personalización por parte de los usuarios y un mayor rendimiento, sin embargo, puede resultar algo más complicada de utilizar para los usuarios sin demasiada experiencia.

2.2.1.2. UBUNTU

Es el sistema operativo Linux más utilizado de toda la red basado en Debian. Con un escritorio apoyado en Unity (no querido por todos), este sistema operativo es ideal para aquellos que buscan un sistema seguro, estable y fácil de utilizar. Ubuntu cuenta con una gran comunidad en la red, por lo que ante cualquier problema fácilmente se encuentran soluciones (Velasco, 2015).

Esta “distribuciones es de las más populares, con un aproximado de 8 millones de usuarios activos para el 2008; su estabilidad y fácil manejo e instalación la han convertido en una de las opciones favoritas incluso para usuarios con conocimientos en informática. Sin embargo, en su búsqueda por más usuarios, esta compañía ha facilitado el uso de aplicaciones y de formatos privativos, según ellos, para facilitar la transición de Windows a Ubuntu. (López, 2010)

2.2.1.3. LINUX MINT

Esta distribución está basada en Ubuntu, aunque aporta una serie de características interesantes (nuevas aplicaciones, un nuevo escritorio para aquellos a quienes no les guste Unity, nuevos ajustes, etc). Una gran alternativa a Ubuntu que poco a poco va ganando una considerable cuota de mercado entre los usuarios (Velasco, 2015).

2.2.1.4. KALI LINUX

Es una distribución basada en Debian diseñada para auditar redes y buscar vulnerabilidades en los sistemas de estas. Cuenta por defecto con un gran número de herramientas pre-instaladas para esta función de manera que los usuarios puedan utilizarla en modo Live sin necesidad de instalar ningún tipo de software adicional (Velasco, 2015).

2.2.1.5. FEDORA

Este sistema operativo ha sido creado y mantenido por la compañía Red Hat. Fedora es diferente a otras distribuciones similares como Debian al utilizar otro gestor de paquetes y disponer así de sus propias aplicaciones compiladas para este sistema y no siendo compatibles, por ejemplo, los paquetes de Debian (o Ubuntu) con él. Pese a ello es una alternativa a tener en cuenta, especialmente para aquellos que buscan “algo diferente a Debian” (Velasco, 2015).

2.2.1.6. RED HAT ENTERPRISE LINUX

Distribución comercial de Linux desarrollada por Red Hat. Ofrece una estabilidad y flexibilidad punteras, lo que la coloca como una de las más recomendadas para empresas y servidores (López, 2014).

2.2.1.7. OPENSUSE

López (2014) explica que una de las alternativas más potente contra la familia de distribuciones basadas en Debian. Está disponible con los entornos de escritorio KDE y Gnome, y cuenta como una de sus mejores armas con la robusta herramienta de instalación y configuración YaST y el configurador gráfico SaX.

2.2.1.8. CENTOS

Nació como un derivado gratuito de la distribución comercial Red Hat Enterprise Linux (RHEL) destinada al uso empresarial. Recientemente unió las fuerzas con el propio Red Hat, y sigue siendo una apuesta segura para los que busquen un código de gran calidad (López, 2014).

2.2.1.9. ARCH LINUX

Una distribución modular en la que empiezas desde cero y tienes que ir añadiéndole los componentes que quieras. No es muy apta para principiante, y utiliza pacman, su propio gestor de paquetes. Se trata de una Rolling Release, lo que quiere decir que todos sus componentes van actualizándose sin necesidad de instalar versiones nuevas del sistema operativo (López, 2014).

2.2.2. DISTRIBUCIONES FREEBSD

BSD son las siglas de “Berkeley Software Distribution”. Así se llamó a las distribuciones de código fuente que se hicieron en la Universidad de Berkeley en California y que en origen eran extensiones del sistema operativo UNIX de AT&T Research. Varios proyectos de sistemas operativos de código abierto tienen su origen en una distribución de éste código conocida como 4.4BSD-Lite. Añaden además un buen número de paquetes de otros proyectos de Código Abierto, incluyendo de forma destacada al proyecto GNU (BSD, 2013).

2.2.2.1. PFSENSE

Zambrano *et al.,* (2015), explica que pfSense es una distribución libre, de código abierto personalizada de freeBSD adaptada para su uso como firewall y router, totalmente gestionada a través de interfaz web.

Fuertes *et al.,* (2011), manifiesta que el principal objetivo de pfSense, es disponer de un cortafuego que permita establecer seguridad entre WAN, LAN y la DMZ, permitiendo proteger una red de accesos ilícitos, redirigir paquetes hacia máquinas de la red interna, otorgar accesos solo desde sitios conocidos y además es una distribución de código abierto muy potente que puede competir con soluciones comerciales. Se considera como el sistema operativo que va servir como base para la implementación del servidor de autenticación del GAD Municipal del Cantón Bolívar.

2.3. SEGURIDAD INFORMÁTICA

La seguridad informática de las tecnologías y de los sistemas de información se ha convertido en un factor clave para el éxito y la rentabilidad de las organizaciones. En los actuales momentos, la seguridad informática es un tema de dominio obligado para cualquier usuario de internet que no esté dispuesto a que su información sea vulnerada. Aunque a simple vista se puede entender que "riesgo" y "vulnerabilidad" se pueden englobar en un mismo concepto, una definición más precisa es que "vulnerabilidad" está ligada a una amenaza y "riesgo" se refiere a un impacto (Villegas, *et al.,* 2011).

Díaz, *et al.,* (2014) indica que proteger la información y los recursos tecnológicos informáticos es una tarea continúa y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades.

Las redes informáticas, y entre ellas el internet son unos de los mayores peligros que existen en la seguridad de un sistema informático. Actualmente la mayoría de ataques y amenazas vienen desde el exterior, a través de la red. Una gran vulnerabilidad en las redes LAN es el uso de puntos inalámbricos que son vulnerado constantemente ya que la información viaja en al aire y cualquier persona mal intencionada puede esnifar los datos (García, 2012).

2.3.1. CRIPTOGRAFÍA

La Criptografía es la ciencia que se encarga del estudio de técnicas para transformar la información a una forma que no pueda entenderse a simple vista; sin embargo, el objetivo de la Criptografía no es sólo mantener los datos secretos, sino también protegerlos contra modificación y comprobar la fuente de los mismos (UNAM, 2012a).

Sanjuan (2012) explica que la criptografía es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: criptografía y criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar; es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis se ocupa de romper esos procedimientos para así recuperar la información. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente.

2.3.1.1. ALGORITMO DE CLAVE SIMÉTRICA

La criptografía simétrica y la criptografía asimétrica se establecieron con el propósito de ofrecer mayor seguridad y aumentar la privacidad, la integridad, y la disponibilidad de los recursos informáticos por métodos de autenticación (Cáceres *et al.,* 2015).

García *et al.,* (2012) habla de las claves simétricas y los tipos de algoritmo:

Los primeros algoritmo de cifrado utilizado eran simétrico y eran utilizado en la criptografía clásica, es decir que tanto el emisor como el receptor del mensaje utilizan la misma clave lo cual eran métodos inseguros si alguien llegase a descubrir o descifrar la contraseña. Para encriptar la información se hace necesario el uso de algoritmo. Dentro de estos algoritmos se encuentran los siguientes:

- **DES** (Data Encryption Standard) o algoritmo estándar de cifrado. Desarrollado y publicado a mediado de los años setenta. Fue uno de los primeros algoritmo estándares de encriptación, es poco resistente a ataques de fuerza bruta debido a la corta longitud de la clave de 64bits, lo cual 56 bits son de clave de cifrado y 8 bits de paridad.

- **3DES** (Triple Data Encryption Standard). Es una versión más segura del algoritmo DES y que todavía se sigue utilizando, la longitud de la clave es de 192 bits de los cuales 168 bits son de cifrado y 24 bits de pariedad.

- **IDEA** (International Data Encryption Algorithm) o algoritmo internacional de cifrado de datos, surgió como un algoritmo para sustituir a DES; tiene una longitud de 128 bits.

- **AES** (Advanced Encryption Standar) o algoritmo estándar de encriptación avanzada; es un algoritmo de cifrado simétrico que puede proporcionar claves de diferentes longitud como de 128, 192, o 256 bits. Es actualmente el algoritmo más seguro y usado dentro de los cifrados simétricos.

2.3.1.2. ALGORITMO DE CLAVE ASIMÉTRICA

De acuerdo con Mendoza (2008), los algoritmos asimétricos son mucho más seguros que los algoritmos simétricos y se diferencia que estos utilizan dos

claves diferentes, una para cifrar y otra para descifrar. Estas dos claves se encuentran asociadas matemáticamente, cuya característica fundamental es que una clave no puede descifrar lo que cifra.

UNAM (2012b) explica los principales algoritmos asimétricos y sus funcionalidades:

- **RSA** (Rivest Shamir Adleman) Fue desarrollado en el MIT en 1977, es el algoritmo de clave pública más popular en la actualidad utilizada tanto para cifrar texto como para generar firmas digitales. Multiplicando dos números primos, genera un número llamado módulo público el cual es utilizado para conseguir las claves pública y privada, la idea es que los números primos escogidos sean muy grandes ya que factorizar el resultado de multiplicar dos números primos es un problema computacionalmente imposible.

- **DSA** (Digital Signature Algorithm) en 1991 el NIST propuso un estándar para firma digital (Digital Signature Standard, DSS), siendo su algoritmo el DSA, en 1994 este algoritmo fue anunciado formalmente como estándar y debe ser utilizado únicamente para generar firmas digitales. El algoritmo se apoya en el uso de funciones hash y está documentado en el FIPS 186.

- **DH** (Diffie Hellman) se trata de un algoritmo que permite a dos usuarios intercambiar una clave secreta a través de un medio inseguro. En otras palabras, los dos usuarios son capaces de acordar una clave, aun cuando los intercambios previos al acuerdo sean públicos.

2.3.2. HERRAMIENTAS DE SEGURIDAD

2.3.2.1. SNIFFER

Según Nina, (2013) un sniffer es un dispositivo o una aplicación que permite capturar los datos o información que pasan a través de una red, que no precisamente van dirigidos hacia él, por lo tanto es un tráfico de información al que no debería tener acceso. De acuerdo con el criterio de Mateo y Veraguas (2012) se refiere que un sniffer es un software que se encarga de capturar paquetes en tránsito (entrada y salida) en una red para analizarlos; es decir que se puede mirar la información y los protocolos en circulación de la red y obtener datos o información de gran importancia de los segmentos de redes en las que es permitido el acceso. Siendo útil para un administrador de redes observar que todo vaya bien, pero a la vez puede llegar a ser un peligro ya que cualquiera puede utilizar un sniffer y capturar información.

2.3.2.1.1. TIPOS DE SNIFFERS

Según Ledesma *et al.,* (2012) estos son algunos de los sniffers más utilizados:

- **Tcpdump:** Es un analizador de paquetes que corre en modo consola. Posibilita al usuario interceptar y visualizar paquetes TCP/IP, y otros que estén siendo transmitidos o recibidos en una red a la cual la computadora se encuentra conectada. Se distribuye bajo la licencia BSD (Berkeley Software Distribution), siendo un software libre y de código abierto (SLCA). Funciona en la mayoría de los sistemas operativos: Linux, Microsoft Windows, Solaris, BSD, Mac Os X, HP-UX y AIX, entre otros. Emplea la librería Libpcap para capturar paquetes y WinDump para Windows. Se puede utilizar también en el entorno inalámbrico.

- **Wireshark.-** Anteriormente conocido como ethereal, es uno de los analizadores de protocolos más empleado. Captura los paquetes que circulan por la red y muestra el contenido de cada campo con el mayor

nivel de detalle posible. Puede capturar paquetes en redes con diferentes tipos de medios físicos, incluyendo las WLAN. Funciona tanto en modo consola como mediante una interfaz gráfica y contiene muchas opciones de organización y filtrado de información. Wireshark se desarrolla bajo licencia pública general (GNU General Public License) y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac Os X, así como en Microsoft Windows y por eso se considera apropiado para realizar pruebas y analizar el tráfico de la red del Municipio del Cantón Bolívar.

- **Kismet.-** Se emplea como sniffer y como sistema de detección de intrusiones para redes 802.11. Trabaja con tarjetas inalámbricas que soporten modo monitor y puedan servir para monitorizar tráfico 802.11 a/b/g/n. Soporta además una arquitectura de plugins que permite incluir el trabajo con otros protocolos. Identifica las redes recolectando de forma pasiva los paquetes y permitiendo detectar redes escondidas a través de los datos del tráfico. Este programa funciona sobre varios sistemas como Linux, Microsoft Windows, Solaris, BSD y Mac Os X.

- **Ettercap.-** Es un interceptor sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo, aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing, los autores creen posible el uso de esta herramienta en un ambiente controlado para demostrar que la red es susceptible ataques informáticos.

2.3.2.2. NMAP

Lyon (sf) describe a Nmap (mapeador de redes) como una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP en formas individual para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) se ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas de gran importancia y analizar el nivel de seguridad de sus propias instalaciones de forma ética, previniendo futuros ataques.

Nmap es Herramienta de exploración de redes y de sondeo de seguridad, esta herramienta es de código abierto imprescindible para un administrador de red o un auditor de seguridad, fue diseñada para analizar grandes redes usándola para ver los sistemas operativos y sus versiones que se ejecutan (de la Casa, 2014).

2.3.3. SERVIDOR RADIUS

La comunicación entre un servidor de acceso de red (NAS) y el servidor RADIUS se basa en el protocolo de datagrama de usuario (UPD). Generalmente, el protocolo RADIUS se considera un servicio sin conexión. Los problemas relacionados con la disponibilidad de los servidores, la retransmisión y los tiempos de espera son tratados por los dispositivos activados por RADIUS en lugar del protocolo de transmisión (Cisco, 2014).

Egli (2015) alega que RADIUS es un protocolo cliente/servidor, el cliente es típicamente un NAS (Network Access Server) o RAS (Remote Access Sever) y el servidor es generalmente un proceso de daemon que se ejecuta en UNIX o una máquina del Windows NT. El servidor RADIUS recibe las peticiones de

conexión del usuario, realiza la autentificación, y después devuelven la información de la configuración necesaria para que el cliente acceda a los servicios.

2.3.3.1. FASES DEL SERVIDOR RADIUS

Debería existir algún mecanismo mediante el cual un usuario autorizado pueda usar los recursos a los que tiene derecho, dejando a los usuarios no autorizados sin acceso. Éste es el propósito de la autenticación, autorización y auditoría de redes; es decir: diferenciar, asegurar y auditar a los usuarios (Arana *et al.,* 2013).

2.3.3.1.1. FASE DE AUTENTICACIÓN

Según Miñarro (2009) el usuario que desea tener acceso a la red, envía al Cliente RADIUS tanto su nombre de usuario como su clave de acceso empleando un protocolo de autenticación a nivel de enlace PPP (Point to Point Protocol). Una vez que el Cliente RADIUS ha obtenido los datos del usuario final, envía mediante un paquete en 'Access-Request' las credenciales de usuario, información de parámetros de conexión y la identificación del cliente RADIUS por la que está recibiendo la petición de acceso.

Vásquez y Vaca (2015) mencionan que la fase de autenticación es el proceso de mayor relevancia en los sistemas AAA, sirve de base a todo el sistema completo, debido a su directa relación con los procesos de autorización y contabilidad. La autenticación permite comprobar la identidad de un usuario a través de los siguientes elementos: Algo que se conoce, como un número de identificación personal (PIN) o contraseña; algo que se tiene, como una tarjeta ATM o una tarjeta inteligente; algo que identifique físicamente al usuario de forma única, como una huella dactilar, el reconocimiento de voz, escaneo de la retina ocular, etc. Utilizar más de un factor para identificar al usuario y añade credibilidad al proceso de autenticación.

2.3.3.1.2. FASE DE AUTORIZACIÓN

Según Miñarro (2009) explica que cuando esta petición llega al Servidor RADIUS, éste verifica la información recibida en el paquete anterior, el servidor verifica la autentificación si es correcta el cliente accede los servicios de red, en coso de que la autentificación no sea correcta el servidor deniega el acceso al medio. Según Vásquez y Vaca (2015) la fase de autorización es el proceso mediante el cual a un usuario se le asigna una determinada cantidad de recursos o servicios de red, en base a las actividades que realice y las políticas de acceso establecidas por el administrador. Esta obligatoriamente relacionado con el proceso de autenticación, si un usuario no se autentica correctamente los siguientes procesos se descartan. Para cumplir con el proceso de autorización, los sistemas AAA utilizan soluciones como bases de datos o directorios que permiten almacenar las políticas de acceso de cada usuario.

2.3.3.1.3. FASE DE AUDITORÍA

De acuerdo con Miñarro (2009) indica que una vez autentificado el cliente, comienza la fase de Accounting con el envío de un paquete Accounting-Request Start, por parte del Cliente RADIUS hacia el Servidor para indicar que el usuario se encuentra logeado en la red. El servidor contesta a éste con otro mensaje (Accounting-Response) y desde ese momento el usuario está accediendo a los recursos solicitados en la fase anterior. De forma periódica el Cliente RADIUS informa por medio del mensaje (Accounting-Request) que la sesión establecida previamente continua activa y por tanto la dirección IP facilitada sigue en uso. Este mensaje será contestado por el Servidor con un paquete (Accounting-Response). Esta pareja de mensajes se repetirá en función de la duración de la sesión y de la periodicidad con que se envíen los mismos. Una vez que el usuario desea finalizar la sesión establecida, el Cliente RADIUS envía un paquete de Accounting Request Stop. Por último el Servidor responde con un paquete Accounting-Response, liberándose la dirección IP anteriormente asignada, no sin antes proceder por parte del Servidor RADIUS a guardar la información relativa a la sesión que acaba de finalizar: Identificación del usuario, hora de

inicio y final de la sesión del usuario, duración de la conexión, Total de paquetes transferidos durante la sesión tanto transmitidos como recibidos y la causa de la finalización de la sesión.

Vásquez y Vaca (2015) se refieren que una vez realizado el proceso de autenticación y autorización se produce la fase de contabilidad o Acconunting. Esta inicia cuando el equipo autenticador o NAS autoriza al suplicante acceder a los servicios de red. La contabilidad es el proceso estadístico y de recolección de datos sobre la conexión, el buen tratamiento de la información recolectada durante el proceso de autenticación y autorización permite al administrador de la red gestionar la futura demanda de sus sistemas para planificar su crecimiento.

2.3.3.2. AUTENTICACIÓN BASADA EN PUERTO 802.1X

Vásquez y Vaca (2015) se refieren que 802.1X es un estándar de autenticación que permite controlar el acceso a los servicios de red a través de sus puertos, opera en la capa dos del modelo OSI, asegura el intercambio de las credenciales de usuario o dispositivo evitando cualquier acceso no autorizado a la red. Una infraestructura de red 802.1x requiere de tres elementos para operar: suplicante, equipos autenticadores y servidor de autenticación que se detalla a continuación (Figura 02.05).

- **Suplicante:** Es un software que se instala en los clientes del equipo autenticador, utilizado en ambientes cableados e inalámbricos. El suplicante se carga en el dispositivo del usuario y se utiliza para solicitar acceso a la red.

- **Autenticador:** Es el componente a través del cual los usuarios acceden a los servicios de red, se encuentra entre el dispositivo que necesita ser autenticado y el servidor utilizado para realizar la autenticación. Ejemplos de Autenticador son conmutadores de red y puntos de acceso inalámbricos.

- **Servidor de Autenticación:** Es un equipo que recibe mensajes mediante una comunicación RADIUS y utiliza esa información para comprobar la autenticidad del usuario o del dispositivo que intenta acceder a la red, por lo general se emplean bases de datos para realizar este proceso tales como SQL, Microsoft Active Directory, LDAP, etc.

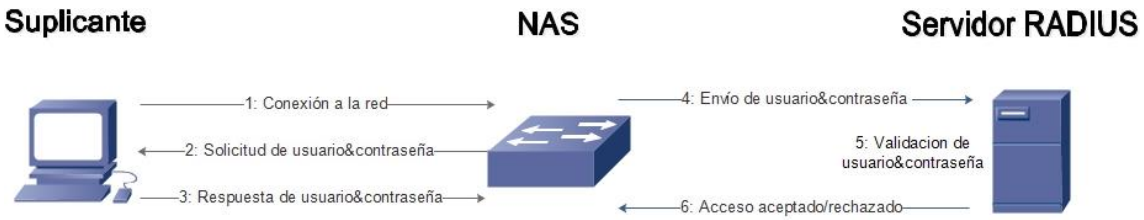


Figura: 02.05. Proceso de autenticación y autorización del servidor RADIUS.

Fuente: Los Autores (2016).

2.3.3.3. AUTENTIFICACIÓN HOTSPOT

La autenticación hotspot o portal cautivo es una función de seguridad de la capa 3 que hace al regulador no permitir el tráfico IP (excepto el DHCP y el DNS) de un cliente en particular hasta que ese cliente haya suministrado correctamente un nombre de usuario y contraseña. Es un método de autenticación simple, que no proporciona el cifrado de los datos, pero si se valida a través de un servidor RADIUS protege la integridad de la información (Cisco, 2014)

2.4. METODOLOGÍA PPDIOO

Tiso (2012) explica que para diseñar una red que satisfaga las necesidades de los clientes; el objetivo de la organización, las limitaciones, objetivo técnico y restricciones técnicas pueden ser identificadas mediante el ciclo de vida que ha propuesto Cisco que comprende seis fases: preparar, planificar, diseñar, implementar, operar y optimizar. No importa el ciclo de vida que se utiliza, siempre y cuando se tome en cuenta que el diseño de la red debe ser realizado en forma planificada, de manera estructurada y modular, en la cual se pueda mejorar o rediseñar la red.

2.4.1. PREPARAR

La fase de preparación es identificar las necesidades del cliente para el diseño o rediseño de una red, incluyendo presupuesto y el cronograma con las actividades detalladas. Establecer los objetivos técnicos y comerciales, así como las limitaciones de diseño. Según Sivasubramanian, *et al.,* (2010) implica el establecimiento de los requisitos de la organización, el desarrollo de una estrategia de red, y proponiendo una arquitectura conceptual de alto nivel de la identificación de tecnologías que pueden apoyar mejor la arquitectura. La fase de preparación puede establecer una justificación financiera para la estrategia de la red mediante la evaluación del caso de negocio para la arquitectura propuesta.

2.4.2. PLANIFICAR

Oppenheimer (2010) indica que los requisitos de la red se identifican en esta fase. Consiste en levantar la información para un análisis de las áreas donde se instalará la red y una identificación de los usuarios que requerirá los servicios de red.

De acuerdo con Sivasubramanian, *et al.,* (2010) indica que esta fase implica la identificación de los requisitos de red iniciales basadas en objetivos, instalaciones, necesidades de los usuarios, y así sucesivamente. La fase de plan implica la caracterización de los sitios y la evaluación de las redes existentes para determinar si la infraestructura del sistema, sitios y el entorno operativo pueden apoyar el sistema propuesto. Un plan de proyecto es útil para ayudar a administrar las tareas, responsabilidades, hitos críticos y los recursos necesarios para implementar cambios en la red. El plan del proyecto debe alinearse con el alcance, costo, y los parámetros de recursos establecidos en los requisitos de negocio originales.

2.4.3. DISEÑAR

En esta fase se plantea un diseño físico como lógico del funcionamiento de la red y la correcta documentación de los detalles técnicos establecidos en la fase de planificación (Oppenheimer, 2010).

Sivasubramanian, *et al.,* (2010) explica que los requisitos iniciales se derivan en la fase de planificación en relación de las actividades para el diseño de la red. Es necesario un diseño detallado integral que cumple con los requisitos técnicos y de negocio actual, e incorpora especificaciones para apoyar la disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento. La especificación de diseño es la base para las actividades de implementación.

2.4.4. IMPLEMENTAR

Oppenheimer (2010) manifiesta que después de la aprobación del diseño, se inicia la implementación. La red está construida de acuerdo con las especificaciones de diseño.

La red se construye o los componentes adicionales se incorporan de acuerdo con las especificaciones de diseño, con el objetivo de integrar dispositivos sin interrumpir la red existente o la creación de puntos de vulnerabilidad (Sivasubramanian, *et al.,* 2010).

2.4.5. OPERAR

Según Oppenheimer (2010) dice que el funcionamiento es la prueba definitiva de la efectividad del diseño. La red se monitorea durante esta fase para comprobar que todo funcione correctamente y de esta forma administrar los recursos de la red convenientemente.

En relación con Sivasubramanian, *et al.,* (2010) determina que la operación es la prueba final de la idoneidad del diseño. La fase operativa implica mantener en

buen funcionamiento la red a través de las operaciones del día a día, incluyendo el mantenimiento de alta disponibilidad y reducir los gastos. El monitoreo de detección de fallos, la corrección, y el rendimiento que se producen en las operaciones diarias proporcionar los datos iniciales de la fase de optimización.

2.4.6. OPTIMIZAR

Sivasubramanian, *et al.,* (2010) manifiesta que el objetivo es identificar y resolver los problemas antes de que afecten a la organización. Es necesaria la detección de fallas para su posterior corrección (resolución de problemas) y de acuerdo con Oppenheimer (2011) explica que la optimización se basa en la gestión de red proactiva que identifica y resuelve los problemas antes de que surjan perturbaciones de la red. La fase de optimización puede conducir a un rediseño de la red si surgen muchos problemas a causa de errores. El rediseño también puede ser necesario cuando los requisitos cambian significativamente.

CAPÍTULO III. DESARROLLO METODOLÓGICO

3.1. METODOLOGÍA PPDIOO

La metodología que se utilizó para la implementación del servidor es PPDIOO (Preparate, Plan, Design, Implement, Operate, Optimize) que comprende seis fases en el ciclo de vida y es la que mejor se adapta a este trabajo brindando un enfoque en el desarrollo, diseño e implementación de redes.

De las seis fases solo se utilizó cinco en la ejecución de la tesis, exceptuando la fase de **preparación** la cual consiste en establecer los requerimientos del cliente, establecer los objetivos, las limitaciones del proyecto, cronograma y la justificación financiera. Estos puntos antes mencionados se realizaron en la preparación del proyecto que se elaboró previo a la ejecución del desarrollo de este trabajo.

3.1.1. FASE DE PLANIFICACIÓN

Se levantó la información del GAD Municipal del Cantón Bolívar de la estructura de la red. Fue necesario utilizar una ficha de recolección de información (Anexo 1); dirigida al jefe del departamento de tecnología, para determinar la cantidad de usuarios, métodos de asignación de IP, servicios de red, control de ancho de banda y el tipo de seguridad; esta información se describe en los resultados.

En la fase de planificación fue necesario elegir la herramienta que permitió determinar el estado en la que se encontraba la red del GAD Municipal del Cantón Bolívar. Se seleccionó Wireshark en la versión 2.0 debido a que es un potente sniffer y analizador de protocolos que permite detectar problemas de redes. Wireshark es software libre y es compatible con la mayoría de plataformas tales como Windows, Linux, Mac OS X, entre otras. Razón por la cual se utilizó esta herramienta.

Además, se instaló el sistema operativo Kali Linux en una máquina virtual. Ésta distribución está enfocada a la seguridad informática y viene con una suite de herramientas que vienen instaladas por defecto; se usó Nmap para realizar pruebas y determinar la cantidad de equipos conectados en la red de acceso público del GAD Municipal del Cantón Bolívar.

El sistema operativo que se usó para la implementación del servidor RADIUS es pfSense 2.2.6, una distribución libre de código abierto muy potente, que brinda funcionalidades tales como: router, firewall, proxy, portal cautivo y está enfocado a la administración de redes, brindando mayor seguridad a la entidad.

3.1.2. FASE DE DISEÑO

En base a la información obtenida se realizó un diseño para la implementación del servidor RADIUS, tomando en cuenta la infraestructura actual de la red del GAD Municipal del Cantón Bolívar y la cantidad de usuarios para la autenticación en la LAN privada.

Para el funcionamiento adecuado del servidor fue necesario segmentar la red a nivel lógico, utilizando diferentes rangos de direcciones IP con mascara de subred fija en la LAN de acceso privado y la LAN de acceso público. La institución no cuenta con switches administrables por esta razón no se crearon VLAN (Virtual Local Area Network) para una mejor administración.

Se utilizó el simulador cisco packet tracert versión 5.3.3 y la herramienta Edraw Max 7 para realizar un diagrama detallado de la red del GAD Municipal del Cantón Bolívar, especificando el direccionamiento IP de la red acceso público y la red de acceso privado, centralizando el tráfico y controlando los recursos a través de dos servidores.

3.1.3. FASE DE IMPLEMENTACIÓN

La instalación del sistema pfSense se llevó acabo en el departamento de tecnología (Anexo 3), para la implementación de los servidores se adaptaron las tarjetas de red de acuerdo al diseño que se muestra en los resultados. En el cuadro 03.01, se especifican las características principales del hardware de los equipos (servidores) utilizados.

Cuadro: 03.01. Característica de hardware de los servidores instalado.

HARDWARE	CARACTERÍSTICAS
Procesador	Intel cor i3
Memoria RAM	2 GB
Disco Duro	500 GB
Tarjeta de Red	ATHEROS 100 Mbps
Tarjeta de Red PCI (Adicionales)	TP-LINK 100 Mbps

Se descargó los paquetes de instalación freeRADIUS 2, Squid 2.7 y SquidGuard 2.7 en el servidor de acceso privado (Figura 03.01) y mientras que el servidor acceso público solo se instalaron los dos últimos servicios del proxy Squid.

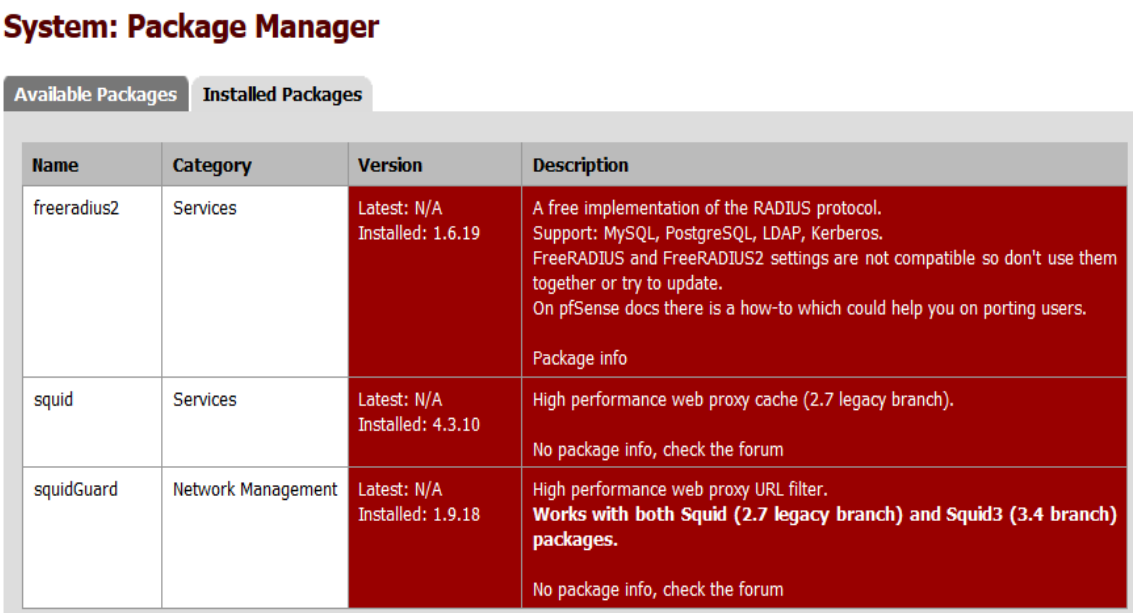


Figura: 03.01. Servicios instalados.

3.1.4. FASE DE OPERACIÓN

En esta fase se observa el correcto funcionamiento de los servidores instalados, que todo marche bien de acuerdo a las configuraciones establecidas y que los servicios de red se encuentren inicializados como se observa en la figura 03.02.

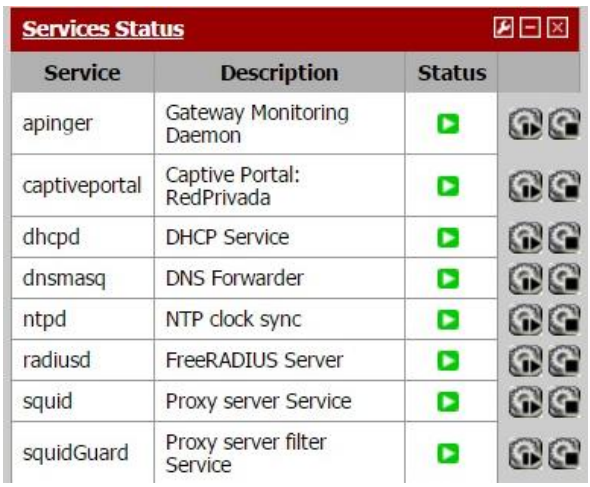


Figura: 03.02. Servicios inicializados en el servidor.

También es necesario ver que las interfaces de red se encuentren levantadas con sus respectivas direcciones IP como se muestra en la figura 03.03 y que los recursos del servidor no estén excediendo sus límites del consumo de memoria, procesador entre otros, figura 03.04.

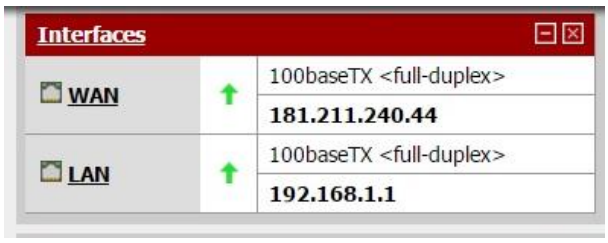


Figura: 03.03. Interfaces de red levantadas.

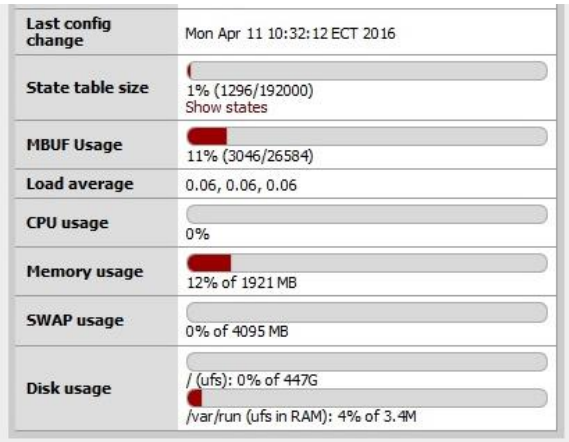


Figura: 03.04. Recursos del servidor.

Además, se comprobó que el servicio de freeRADIUS esté funcionando correctamente a través del portal cautivo en el servidor privado, cumpliendo con el estándar AAA (Autentication, Access, Acounting) y teniendo en cuenta que la configuración de los clientes solo les permita autenticarse en un máximo dos equipos (PC, laptop, teléfonos móviles, tabletas, entre otros) todo esto mencionado se respalda en los resultados.

Es de gran importancia saber que cada vez que se realice un cambio en las configuraciones o se instalen nuevos servicios de red, es necesario realizar un backup que respalde la información del servidor. En caso de emergencia a fallos físico del hardware se pueda restaurar rápidamente (Anexo 5).

3.1.5. FASE DE OPTIMIZACIÓN

Se organizó los recursos que existen en la red para optimizar el desempeño de la misma en la institución, teniendo en cuenta parámetros importantes como el ancho de banda y la cantidad de usuarios que van a disponer de los servicios. Se dio mayor prioridad a los usuarios de la red de acceso privado y mientras que los usuarios de acceso público tienen ciertas limitaciones.

Se distribuyó el ancho de banda (Cuadro 03.02) para que la red de acceso privado tenga mayor disponibilidad, y que la red de acceso público ocupe la cantidad restante. Sin embargo en horarios no laborables la red de acceso

público va aprovechar al máximo el ancho de banda que no se ocupa en la red privada del GAD Municipal del Cantón Bolívar dando mayor disponibilidad a las áreas públicas.

Cuadro: 03.02. Distribución de ancho de banda del GAD Municipal del Cantón Bolívar.

RED	ANCHO DE BANDA
LAN acceso privado	3 Mbps
LAN acceso público	2 Mbps
LAN Biblioteca	1 Mbps
Total	**6Mbps**

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

RESULTADOS

El GAD Municipal del Cantón Bolívar cuenta aproximadamente con 50 computadoras conectadas en la red distribuidas en sus diferentes departamentos. El método que utiliza para la asignación de direcciones IP es estático. Utiliza una dirección de clase C 192.168.X.X, ya que no cuentan con un número excesivo de equipos conectados en la red. Además, dispone con 2 switches (conmutador capa 2) para distribuir todas las conexiones en la intranet.

Se encuentran 10 puntos de acceso AP (Access Point) distribuidos en 15 departamentos o áreas de trabajo, además cuentan con 4 AP de acceso público de los cuales uno de estos puntos inalámbricos se encuentra en la planta baja y tres puntos inalámbricos en la planta alta (Anexo 2). Dicha entidad tiene contratado un ancho de banda de 6Mbps para proporcionar acceso a la Internet a toda la red. Además, cuenta con un servidor proxy y firewall para brindar mayor seguridad a la infraestructura (figura 04.01).

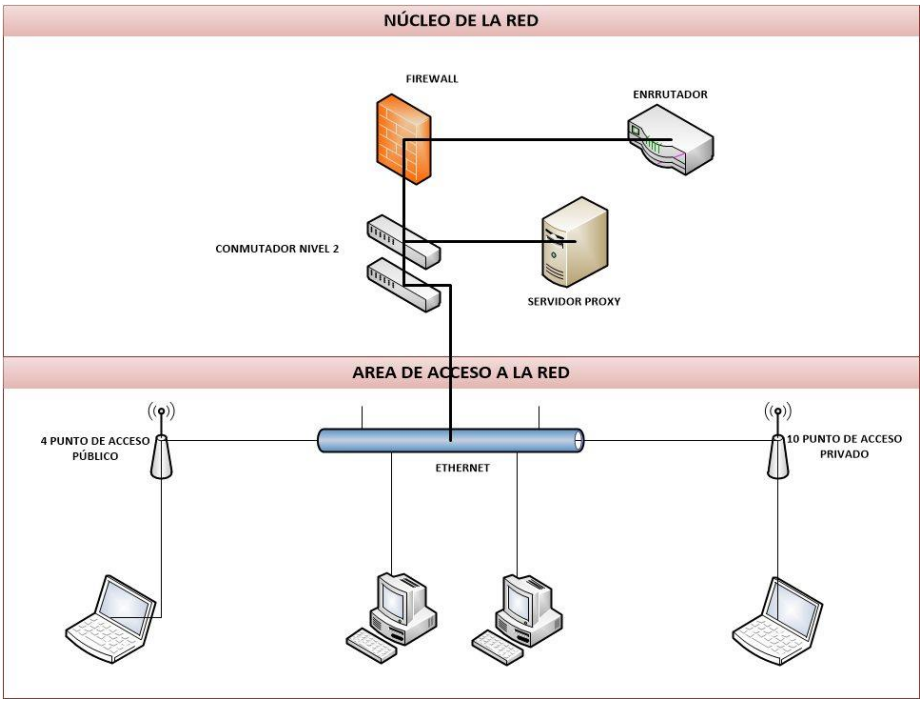


Figura: 04.01. Diagrama de red del GAD Municipal del Cantón Bolívar

Se realizó un análisis del tráfico de la red pública del GAD Municipal del Cantón Bolívar, utilizando la herramienta Wireshark 2.0 para comprobar que durante la transmisión de los datos, los paquetes sean enviados de forma correcta y sin errores. Se capturó el tráfico aproximadamente por cuatro minutos recolectando 11443 paquetes que generó un solo usuario (figura 04.02).

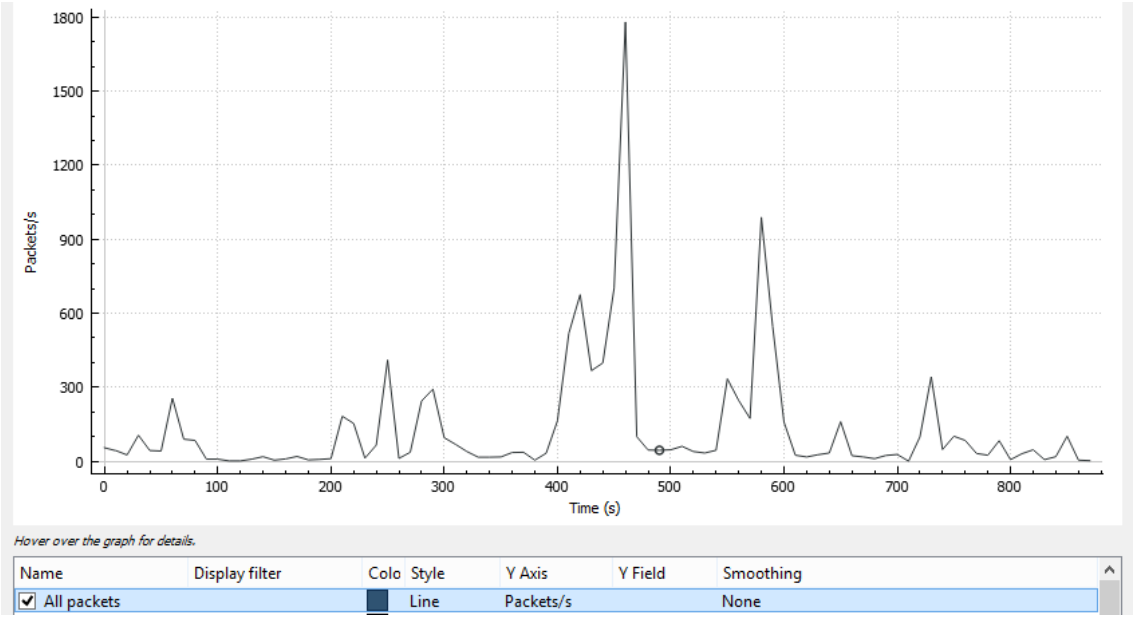


Figura: 04.02. Análisis del tráfico en general. (Página generada por Wireshark)

Los errores en la transmision de datos a través del protocolo de control de transporte TCP (Transport Control Protocol) son míninos, comprobandose que la red no presenta problemas de comunicación y que los tiempos de respuesta de las peticiones TCP se encuentran en rangos normales de funcionamiento, tal como se puede apreciar en la figura 04.03.

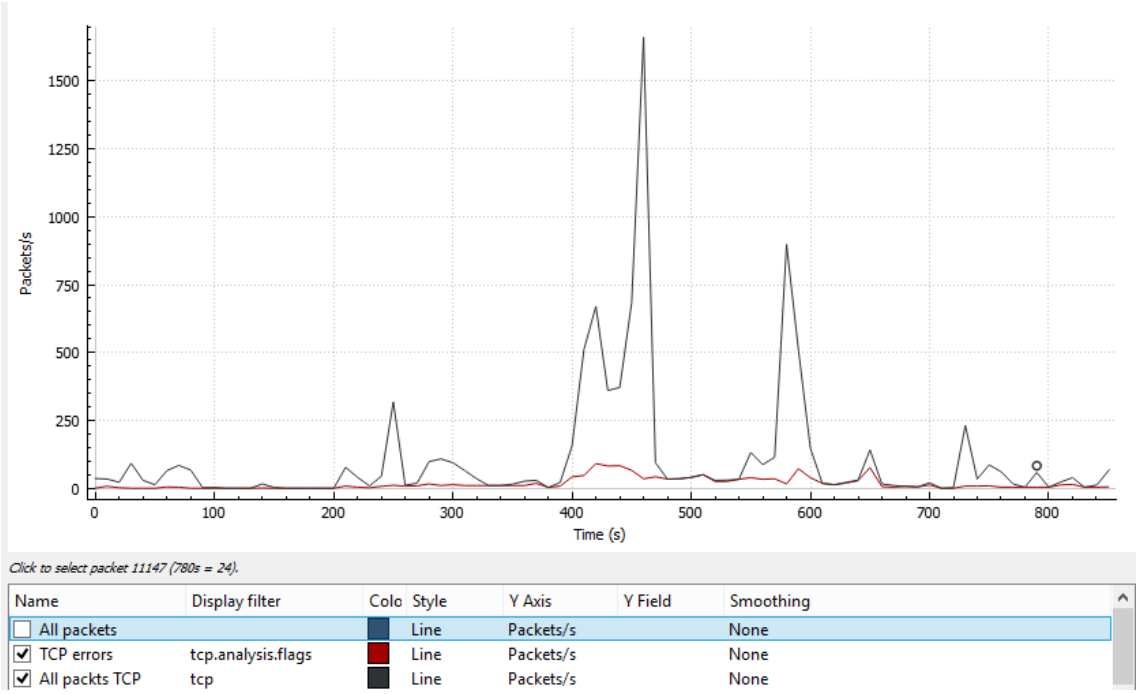


Figura: 04.03. Análisis del tráfico TCP. (Página generada por Wireshark)

El problema se acrecienta cuando las redes no están segmentadas adecuadamente, y los puntos de conexión no utilizan métodos de autenticación más seguros o herramientas que permitan administrar eficientemente los recursos de la red. Se capturó el tráfico HTTP y HTTPS generado al navegar en internet, considerando que cuando no hay limitaciones del ancho de banda, el flujo de información es mayor (figura 04.04).

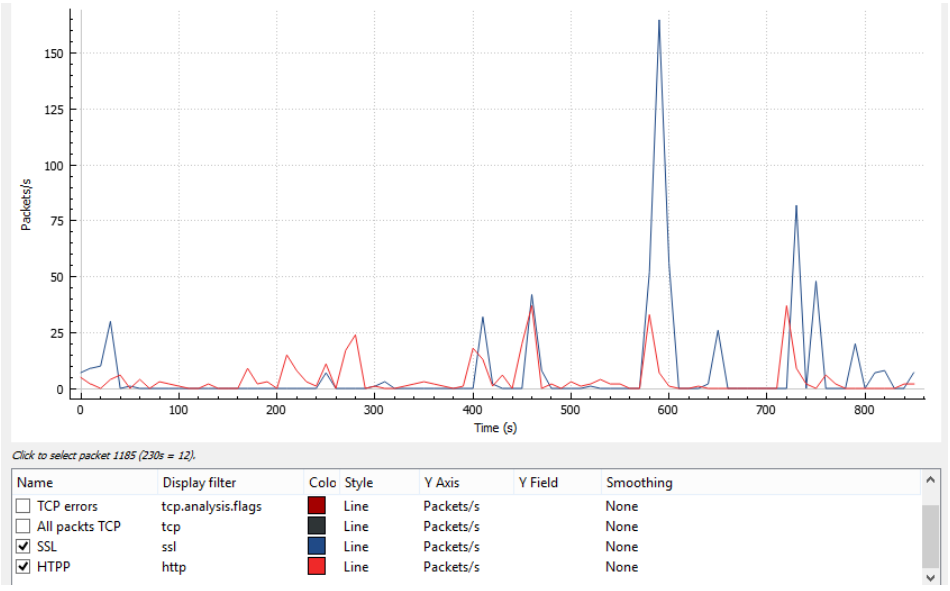


Figura: 04.04. Análisis del tráfico HTTP, HTTPS. (Página generada por Wireshark)

Se utilizó el sistema operativo Kali Linux para hacer uso de la herramienta Nmap (Network Mapper o Mapeador de red). Se procedió a conectarse a un punto inalámbrico de libre conexión del GAD Municipal del Cantón Bolívar, ejecutando el comando ***nmap –sP 192.168.1.****, realizando un escaneo rápido del segmento de red y como resultado se encontró 97 equipos conectados (computadoras, dispositivos móviles) (Figura 04.05).

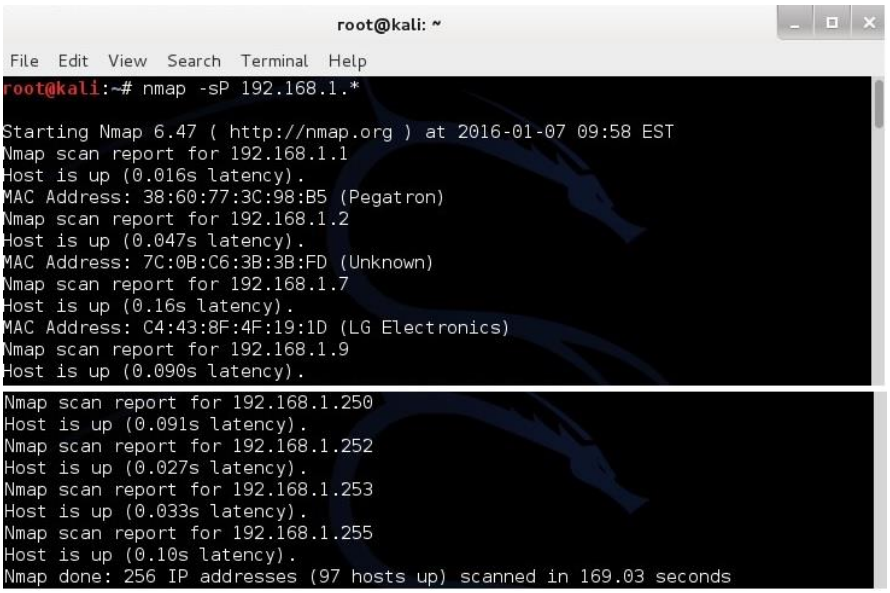


Figura: 04.05. Escaneo de la red informática del GAD Bolívar. (Página generada por Nmap)

Mediante el comando ***nmap 192.168.1.**** o ***nmap –sV 192.168.1.**** se obtuvo información detallada de los equipos conectados en la red, tales como los puertos abiertos y los servicios que corren en cada host como se observa en la figura 04.06.

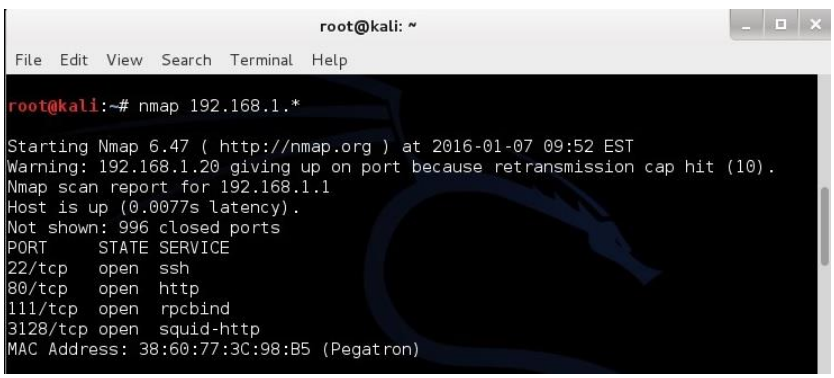


Figura: 04.06. Escaneo de la red informática del GAD Bolívar con detalles de los puertos abiertos. (Página generada por Nmap)

En la figura 04.06 se puede apreciar que en el equipo con la IP 192.168.1.1 se encuentran abiertos los puertos 22, 80, 111, 3128 con los servicios SSH, HTTP, RCP, Proxy respectivamente; esto se debe a que dicho equipo funciona como servidor gestionado las comunicaciones a través del proxy Squid, que es una aplicación que mejora el rendimiento y gestiona el tráfico web.

Se realizó un test de velocidad, para ver la asignación del ancho de banda de un solo equipo (PC o Laptop) del GAD Municipal de Cantón Bolívar. Detectando que al conectarse a la red de acceso público se puede obtener una velocidad de descarga (Download speed) de 2.01 Mbps y una velocidad de subida (Upload speed) de 0.75 Mbps, (Figura 04.07).

Figura: 04.07. Test de velocidad del ancho de banda. (Página generada por www.speedtest.net)

Se desarrolló un modelo de implementación creando una arquitectura cliente/servidor mediante una topología estrella física, tomando en cuenta la red privada para la autenticación a través del servidor RADIUS (Figura 04.08).

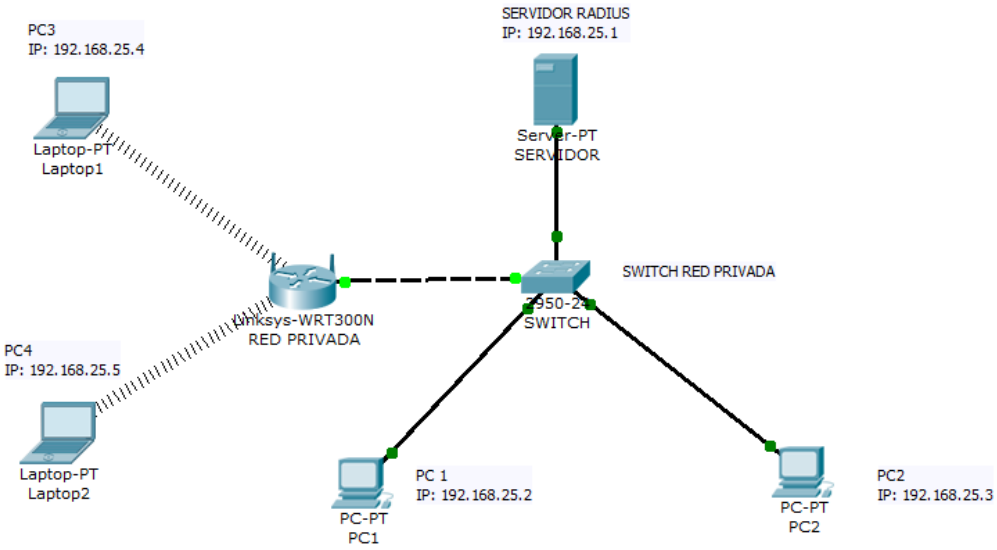


Figura: 04.08. Topología del servidor RADIUS en la red privada.

En la red de acceso privado, se usó dos tarjetas de red eth0 y eth1; WAN y LAN respectivamente tal como se observa en la figura 04.09.

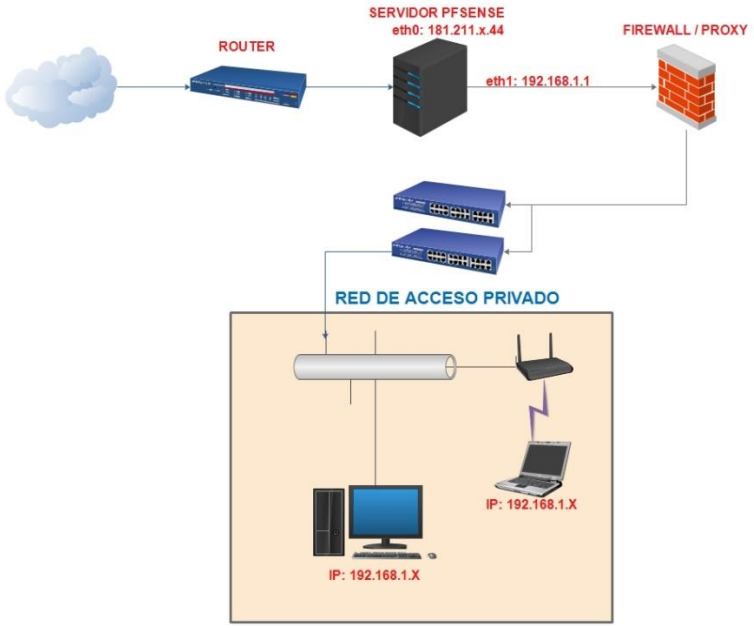


Figura: 04.09. Diagrama de red propuesta para el servidor del control de acceso privado.

En el servidor de acceso público se utilizaron tres tarjetas de red eth0, eth1 y eth2; respetivamente WAN, LAN-pública y LAN-biblioteca. Usando una topología física de estrella y conjuntamente la arquitectura cliente servidor (Figura 04.10).

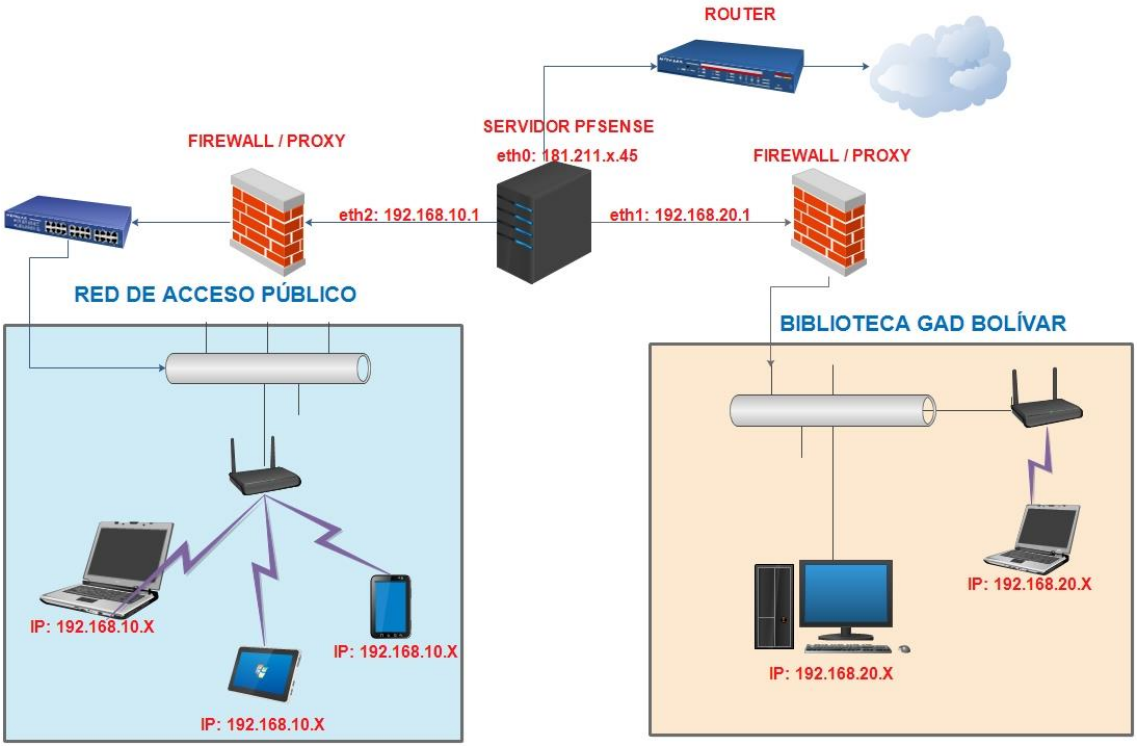


Figura: 04.10. Diagrama de red propuesta para el servidor del control de acceso público y biblioteca.

Se instaló los servidores siguiendo las especificaciones del diseño, configurando los correspondientes parámetros de red, DNS y DHCP para la conexión a internet (Figura 04.11).

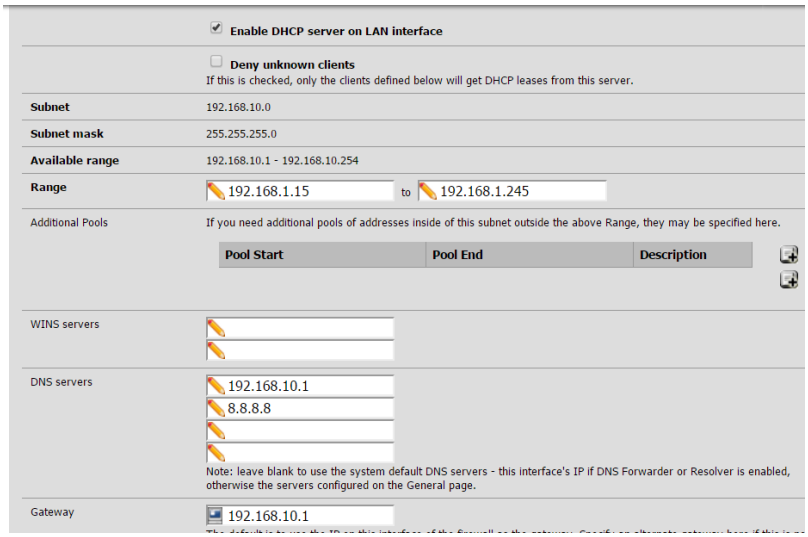


Figura: 04.11. Configuración DHCP.

Se realizó la configuración del servicio freeRADIUS en el servidor privado para la autenticación a través de la red, creando los usuarios con su determinado perfil de navegación (horario de autenticación, ancho de banda, límite de navegación) como se muestra en la figura 04.12; (Ver anexo 4).

Username	Use One Time Password	Simult. Connections	IP Address	Expiration Date	Session Timeout	Possible Login Times
jose-pinargote		2				
miguel-velasquez		2				WK0730-1700
gaby-pazmino		2				
maria-duenas		3				WK0730-1700
xavier-garcia		2				WK0730-1700
irina-carranza		2				WK0730-1700
jessenia-santibanez		2				WK0730-1700
nieve-menendez		2				WK0730-1700
gabriela-brito		2				WK0730-1700
fatima-vera		2				WK0730-1700
mariana-parraga		2				WK0730-1700
franklin-zambrano		2				WK0730-1700
fremy-loor		2				WK0730-1700
yandri		2				WK0730-1700
ruben-molina		3				WK0730-1700
luis-heredia		2				WK0730-1700
josue-vera		3				WK0730-1700
cesar-basurto		2				WK0730-1700
luis-gonzalez		2				WK0730-1700

Figura: 04.12. Usuarios para la autenticación RADIUS en la red privada del GAD Bolívar

El servicio del proxy se instaló en ambos servidores con la misma configuración, permitiendo filtrar ciertos contenidos que no son de utilidad para el GAD Municipal del Cantón Bolívar como se aprecia en la figura 04.13.

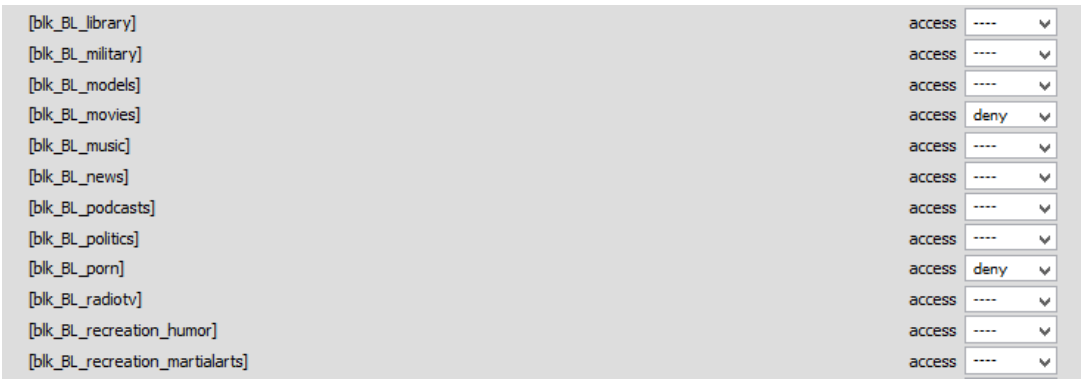


Figura: 04.13. Lista de filtrado de páginas web

Se configuró el firewall de acuerdo a las necesidades de navegación que tiene el GAD Municipal del Cantón Bolívar. Estableciendo reglas que limitan el tráfico

por determinados puertos, filtrando información (entrante, saliente) y disminuyendo el riesgo de posibles ataques informáticos (Figura 04.14).

Firewall: Rules

Floating | WAN | LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
☐		IPv4 *	LAN net	*	LAN net	*	*	none		
☐		IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		
☐		IPv4 ICMP	LAN net	*	*	*	*	none		
☐		IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		
☐		IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		

Figura: 04.14. Reglas de firewall

Al conectarse a la red de acceso privado, es necesario autenticarse por medio del portal cautivo para acceder al internet, donde pedirá un usuario y contraseña previamente establecido por el administrador y validados a través del servicio freeRADIUS como se observa en la figura 04.15.

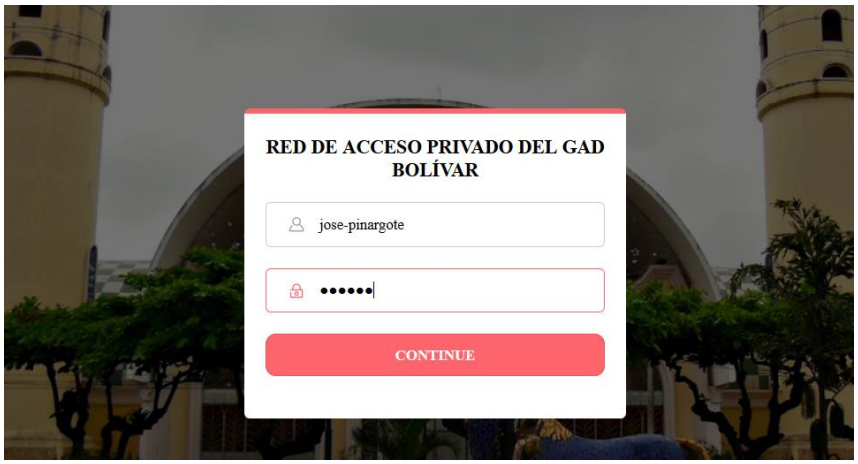


Figura: 04.15. Autenticación RADIUS por medio del portal cautivo (hostpot).

En caso de que haya introducido el usuario y/o contraseña de forma incorrecta o el usuario intente autenticarse en más de dos equipos, los servicios serán limitados, restringiendo el acceso al internet (Figura 04.16).

Figura: 04.16. Autenticación RADIUS, usuario incorrecto.

En el servidor de acceso público se configuró un portal cautivo sin autenticación (Figura 04.17) que permita a los clientes navegar por 45 minutos de acuerdo con las especificaciones del departamento técnico del GAD Municipal del Cantón Bolívar, contralando el ancho de banda por cada dispositivo conectado y evitando saturación de los equipos de comunicación (Router, Switch, Access Point).

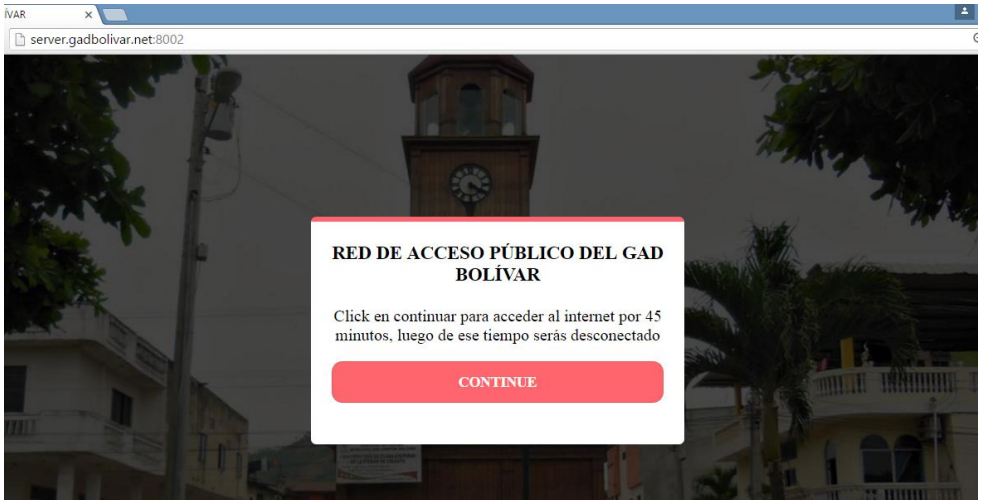


Figura: 04.17. Portal cautivo servidor de acceso público.

Y por último se comprobó correcto funcionamiento de autenticación, autorización y acceso del servidor RADIUS de forma nativa, usando un usuario de prueba

(usuario=”josep” password=”92jose”), ejecutando el siguiente comando: ***“radtest josep 92jose 192.168.10.1:1812 0 123456”*** (Figura 04.18).

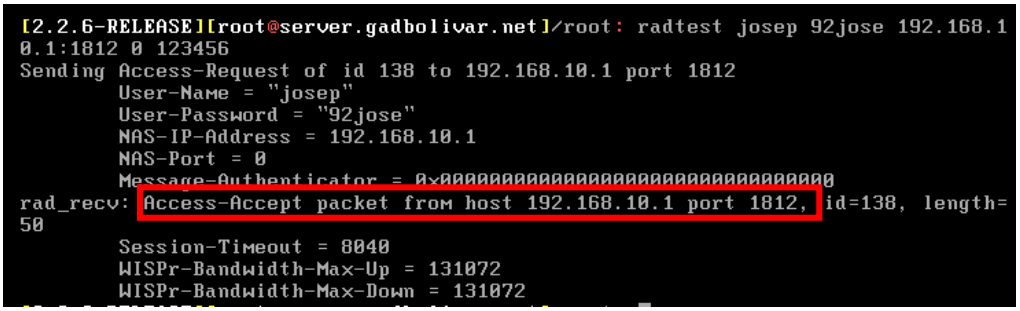


Figura: 04.18. Test de comprobación del servidor RADIUS.

Además, con los servicios del proxy corriendo en ambos servidores, se controla que los clientes conectados a la red del GAD Municipal del Cantón Bolívar no puedan visitar páginas web restringidas, debido a su contenido (Figura 04.19).

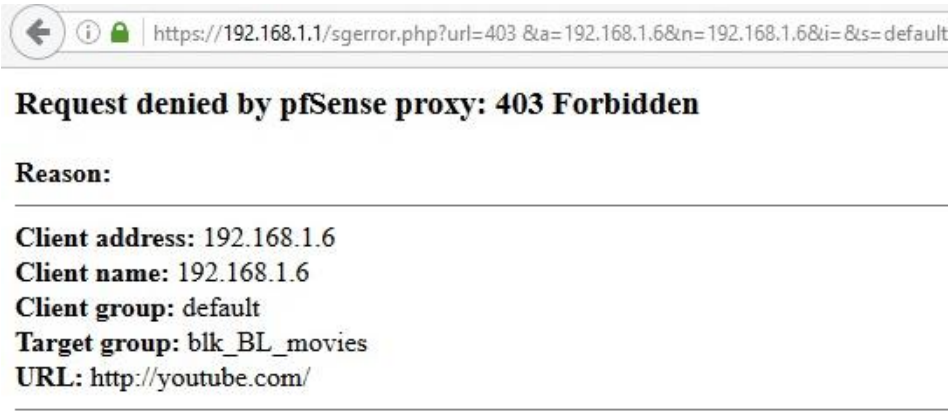


Figura: 04.19. Filtro de navegación del proxy.

En la red de acceso privado, se logró que el consumo del ancho de banda se encuentre entre 2 a 3 Mbps, con todos los usuarios autenticados; dando prioridad a los empleados del GAD Municipal del Cantón Bolívar tal como se observa en la figura 04.20.

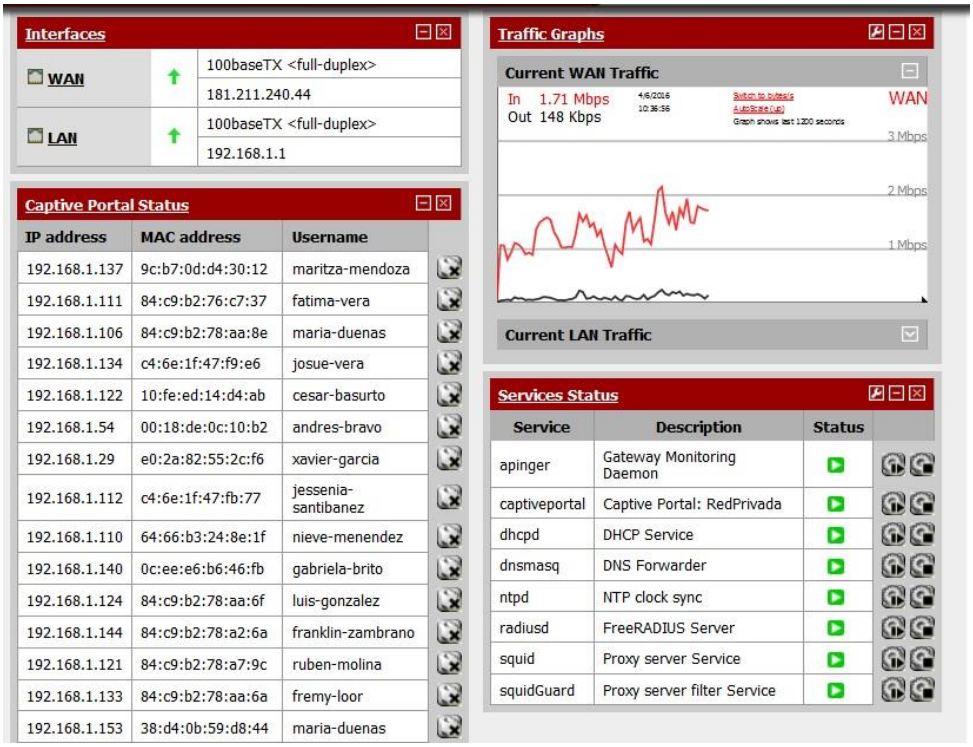


Figura: 04.20. Control de ancho de banda LAN privada.

Se mejoró el tráfico en el segmento de red de acceso público, por consiguiente, se redujo el número de usuarios conectados simultáneamente en los puntos de libre conexión. Se segmentó el ancho de banda garantizando que todos los usuarios puedan acceder al servicio de internet sin interrupciones (Figura 04.21).

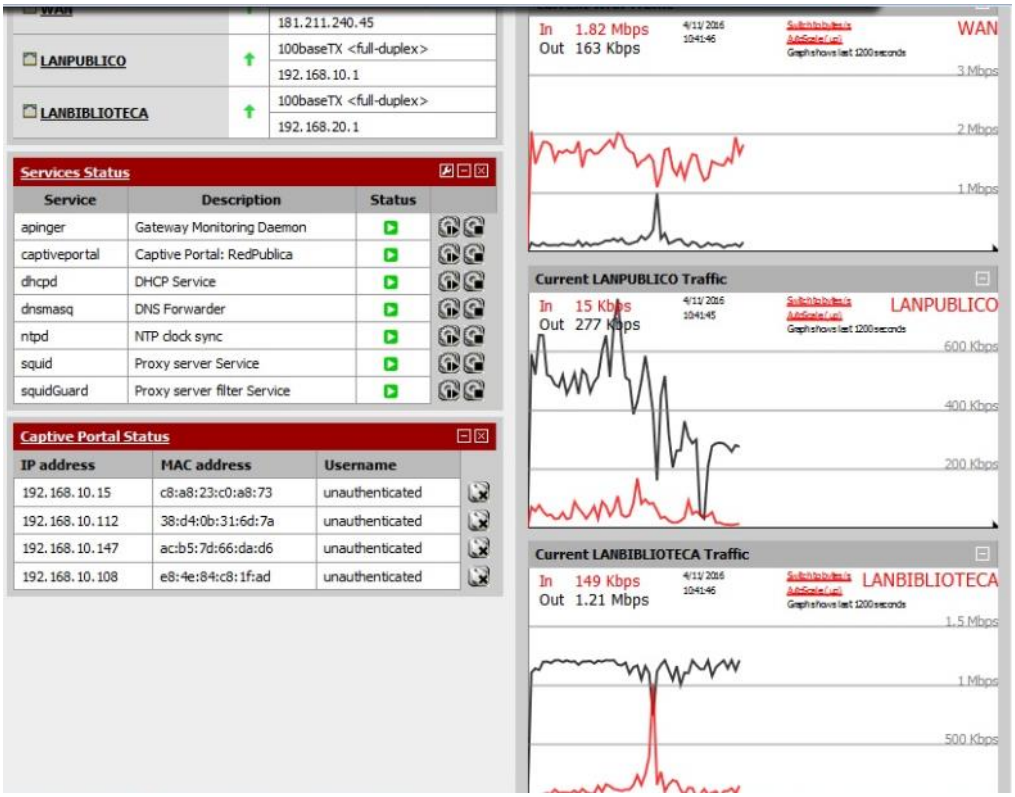


Figura: 04.21. Control de ancho de banda LAN público LAN biblioteca.

El consumo del ancho de banda se reguló, priorizando el acceso a los servicios de internet tanto en la red de acceso privado como la red de acceso público. En la figura 04.22 se muestra el consumo en general de un día laboral en la red privada.

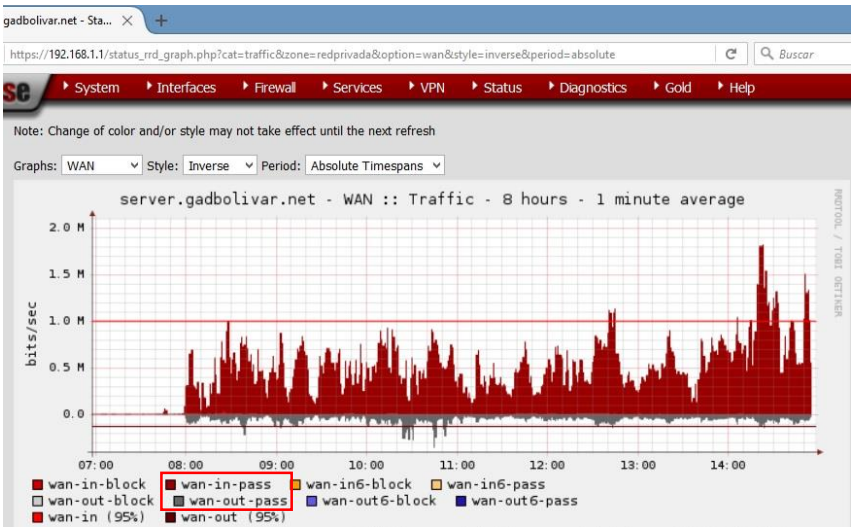


Figura: 04.22. Consumo de ancho de banda en la red privada.

Además, se comprobó que el consumo del ancho de banda se mantiene constante como se observa en la figura 04.23, sin que el tráfico se exceda mejorando la disponibilidad de los recursos de la red. Es importante saber que este tipo de resultados (reportes) son útiles, permitiendo monitorizar en tiempo real y controlar adecuadamente el tráfico entrante y saliente.

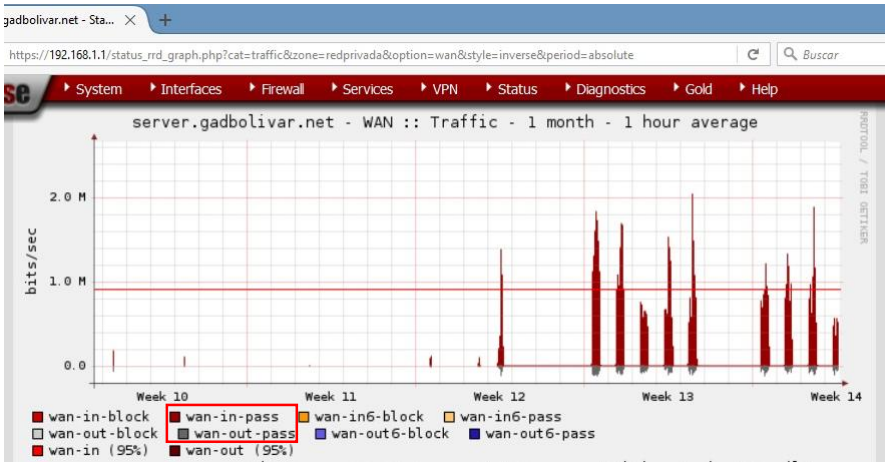


Figura: 04.23. Consumo de ancho de banda en periodo semanal

Por último se realizó un test para comprobar la velocidad asignada a cada equipo autenticado en la red, sabiendo que los usuarios de la red de acceso privado tienen diferente ancho de banda asignado (hasta 1 Mbps) y mientras que en la red de acceso público todos los usuarios poseen la misma restricciones (256 Kbps de descarga y 256 Kbps de subida).

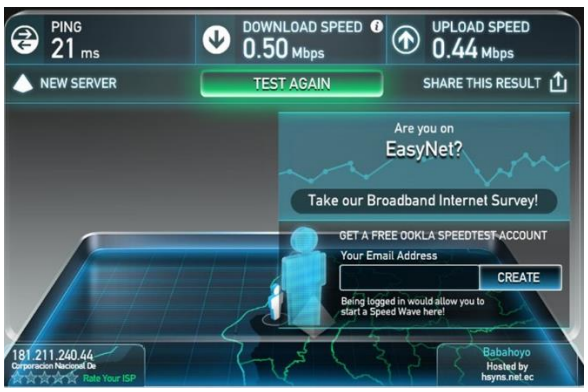


Figura: 04.24. Test de velocidad, usuario de la red de acceso privado. (Página generada por www.speedtest.net)

Figura: 04.25. Test de velocidad, usuario de la red de acceso público. (Página generada por www.speedtest.net)

Debido al fenómeno natural ocurrió el 16 de abril de 2016 (Catástrofe ocurrida por el terremoto), la infraestructura del GAD Municipal del Cantón Bolívar quedó disfuncional, en consecuencia la infraestructura de red sufrió múltiples averías (equipos, servidores, cableado entre otros). Se reinstaló el servidor de acceso privado en el establecimiento provisional del Patronato Municipal del Cantón Bolívar, y debido a estos acontecimientos, parte de la topología de red propuesta (servidor de acceso público) no se encuentra en total funcionamiento.

DISCUSIÓN

Arana *et al.,* (2013) presenta el diseño e implementación de un sistema de control de acceso a la red, que proporciona el servicio de Autenticación, Autorización y Auditoría (AAA) usando software libre y haciendo uso de VLAN para la administración de diferentes departamentos y registros de los usuarios, mientras que los autores del presente trabajo han utilizado el sistema AAA enfocado a mejorar la seguridad y optimizar los recurso de red del GAD Municipal del Cantón Bolívar aplicando políticas de firewall y utilizando filtros de navegación que mejoren el flujo de información en la institución.

Vásquez y Vaca (2015), han realizado el control de acceso y administración de recursos de red mediante un servidor AAA en el GAD Municipal del Cantón Urcuquí gestionando la red de acceso privado a través VLAN, empleando el método EAP-TTLS que basa su seguridad en certificados digitales para la autenticación de los usuarios. Con la implementación del servidor en el GAD Municipal del Cantón Bolívar se administró la red de acceso privado y la red de acceso público, enfocándose en la asignación de los recursos por equipos conectado a la red, de tal manera ofreciendo disponibilidad del servicio al momento de navegar en internet con las debidas restricciones de uso y además con las políticas de firewall se protege de ataques externos de la red; que de acuerdo con el “Plan Nacional Para El Buen Vivir” se trata de democratizar progresivamente el acceso al ciberespacio para todos.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La recolección de información del departamento de tecnología del GAD Municipal del Cantón Bolívar, facilitó comprender la estructura de la red. El análisis ayudó a examinar el tráfico de los protocolos de comunicación verificando el estado de la intranet.

- El diseño físico y lógico es de gran importancia para un correcto funcionamiento de la red, y es parte fundamental para la implementación seguir un modelo de estructura esquematizada.

- La implementación del servidor, permitió una mejor administración y control de los servicios de red. El uso de firewall y proxy ayudó a disminuir el tráfico que generan las redes sociales y páginas multimedia, logrando optimizar el flujo de información.

- El método de autenticación, acceso y contabilización del servidor RADIUS ayudó generar perfiles de navegación y por ende a mejorar la seguridad de la institución, permitiendo el ingreso a la red privada al usuario correcto.

RECOMENDACIONES

- Tener una correcta documentación de la infraestructura de red y las políticas de navegación, que sean adaptables en caso de que surjan nuevas necesidades.

- Hacer uso de dispositivos de alta disponibilidad (switches administrables), para un mayor rendimiento y una buena administración de los recursos de la red.

- Monitorizar el estado de la red constantemente, revisando los archivos de log, haciendo uso de las herramientas que vienen instaladas por defecto en servidor pfSense.

- Al momento de crear las credenciales de autenticación, se debe dar a conocer al cliente que no debe divulgar o entregar su usuario y contraseña a ningún tipo de persona, ya que compromete la seguridad que ofrece el servicio freeRADIUS.

BIBLIOGRAFÍA

Amezaga, X. 2013. Medios de transmisión en redes de área local. Formato (HTML). Consultado el 19 de noviembre de 2015. Disponible en: https://xabiamezaga.wordpress.com/2013/02/05/medios-de-transmision-en-redes-de-area-local/

Arana, J; Villa, l; Polanco, O. 2013. Implementación del Control de Acceso a la Red Mediante los Protocolos de Autenticación, Autorización y Auditoría. Cali, CO. Revista Ingeniería y Competitividad. Vol. 15. p 127-137.

Bernal, L 2012. Medios de transmisión. (En Línea). Consultado el 16 de agosto del 2015. Formato (PDF). Disponible en http://es.slideshare.net/mscamposl/medios-de-comunicacin-guiados-y-no-guiados

BSD (Berkeley Software Distribution). 2013. Qué es BSD. (En Línea). Consultado el 11 de enero del 2016. Formato HTML. Disponible en https://www.freebsd.org/doc/es/articles/explaining-bsd/article.html

Cáceres, L; Fritis, R; Collao, P. 2015. Desarrollo de un Simulador para el Protocolo de Criptografía Cuántica E91 en un Ambiente Distribuido. Arica, CL. Revista Chilena de Ingeniería. Vol. 23. p 245-258.

Cisco. 2014. Como el servidor RADIUS trabaja. (En línea). Consultado el 19 de Mayo del 2015. Formato PDF. Disponible en http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

De la Casa, A. 2014. Nmap una aplicación para el análisis de redes. (En línea). Consultado 19 de Nov. 2015. Formato HTML. Disponible en http://rootear.com/ubuntu-linux/nmap-aplicacion-analisis-redes

De Zayas, L y Sao, A. 2002. Elementos conceptuales básicos útiles para comprender las redes de telecomunicación. Habana, CU. Revista ACIMED, vol.10. p 5-6.

Díaz, G. sf. Redes de Computadoras: tipos de Topologías de redes. Consultado el 15 de Mayo del 2015. Formato PDF. Disponible en http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/04_conceptosBasicos2.pdf

Díaz, Y; Pérez, Y; Proenza, D. 2014. Sistema para la Gestión de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Santiago de Cuba, CU. Revista Ciencias Holguín. Vol. 10. p 1-14.

Dordoigne, J. 2011. Redes informáticas: clasificación de las redes. 4 ed. Barcelona. Ediciones ENI. p 17-18.

Egli, P. 2015. Remote authentication dial in user service. (En línea). Consultado el 19 de mayo del 2015. Formato PDF. Disponible en http://www.indigoo.com/dox/itdp/09_Access/AAA_RADIUS.pdf

Fuertes, W; Rodas, F; Toscano, D. 2011. Evaluación de ataques UDP Flood utilizando escenarios virtuales como plataforma experimental. Tunja, CO. Revista Facultad de Ingeniería. Vol. 20. p 37-53.

García, A; Hurtado, C; Alegre, M. 2012. Seguridad informática: seguridad en redes. 1 ed. España. Paraninfo. p 145.

_____. 2012. Seguridad informática: tipos de cifrado de claves. 1 ed. España. Paraninfo. p 103–104.

Gómez, N. 2012. Redes informáticas, Clasificación. (En línea). Consultado el 19 de noviembre de 2015. Formato HTML. Disponible en: http://www.taringa.net/post/info/15321302/Clasificacion-de-Redes-Informaticas-por-alcance.html

Henríquez, S. 2013. Tipos de redes informáticas. Redes por alcance. (En línea). Consultado el 19 de noviembre de 2015. Formato HTML. Disponible en: https://gobiernoti.wordpress.com/2013/09/05/internet-la-red-de-redes-%E2%80%93-redes-por-alcance/

Herrera, E. 2011.Tecnología y redes de transmisión de datos: medios de transmisión de datos. 2 ed. Noriega p 81.

Ledesma, T; Coya, L; Marichal, L. 2012. Herramientas de monitorización y análisis del tráfico en redes de datos. Revista telemática. Vol. 11. p 46-59.

LOES (Ley Orgánica de Educación Superior). 2010. Suplemento del Registro Oficial Órgano del Gobierno del Ecuador. N° 298, Art. 8. Serán fines de la educación superior. p 6.

López, A. 2010. La guerra de los sistemas operativos. CR. Revista Reflexiones. Vol. 89. p 61-73.

López, M. 2014. 31 distribuciones Linux para elegir bien la que más necesitas. (En Línea). Consultado el 19 de julio del 2015. Formato PDF. Disponible en http://www.genbeta.com/linux/31-distribuciones-de-linux-para-elegir-bien-la-que-mas-necesitas

LOT (Ley Orgánica de Telecomunicaciones). 2015. Suplemento del Registro Oficial Órgano del Gobierno del Ecuador. N° 439, Art. 2. Ámbito, Art. 3. Objetivo, Art. 9. Redes de telecomunicaciones. p 4-6.

Lyon, G. sf. Guía de referencia de Nmap. (En Línea). Consultado 19 de Nov. 2015. Formato HTML. Disponible en https://nmap.org/man/es/

Márquez, B. 2011. Efecto de los obstáculos tipo polímero resina en rendimiento de redes tcp/ip/ieee 802.119 modo ad-hoc. VE. Revista Electrónica de estudios telemáticos. Vol. 10. p 102-115.

Mateo, F y Veraguas, O. 2012. Sniffers analizadores de paquetes. (En Línea). Consultado el 18 de julio del 2015. Formato DOC. Disponible en http://www.decom-uv.cl/

Mendoza, J. 2008. Cifrado simétrico y asimétrico. (En línea). Consultado el 26 de julio del 2015. Formato PDF. Disponible en http://dspace.ups.edu.ec/bitstream/123456789/8185/1/Demostraci%C3%

B3n%20de%20cifrado%20sim%C3%A9trico%20y%20asim%C3%A9trico.pdf

Miñarro, A. 2009. Mecanismo de seguridad en accesos desde movilidad. (En línea). Consultado el 19 de mayo del 2015. Formato PDF. Disponible en http://www.coitt.es/res/revistas/06c%20Rep%20Radius%20OF9.pdf

Naveas, G; Urrutia, E. 2013. Un modelo multifractal simplificado para flujos de tráfico en redes de computadoras de alta velocidad. Arica, CL. Revista Chilena de Ingeniería. Vol. 21. p 408-413.

Nina, L. 2013. Sniffers. La Paz, BL. Revista Boliviana. ISSN 1997-4044. p 36-37.

Oppenheimer, P. 2010. Top Down Network Design: methodology PDIOO. 3 ed. USA. Cisco Press. p 7-8

Pech, G. 2013. Medios de transmisión y topologías. (En línea). Consultado el 19 de noviembre de 2015. Formato HTML. Disponible en http://concepredes.blogspot.com/2013/04/medios-de-transmision.html

Pérez, C; De Los Cobos, S. 2010. Diseño óptimo de redes y enrutamiento de computadoras. San José, CR. Revista de Matemática: Teoría y Aplicaciones. Vol. 17. p 69-80.

Ramírez, G. 2012. Medios guiados y Medios no guiados. (En línea). Consultado el 15 de Mayo del 2015. Formato PDF. Disponible en http://es.slideshare.net/gramirezpi/medios-guiados-y-medios-no-guiados

Rojo, Y. 2012. Redes de Computadoras. (En línea). Consultado el 19 de noviembre de 2015. Formato HTML. Disponible en http://socializandoredes.blogspot.com/2012/11/medios-de-transmision-de-datos.html

Sanjuan, L. 2012. Criptografía I. (En Línea). Consultado el 26 de Julio del 2015. Formato PDF. Disponible en http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Criptograf%EDa%20I.pdf?sequence=1

Sivasubramanian, B; Frahim, E; Froom, R. 2010. Analyzing the Cisco Enterprise Campus Architecture. (En línea). Consultado 19 de Nov. 2015. Formato HTML. Disponible en http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3

Suárez, M. 2012. Sistemas Operativos de Red. (En Línea). Consultado el 19 de julio del 2015. Formato PDF. Disponible en www.uv.mx/personal/.../Apuntes-del-Curso-de-SOR-Temas-1-a-5.pdf

Tanenbaum, S; Wetherall, D. 2012. Redes de Computadoras. 5 ed. México. Pearson Prentice Hall. p 15-23

Tiso, J. 2012. Designing Cisco Network Service Architectures. 3 ed. USA. Cisco Press. p 13-14

Torres, J. 2011. Topologías de redes. (En línea). Consultado el 15 de Mayo del 2015. Formato PDF. Disponible en https://cursotecnicoredes2011.files.wordpress.com/2011/03/tema-3-topologc3adas-de-redes.pdf

UNAM (Universidad Nacional Autónoma de México). 2012a. Concepto de criptografía. (En línea). Consultado el 15 de Mayo del 2015. Formato HTML. Disponible en http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/11-concepto-de-criptografia

_____ . 2012b. Principales algoritmos asimétricos. (En línea). Consultado el 26 de Julio del 2015. Formato HTML. Disponible en http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/51-introduccion-a-la-criptografia-asimetrica/513-principales-algoritmos-asimetricos?showall=&start=3

Vásquez, C y Vaca, W. 2015. Control de acceso y administración de recursos de red mediante un servidor AAA en el GAD Municipal de Urcuquí usando software libre: Sistema AAA. (En Línea). EC. Consultado 13 de Nov. 2015. Formato PDF. Disponible en http://repositorio.utn.edu.ec/handle/123456789/4337

Velasco, R. 2015. Las mejores 20 distribuciones de Linux para el día a día. (En Línea). Consultado el 19 de julio del 2015. Formato HTML. Disponible en http://www.redeszone.net/2015/02/21/las-mejores-20-distribuciones-de-linux-para-el-dia-dia/

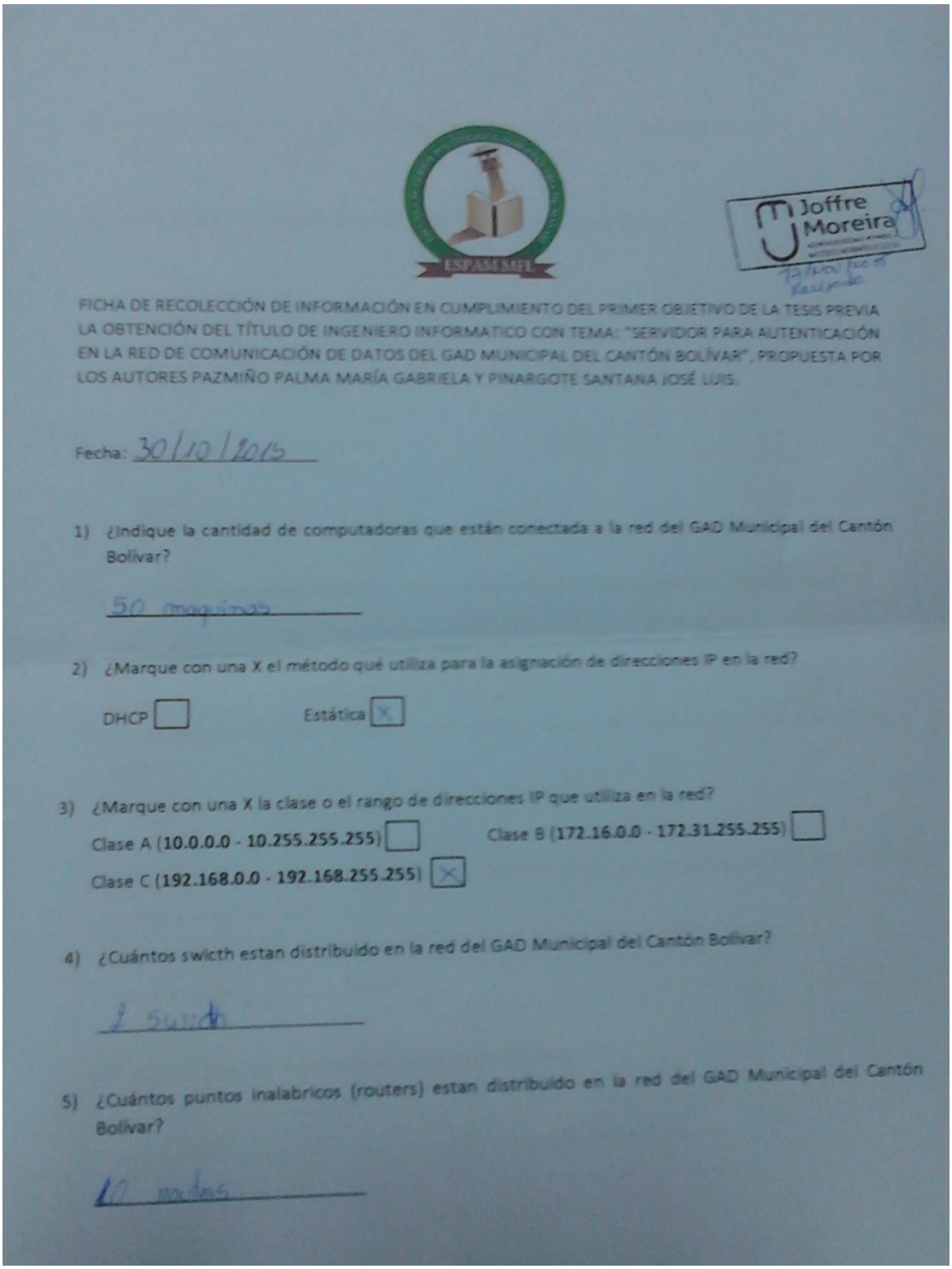
Villegas, M; Meza, M; León, P. 2011. Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Zulia, VE. Revista Télematique. Vol. 10. p 4 - 6.

Zambrano, W; Chafla, G; Moreira, C; Cuzme, G. 2015. Software como servicio de cita médicas en línea un modelo aplicado a la salud. Calceta, EC. Revista ESPAMCIENCIA. Vol. 6. p 37-44

ANEXOS

ANEXO 1

FICHA DE RECOLECCIÓN DE INFORMACIÓN EN EL GAD BOLÍVAR



Joffre Moreira

FICHA DE RECOLECCIÓN DE INFORMACIÓN EN CUMPLIMIENTO DEL PRIMER OBJETIVO DE LA TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMATICO CON TEMA: "SERVIDOR PARA AUTENTICACIÓN EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR", PROPUESTA POR LOS AUTORES PAZMIÑO PALMA MARÍA GABRIELA Y PINARGOTE SANTANA JOSÉ LUIS.

Fecha: 30/10/2015

1) ¿Indique la cantidad de computadoras que están conectada a la red del GAD Municipal del Cantón Bolívar?

50 maquinas

2) ¿Marque con una X el método qué utiliza para la asignación de direcciones IP en la red?

DHCP [ ] Estática [X]

3) ¿Marque con una X la clase o el rango de direcciones IP que utiliza en la red?

Clase A (10.0.0.0 - 10.255.255.255) [ ] Clase B (172.16.0.0 - 172.31.255.255) [ ]

Clase C (192.168.0.0 - 192.168.255.255) [X]

4) ¿Cuántos swicth estan distribuido en la red del GAD Municipal del Cantón Bolívar?

2 Swith

5) ¿Cuántos puntos inalabricos (routers) estan distribuido en la red del GAD Municipal del Cantón Bolívar?

10 antes

6) ¿La red del GAD Municipal del Cantón Bolívar está segmentada por departamentos?

Si [X] No [ ]

7) ¿Cuántos departamentos existen en el GAD Municipal del Cantón Bolívar?

19

8) ¿Existen redes publicas de libre conexión?

Si [X] No [ ]

9) ¿Cuántas redes publicas existen?

Una Red

10) ¿Cuánto es el ancho de banda disponible para la red del GAD Municipal del Cantón Bolívar?

6 MB

11) ¿Está distribuido el ancho de banda por cada usario conectado en la red del GAD Municipal del Cantón Bolívar?

Si [X] No [ ]

12) ¿Marque con una X los servicios que tiene instalado en la infraestructura del GAD Municipal del Cantón Bolívar?

Servidor Web [ ] Firewall [X] Servidor Proxy [X]

Servidor Correo [ ] Otros [ ]

En caso de tener otros servicios instalado indique cuales son.

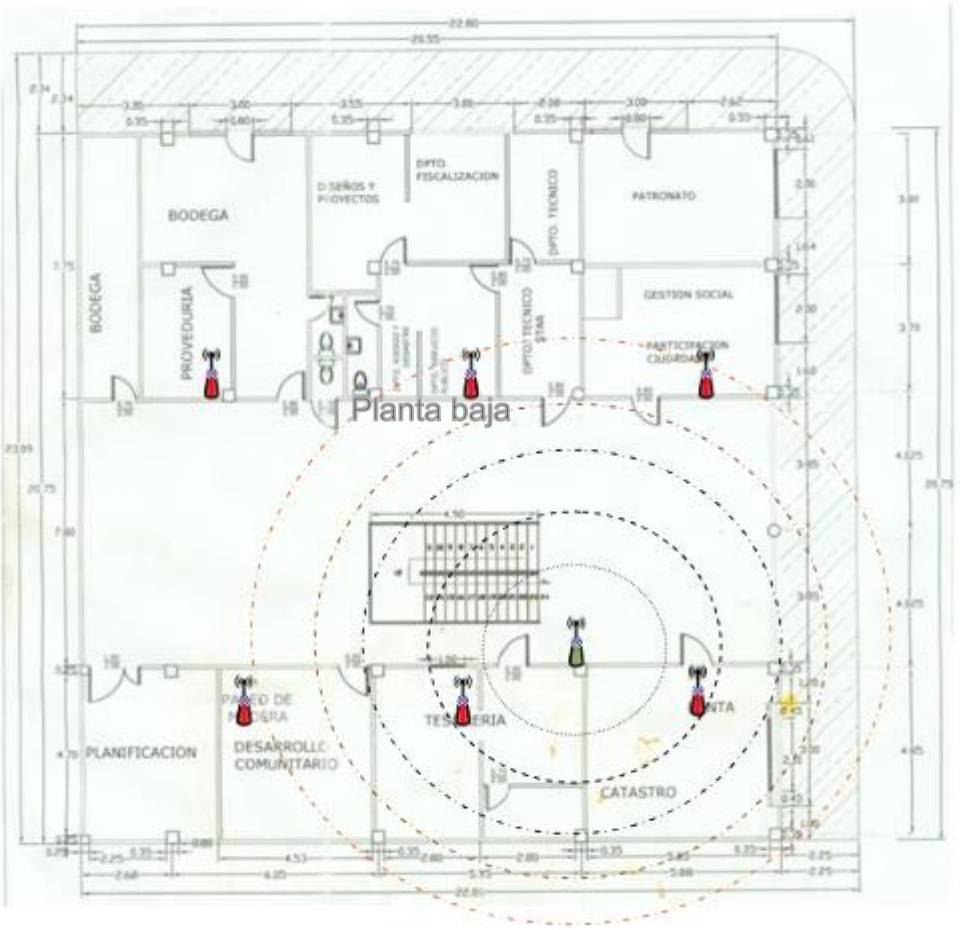
_____ _____

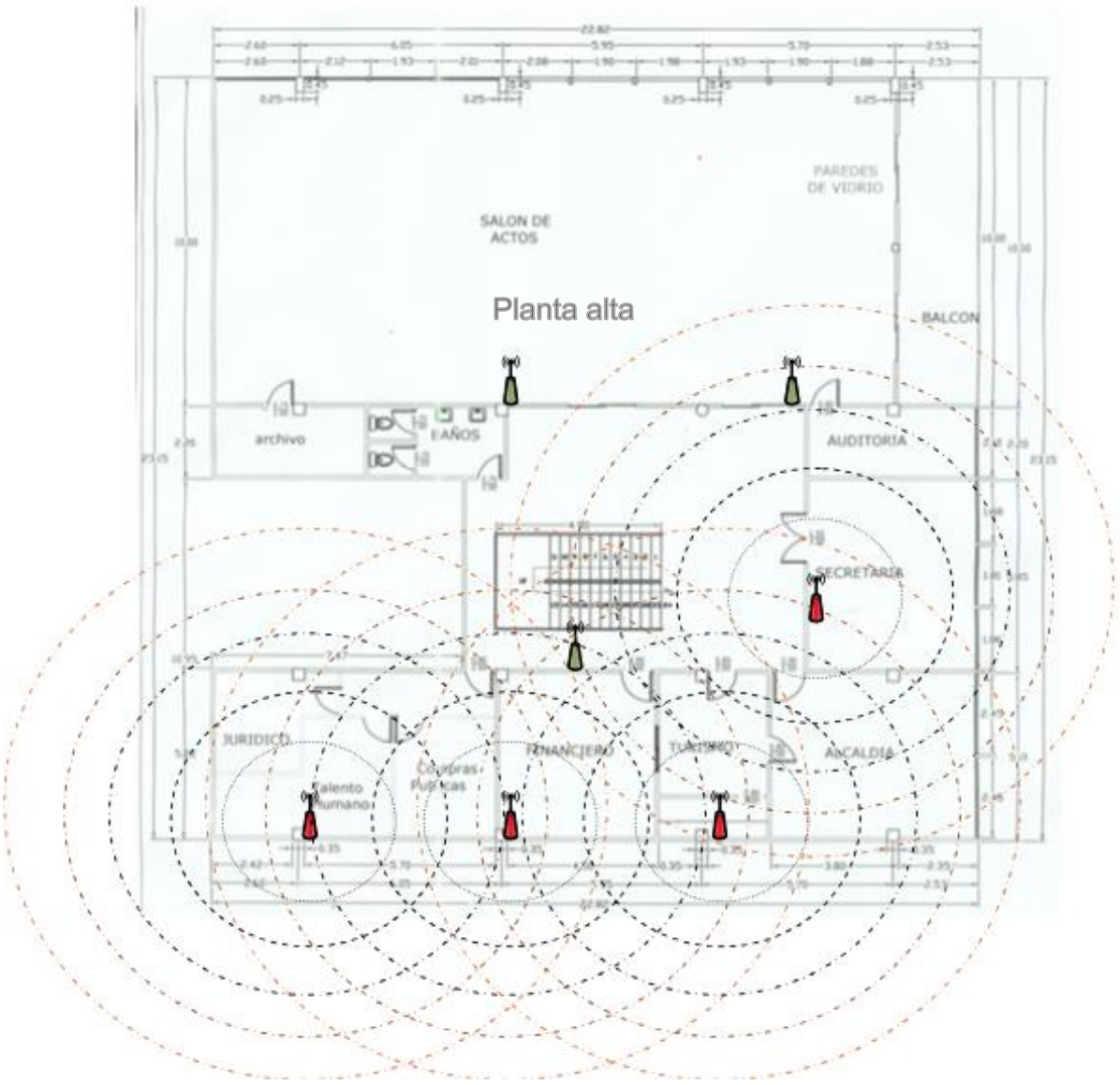
_____ _____

_____ _____

ANEXO 2

PLANOS DE RED PLANTA BAJA Y PLANTA ALTA DEL GAD BOLÍVAR




Planta alta
SALON DE ACTOS
PAREDES DE VIDRIO
BALCON
archivo
BAÑOS
AUDITORIA
SECRETARIA
JURIDICO
Talento Humano
Compras Publicas
FINANCIERO
TURISMO
ALCALDIA

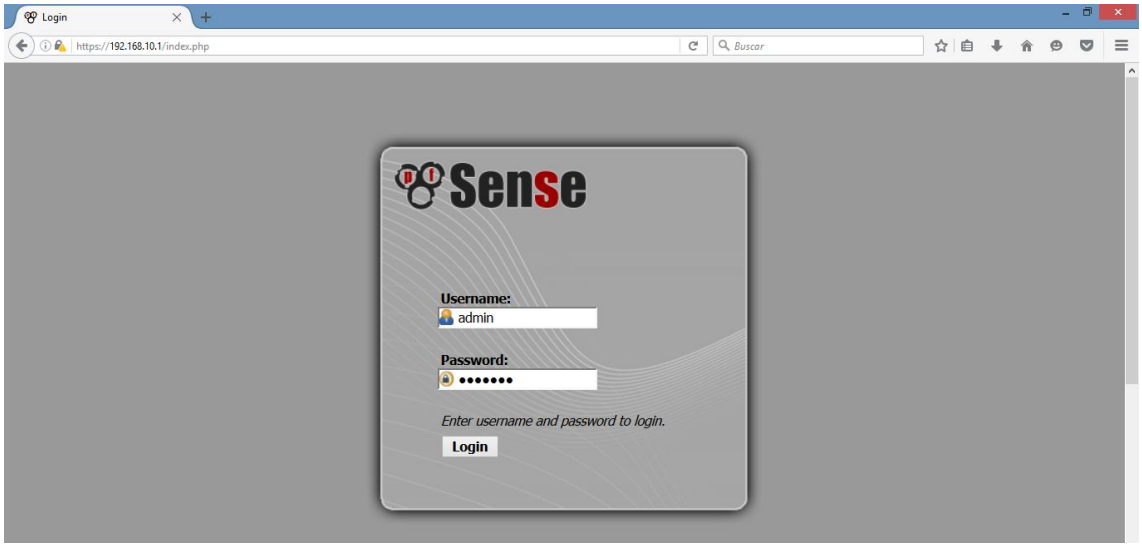
ANEXO 3

IMPLEMENTACIÓN DEL SERVIDOR

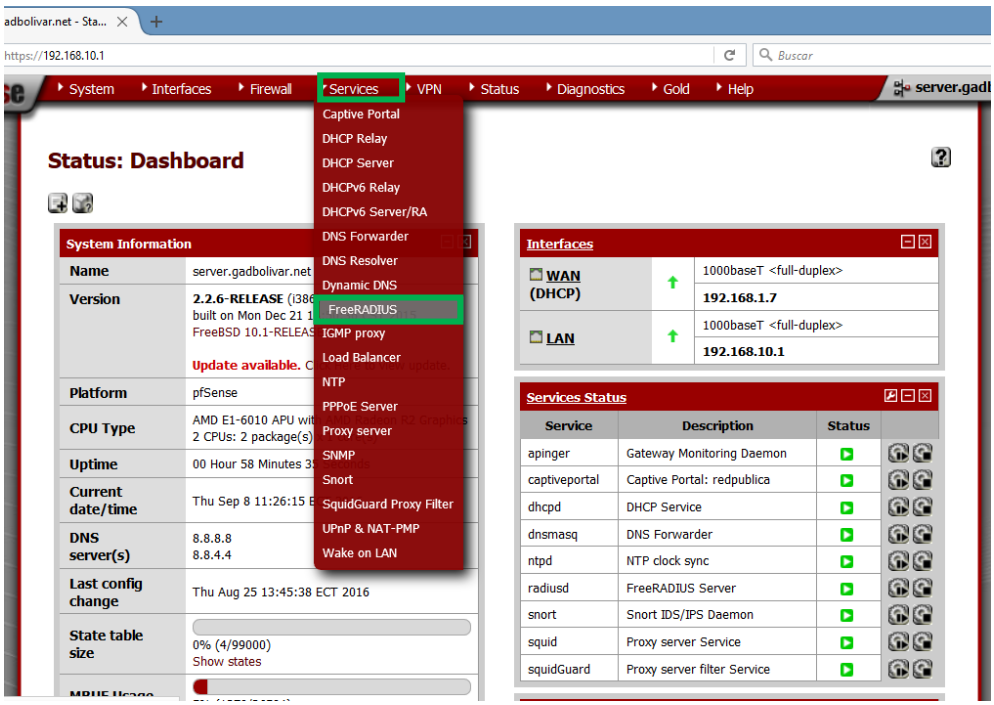
ANEXO 4

CONFIGURACIÓN DE FREERADIUS PARA LA ADMINISTRACIÓN DE LOS USUARIOS AL ACCESO A LA RED

Entrar al servidor pfSense vía web y logearse como administrador para acceder a las configuraciones.

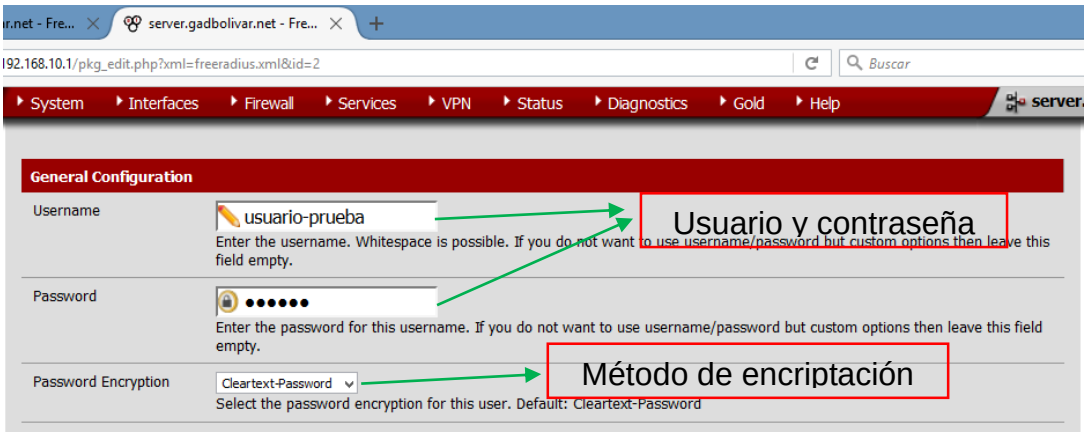


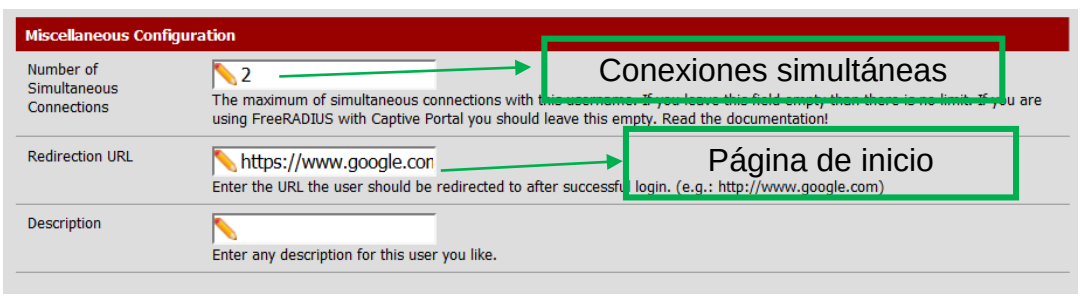
Una vez logeado aparecerá el panel o menú principal, escoger la opción services y freeradius.



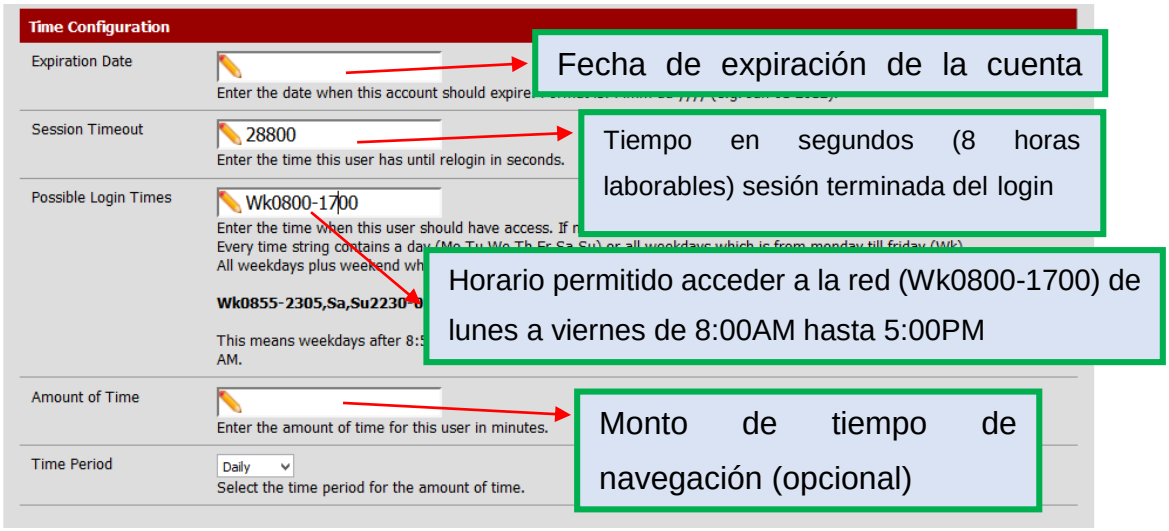
Se visualiza el menú donde se gestionan los usuarios que tendrán permiso de acceder a la red del GAD Municipal del Cantón Bolívar.

Dar clic en agregar nuevo usuario, para la configuración del nuevo registro.

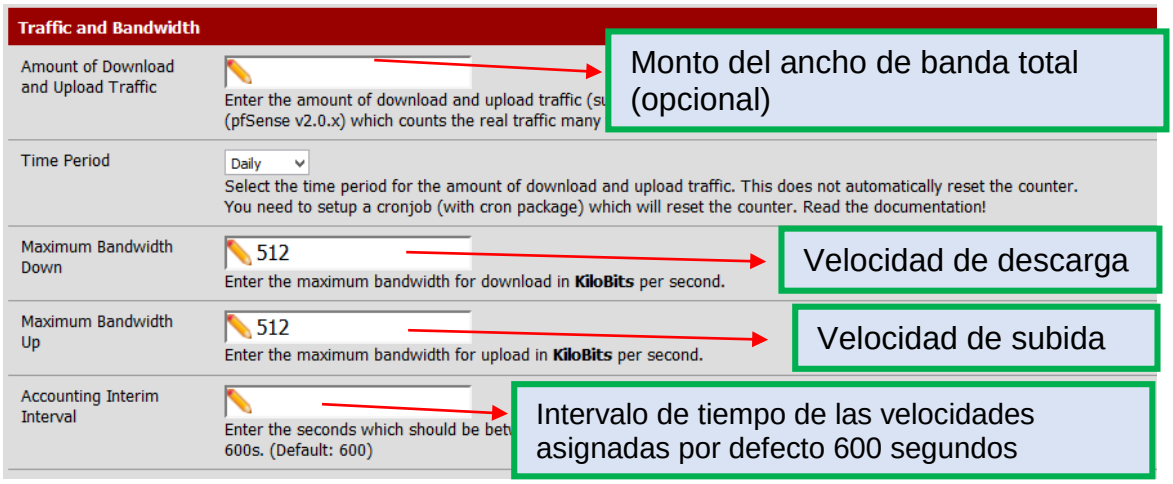




Configuración de horarios y permisos de acceso a la red



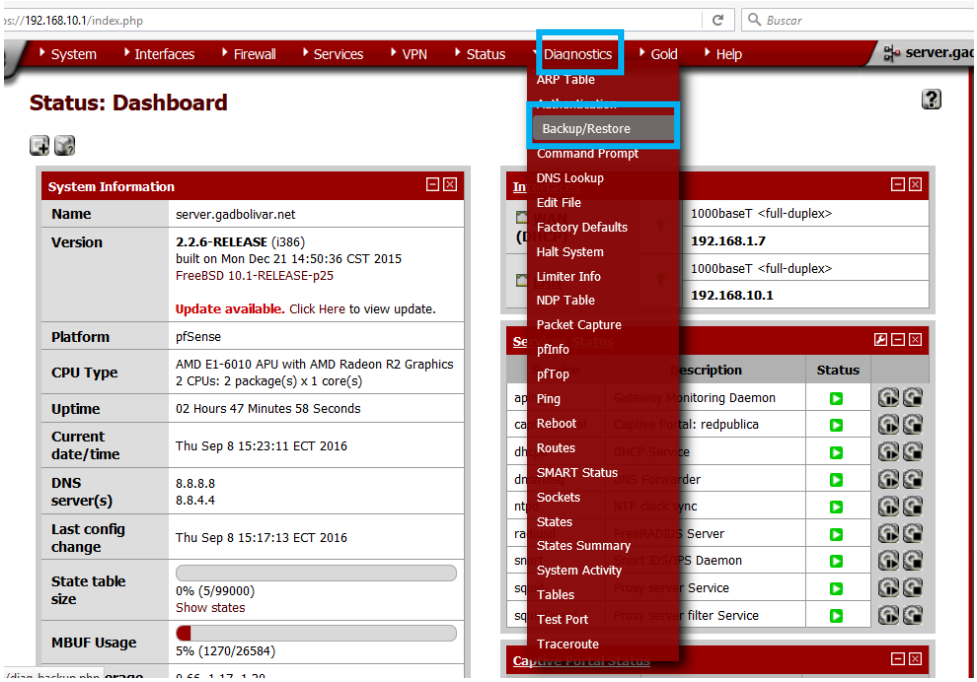
Configuración del ancho de banda



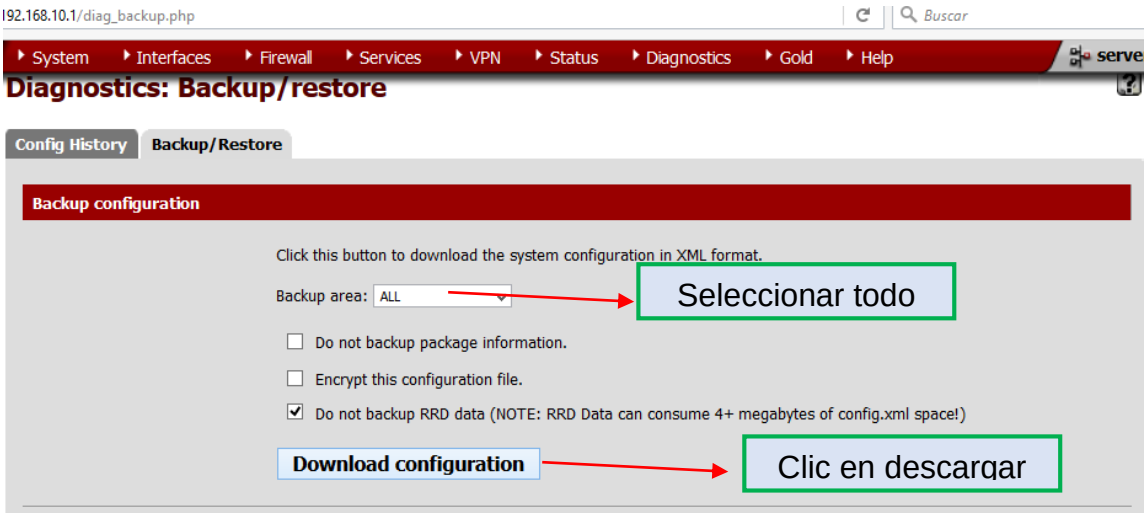
ANEXO 5

COPIA DE SEGURIDAD Y RESTAURACIÓN DE TODAS LAS CONFIGURACIONES DEL SERVIDOR PFSENSE

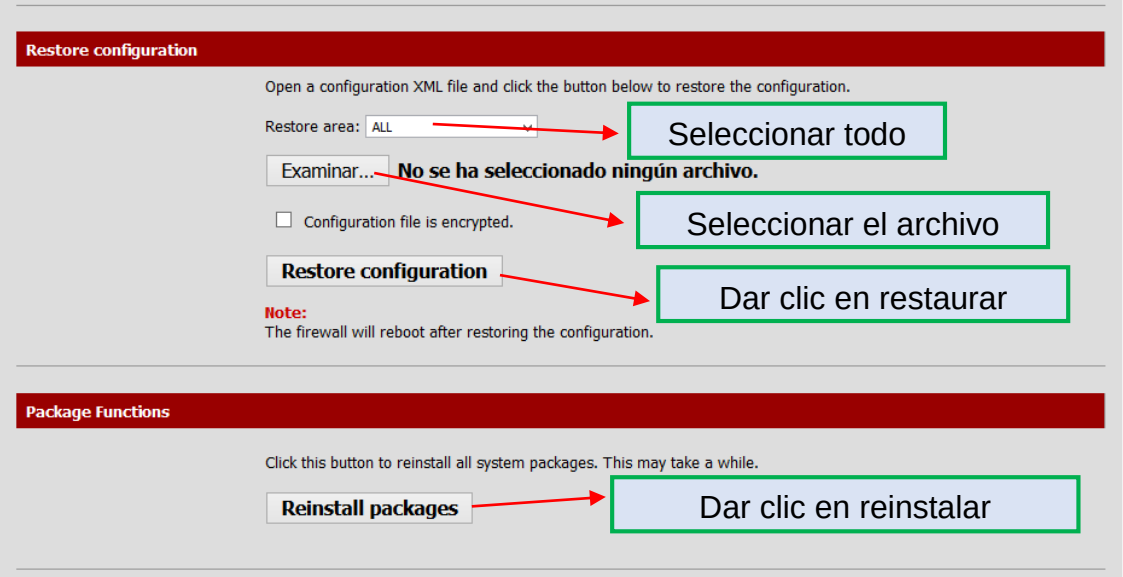
Previamente se debe haber logeado como administrador ir a la opción Diagnostics y Backup/Restore.



Realizar backup completo de las configuraciones del pfSense



Para realizar la restauración es necesario tener instalado la imagen del pfSense en la misma versión en la que se hizo el backup para evitar inconvenientes. Ir a la opción Diagnostics, Backup/Restore.



ANEXO 6

CERTIFICADO DE LA UNIDAD DE TECNOLOGÍA Y CONTRATACIÓN PÚBLICA DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR

Gobierno Autónomo Descentralizado
Municipal del Cantón Bolívar – Manabí
UNIDAD DE TECNOLOGIA Y CONTRATACION PÚBLICA

Calceta, 16 mayo del 2016.

Señora
Maritza Mendoza de Santos
JEFE DEL SUBPROCESO DE TALENTO HUMANO
En su despacho.-

Por medio de la presente tengo a bien informar a Usted que los Señores **JOSE LUIS PINARGOTE SANTANA** y **MARIA GABRIELA PAZMIÑO PALMA**, Estudiantes de la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM – MFL, realizaron la elaboración del trabajo de Investigación **SERVIDOR PARA AUTENTICACION EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTON BOLIVAR**, bajo la coordinación y supervisión del Señor Miguel Velásquez Murillo – Asistente Técnico de esta Unidad, trabajo que fue implantado en esta dependencia y se encuentra acorde a las necesidades y requerimientos de la Municipalidad.

Lo que informa a Usted para los fines legales y pertinentes.

Atentamente,

Ing. Verónica Vera Valdez
UNIDAD DE CONTRATACION PÚBLICA

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN BOLÍVAR
RECIBIDO
Fecha: 16 mayo 2016
Hora: 10.45
FIRMA AUTORIZADA

ANEXO 7

CERTIFICADO DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL
CANTÓN BOLÍVAR - MANABÍ
R.U.C.: 1360000390001

ESPECIE VALORADA
USD. 1,00

077957

CERTIFICACIÓN

Maritza Elizabeth Mendoza Vivas, Jefe del Subproceso de Talento Humano del Gobierno Autónomo Descentralizado Municipal del cantón Bolívar, CERTIFICA que los señores José Luis Pinargote Santana y María Gabriela Pazmiño Palma, Estudiantes de la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, desarrollaron la Investigación denominada SERVIDOR PARA AUTENTICACIÓN EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR, trabajo que fue implantado en la Unidad de Tecnología y Contratación Pública y satisface las necesidades y requerimientos de la Municipalidad.

Particular que certifico para los propósitos consiguientes.

Calceta, 16 de mayo del 2016

Sra. Maritza Mendoza Vivas
JEFE DEL SUBPROCESO DE TALENTO HUMANO
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN BOLÍVAR

ANEXO 8

AVAL DEL TUTOR

Carrera de COMPUTACIÓN

Calceta, 02 de agosto de 2016

Ingeniero
Daniel Agustín Mera Martínez, Mg.
Presidente del Tribunal de Hardware
Carrera de Computación - ESPAM MFL

Asunto: CARTA AVAL

En calidad de Tutor de la Tesis titulada:

"SERVIDOR PARA AUTENTICACIÓN EN LA RED DE COMUNICACIÓN DE DATOS DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR"

De los postulantes ***Pazmiño Palma María Gabriela*** y ***Pinargote Santana José Luis*** de la Carrera de Computación, considero que cumple con los requerimientos metodológicos y aportes científicos-técnicos suficientes, además de haber desarrollado los objetivos planteados. Motivo por el cual postulo y avalo la presente tesis para ser sometida a evaluación del Tribunal de Hardware, para su correspondiente revisión, sustentación y calificación.

Para los fines legales pertinentes, me suscribo a usted.

Atentamente,

Joffre Moreira
INGENIERO EN SISTEMAS INFORMÁTICOS
MAGÍSTER EN INFORMÁTICA DE GESTIÓN

03/08/2016

Mgtr. Joffre Moreira Pico
Carrera de Computación
ESPAM MFL
Correo: jmoreira@espam.edu.ec