UNIVERSIDAD AMAZÓNICA DE PANDO
ÁREA CIENCIAS Y TECNOLOGÍA
CARRERA INGENIERÍA INFORMÁTICA

INFORME FINAL DE PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE LICENCIADO EN INGENIERÍA DE **SISTEMAS INFORMÁTICOS**

"SISTEMA DE AUTENTICACIÓN, AUTORIZACIÓN Y ACCESO A LA RED LAN DEL GOBIERNO AUTÓNOMO MUNICIPAL DE COBIJA"

Postulante : Univ. Renelsy Rojas Gustañer.

Tutor Colectivo : Msc. Lic. Humberto Fernández Calle

Asesor : Ing. José Balderrama Méndez

Cobija- Pando – Bolivia

2013

Agradecimientos

A Dios

Por darme vida, salud y estar siempre presente en mis oraciones, en los momentos de alegría, desilusión, abatimiento, logros, fracasos y en momentos cuando más necesito.

A mi familia

Mi May y mi gran pá que siempre me brindaron su apoyo cariño y comprensión sin importar los momentos buenos o malos de mi vida.

A mi amado esposo por brindarme todo su apoyo incondicional, por estar siempre dándome un impulso para no desmayar en el camino, que no ser por su constante consejo me impulso para la culminación de este proyecto.

Mi amada y preciada hija Elsy Shecid por el gran amor que le tengo y además de estar siempre presente en todo los momentos de mi vida y por ser el regalo más preciado que Dios me dio.

A mis docentes

En especial al Ing. José Balderrama, Eduardo Zubieta y Lic. Humberto Fernández. Por los conocimientos e ideales impartidos durante todo el proceso de formación universitaria, además de compartir sus vivencias y brindar su amistad incondicional, que de alguna u otra manera ayudo en mi formación profesional.

A mis amigos y compañeros

A Tania por brindarme su amistad sincera y su colaboración desinteresada durante el trayecto de vida universitaria, y en el desarrollo del proyecto final

A la Ing. Silvia Caraballo, Jefa de la Unidad de Sistemas del Gobierno Autónomo de Cobija y a mis colegas de trabajo, por confiar y darme la oportunidad de realizar este proyecto de grado en esta institución.

A todas las personas que de alguna manera contribuyeron e hicieron posible la realización de este proyecto de grado mil gracias.

Dedicatoria

A mi madre Carmen Gustañer Reyes, por el cariño que siempre me da, por impulsarme y apoyarme incondicionalmente en el proceso de mi formación profesional.

A mi amado esposo Rene Emigdio Yana Choque, por el amor que me da día a día, por impulsarme y apoyarme en proceso de mi formación profesional y el desarrollo de este proyecto.

A mi hija Elsy Shecid Yana Rojas, que fue la fuente de inspiración y motivación, durante el desarrollo de este proyecto.

RESUMEN

Desde los inicios de la historia de la humanidad el hombre ha sentido la necesidad de resguardar elementos que le permitan sobrevivir en su entorno desde alimentos y objetos que permitan su subsistencia, en la actualidad el concepto de seguridad ha prevalecido pero los elementos que protege ha cambiado y uno de ello es la información que se ha convertido en lo más preciado por países, naciones y en especial por organizaciones. Actualmente la información con la tecnología de las comunicaciones puede ser distribuida a diferentes niveles de la sociedad con el fin de promover el bienestar de la humanidad, pero estas mismas tecnologías ha permitido su uso inadecuado y obtener réditos de manera ilegal y en especial si esta información es parte de una red de computadoras.

Mediante la ejecución del presente Proyecto de Grado, se logró la implementación de un sistema de autenticación, autorización y registro, a través de un servidor Radius e integrando el manejador de bases de datos LDAP apoyado por la política de seguridad de acceso a los recursos de la red del Gobierno Municipal la cual valida el acceso con el fin de contrarrestar el problema principal que es la carencia de control de acceso a la red permitiendo así controlar el acceso lógico a los recursos, este proceso de autenticación permite validar las credenciales que son enviadas al servidor de autenticación que se encarga de aceptar o denegar el acceso a fin de evitar la manipulación directa de información y uso indiscriminado de los recursos a terceros. La Metodología utilizada es la basada en acciones que implica que para cada objetivo específico se plantean actividades o acciones en base a la teoría que permitirá su desarrollo y los instrumentos propuestos por ella.

ÍNDICE

CAPÍTULO I
INTRODUCCIÓN

PÁG.

CAPÍTULO II
MARCO TEÓRICO

CAPÍTULO III

IMPLEMENTACIÓN

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

LISTA DE TABLAS

PÁG.

LISTA DE FIGURAS

PÁG.

CAPÍTULO I
INTRODUCCIÓN

Este capítulo describe los antecedentes y razones para realizar el proyecto de grado en el Gobierno Autónomo Municipal de Cobija, determinando problemas de carencia en el control de acceso a la red LAN existente, describiendo las causas que ocasionan los efectos, la solución propuesta, los objetivos que se cumplirán en busca de lograr la eficiencia en el control de acceso a los recursos de la red de la institución.

1.1. ANTECEDENTES Y MOTIVACIÓN

Desde principio de la historia el ser humano vio la necesidad de resguardar sus pertenencias y generar aspectos de autenticación a sus capitales, que con el transcurrir del tiempo las pertenencias más valiosas son el conocimiento y la información, este último, se dice puede alterar economías de países, generar problemas sociales, información que actualmente se encuentra en sistemas de información que son parte de una red de datos, mismo que debe ser resguardada y para que esta tenga un nivel de seguridad aceptable las diferentes entidades públicas y privadas a nivel mundial establecen mecanismos de protección que permitan identificar y minimizar su vulnerabilidad.

En relación a lo anterior se establecen formas de seguridad que permitirán resguardar la información de una organización las cuales son la física y la lógica, se entiende que el primero es la aplicación de barreras físicas y mecanismos de control como medidas de precaución ante amenazas a los recursos e información confidencial y la última a través de la aplicación de barreras y procedimientos que resguarden el acceso a los datos o recursos de la red y solo se permita acceder a ellos a las personas autorizadas para hacerlo. (Borghello, 2001)

El Gobierno Autónomo Municipal de Cobija (GAMC), no es ajeno a este contexto para lo cual desde la implementación de su red LAN en su predio central se han ido desarrollando trabajos que han pretendido resguardar la información que se encuentra en los diferentes sistemas informáticos los cuales se encuentran interconectados, trabajos que permitieron en su momento minimizar la vulnerabilidad de la red, estos son, “Administración de la red de datos e Internet”, desarrollado por el universitario Daniel Torrico, integrando los conceptos de seguridad informática en las redes LAN.

La red Informática del Gobierno Autónomo Municipal de Cobija se encuentra en un proceso de reestructuración e implementación, el mismo también se encuentra en un punto inicial para su administración en la distribución del ancho de banda del servicio de Internet a lo cual se suma la necesidad de brindar a la red seguridad, escalabilidad y flexibilidad que compromete el uso de mecanismos y herramientas aun no implementados como es el de autenticación y autorización, redes virtuales (VPN), monitorización entre otros, lo que se considera motivante en el aspecto de poder implementar mecanismos de seguridad que apoyen a la mejora en la administración de la red.

En tal sentido de acuerdo a lo descrito y la complejidad actual de la red LAN del GAMC se define que existe un insuficiente control de acceso a los recursos que existen en la red LAN del predio central del Gobierno Municipal de Cobija, en base a este problema se plantea la propuesta de implementar el control de acceso a los recursos de la red LAN del predio central del GAMC.

A fin de cumplir con la anterior proposición se toma como referencia principal los proyecto de **"Seguridad Informática, sus implicancias e implementación"** realizado por A.S.S. Borghello, Cristian Fabián, en la Universidad Tecnológica Nacional-2001 y la tesis: **"Diseño de un sistema de seguridad informática-caso: CADE Bolivia S.A."** Víctor Adrián Gutiérrez Tintares-2004 de la Escuela Militar de ingeniería de Bolivia, además de tomar como base metodológica el "**Método Basada en Acciones", EMI-Zegarra 2008,** el cual permite cumplir el objetivo general al cumplimiento de los objetivos específicos que se cimientan en base a la fundamentación teórica que considera para su ejecución y los instrumentos que deberá utilizar.

En tal sentido el propósito del proyecto de grado es, implementar un sistema que proporcione los servicios de Autenticación, Autorización y Registro AAA[1], para operabilizar los recursos que provee la red del GAM, apoyado por el desarrollo de políticas de acceso a los recursos de la red.

1.2. DESCRIPCIÓN DEL PROBLEMA

En base a la recopilación de la información obtenida, mediante la observación directa a los involucrados en la sección de redes del GAMC, se puede identificar las siguientes causas relacionadas a los problemas de los recursos de la red:

[1]AAA[Aauthentication), Authorization), Aaccounting=Registro a menudo traducido también como contabilidad)

- No existen mecanismos de seguridad para el control de acceso.
- Falta de generación de reportes de control de acceso a los recursos.
- Inexistencia de políticas de control de acceso a la red
- Deficiente administración del control de acceso a los recursos de la red.

A consecuencia de los problemas mencionados anteriormente se define como problema principal: la "**Carencia de control de acceso a la red LAN del predio central del Gobierno Autónomo Municipal de Cobija"**

En consecuencia el problema mencionado, trae consigo efectos observables como:

- Cómodo ingreso a los sistemas de información por parte de intrusos
- Modificación y robo de información de los sistemas de información.
- Acceso irrestringido a los sistemas de información y recursos de la red.
- Uso indiscriminado de los recursos de la red
- Demora en la identificación de intruso en la red y la toma de decisiones.

1.3. SOLUCIÓN PROPUESTA

Tomando en cuenta los requerimientos se considera como características de la propuesta de proyecto de grado las siguientes:

- ✓ Autentificar a los usuarios por código y clave a través de un servidor Radius.
- ✓ Políticas de seguridad
  - o Control de acceso
  - o Uso de los recursos de red

Que permitirá él:

- ✓ Control y monitoreo de acceso de los usuarios a la red.
- ✓ Minimizar la vulnerabilidad de la red por ataques internos.
- ✓ Reglamentar por autoridad competente el uso de los recursos de la red.

1.4. OBJETIVOS

1.4.1. Objetivo general

Implementar el control de acceso a la red LAN del predio central del Gobierno Autónomo Municipal de Cobija través de un sistema de autenticación, autorización y registro para minimizar su vulnerabilidad.

1.4.2. Objetivos específicos

- Investigar los antecedentes de la red LAN, para identificar las vulnerabilidades a través de la recopilación de información.
- Analizar el desempeño de la red, a través de la Metodología para la medición y evaluación del desempeño de redes LAN.
- Diseñar el sistema de control de acceso a la red informática para el control de acceso a los usuarios.
- Implementar el mecanismo de seguridad de Control de Acceso, para controlar los recursos de la red informática.
- Desarrollar políticas de acceso a los recursos de la red.

1.5. ALCANCES.

Los alcances que se logran con el presente proyecto son:

- Instalación y configuración del sistema de autenticación, autorización y acceso en el predio central del Gobierno Autónomo Municipal de Cobija.
- Gestionar el acceso del usuario a los recursos disponibles en la red, proporcionándole al usuario todo su perfil (privilegio y atributos), de acuerdo a su jerarquía de trabajo.
- Gestión de usuarios.
- Elaborar e implementar políticas de seguridad para el control de acceso a los recursos de la red.

1.6. METODOLOGÍAS Y HERRAMIENTAS UTILIZADAS

La metodología empleada en el presente proyecto de grado es el diseño metodológico “Basado en acciones”, mismo que está enfocado en las acciones a desarrollar para lograr los

objetivos específicos que nos llevan a cumplir con el objetivo general planteado, estas acciones permiten lograr cada objetivo específico, permitiendo así definir el contenido del sustento teórico, el diseño de la investigación y la redacción del temario tentativo del documento final. Entonces el presente proyecto de grado define las acciones a tomar para cada uno de los objetivos específicos con fundamentación teórica y el uso de instrumentos de acuerdo al siguiente diseño metodológico.

TABLA 1.1: *Diseño metodológico*

Fuente*: Elaboración propia.*

OBJETIVOS ESPECÍFICOS	ACCIONES	INSTRUMENTO
Investigar los antecedentes de la red LAN, para identificar las vulnerabilidades.	• Averiguar los antecedentes de la red LAN, para identificar las vulnerabilidades. • Identificar aquellos recursos con mayor probabilidad de ataques internos y externos para salvaguardarlos contra pérdidas y daños.	• Hoja de trabajo para desarrollar un planteamiento de seguridad. • Hoja de trabajo para el análisis de riesgo de seguridad en la red. • Hoja de trabajo para otorgar acceso a los recursos de sistema y red. Software ZENMap.
Analizar el desempeño de la red, a través de Analizar y verificar los recursos de la red la Metodología para la medición y evaluación del desempeño de redes LAN.	• Escaneo de la red con el software Wireshark • Interpretación de la información • Elaboración de cuadros estadísticos de tráfico en la red.	Software: • Wireshark • Cuadros estadísticos
Diseño del sistema de control de acceso a la red informática.	• Desarrollar el diseño lógico de la ubicación física del servidor Freeradius	
Implementar el mecanismo de seguridad de control de acceso, para operabilizar los recursos de la red de datos.	• Configuración del servidor FreeRadius	Protocolo RADIUS Servidor RADIUS LDAP
Desarrollar políticas de acceso a los recursos de la red.	• Elaborar la propuesta de políticas de acceso a los recursos de la red	✓ Guía de elaboración de políticas de seguridad para una red

1.7. ORGANIZACIÓN DEL DOCUMENTO

Capítulo I: Es la etapa donde se establece la parte introductoria del proyecto de grado donde se describe la introducción, el problema, la solución propuesta, objetivos planteados, alcances y la metodología a utilizar.

Capítulo II: Hace referencia a los fundamentos teóricos y conceptuales del tema, la metodología, herramientas y técnicas aplicadas en el desarrollo, sobre los cuales se fundamenta el Proyecto de Grado.

Capítulo III: En este capítulo se realiza la ejecución del proyecto en base la metodología, sus etapas y actividades como ser el análisis previo, planeación del diseño de implementación, instalación y configuración y puesta en marcha del servicio, hasta la administración del sistema, definida el cual se presentara los resultados previamente ejecutados.

Capítulo IV: Este capítulo refleja las conclusiones obtenidas del proyecto de grado, en base a los objetivos planteados en el primer capítulo manifestando el grado de alcance y las recomendaciones para mejorar o ampliar este servicio, dentro de la institución

CAPÍTULO II
MARCO TEÓRICO

El presente capítulo presenta el sustento teórico sobre la cual se basa el desarrollo del presente proyecto de grado. Se define en primera instancia el marco institucional, seguido por los aspectos legales considerados de acuerdo a la documentación actual relacionada al tema de seguridad de la información, continuando con una descripción detallada de la seguridad en redes de datos y sus aspecto más importante el de redes de datos, la cual podrá apoyarse con teoría relacionada a su administración, a continuación se resalta uno de los aspectos más importantes del proyecto que es la seguridad en las redes de datos y por último la revisión bibliográfica relacionada al desarrollo de políticas de acceso a las redes de datos.

2.1. MARCO INSTITUCIONAL

El Gobierno Autónomo Municipal de Cobija (GAMC), es una de las principales entidades pública con autonomía de gestión, con personalidad jurídica y patrimonio propio, que presta servicios y promueve el desarrollo sostenible del municipio para mejorar la calidad de vida y satisfacer las necesidades de la población. (MISIÓN DEL GAMC).

En vista de la creciente demanda de población hacia los servicios del municipio esta se ve obligada a tener que hacer cambios en su estructura y equipamiento para satisfacer los servicios requeridos, al igual que en otras organizaciones e instituciones que el resto del país.

La unidad de sistemas se vio en la necesidad de reestructurar la red local para el uso compartido de información y recursos que esta ofrece, en la actualidad existe un servicio de Internet, para operar los diferentes sistemas de información como ser RUAT (Registro único para la administración tributaria municipal), SISIN, SINCOM, DAVINCHI, SITRAM Y SICOES, por lo que la división de redes e Internet realiza la administración de este servicio.

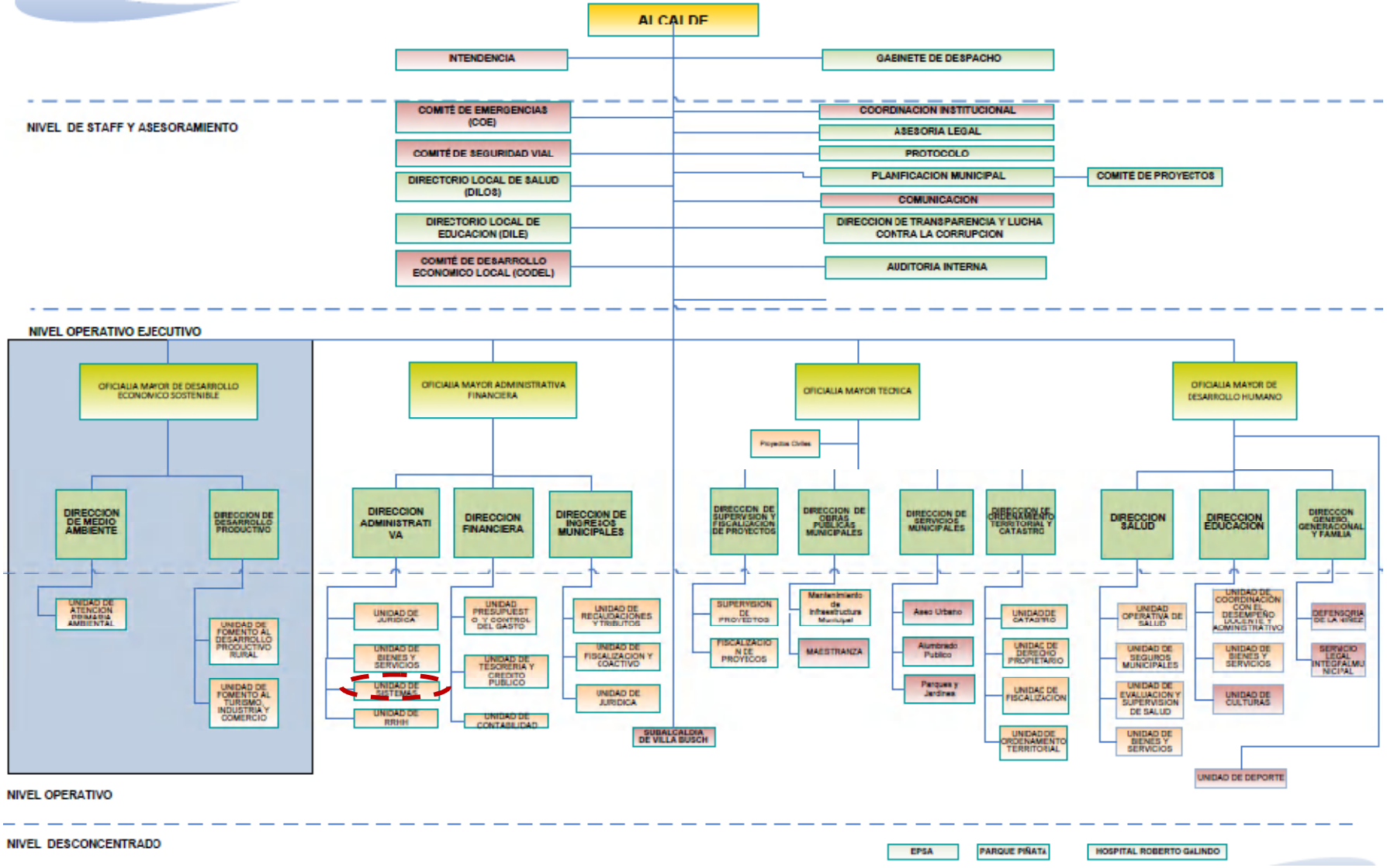


FIGURA 2.1: Organigrama general del Gobierno Autónomo Municipal de Cobija.

Fuente: *Gobierno Autónomo Municipal de Cobija*

2.2. MARCO LEGAL

El GAMC basa la implementación de las tecnologías de información y comunicación en cumplimiento al:

Artículo 103 de la Constitución Política del estado Plurinacional de Bolivia, donde el estado deberá garantizar el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general, además asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación en las empresas productivas y de servicio públicas para fortalecer la base productiva e impulsar el desarrollo integral de la sociedad, de acuerdo con la ley.

El presente proyecto de grado basa su principio de desarrollo en cumplimiento a la Ley 164 General de Telecomunicaciones 164 Articulo 5, en los principios de:

2.2.1. Continuidad. Los servicios de telecomunicaciones y tecnologías de información y comunicación, así como el servicio postal, deben prestarse en forma permanente y sin interrupciones, salvo los casos previstos por norma.

2.2.2. Inviolabilidad. Las conversaciones o comunicaciones privadas efectuadas a través del uso de telecomunicaciones y tecnologías de información y comunicación, así como del servicio postal, son inviolables y secretas, no pudiendo ser interceptadas, interferidas, obstruidas, alteradas, desviadas, utilizadas, publicadas o divulgadas, salvo en los casos determinados por Ley.

2.3. MARCO CONCEPTUAL

2.3.1. Redes de Datos.

Según (José María Barceló Ordinas, 2004), es el conjunto de componentes informáticos (computadora, impresoras, conmutadores, etc.), que se encuentran físicamente conectados y programas informáticos empleados para conectar dos o más computadoras.

Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos. Una red de datos es un sistema de comunicación entre computadoras que permite la transmisión de

datos de una máquina a otra con lo que se lleva a cabo un intercambio de todo tipo de información y de recursos una red está integrada por los siguientes componentes:

- Clientes: usuarios de la red como Pc´s- laptops, impresoras, cámaras, teléfonos, etc.
- Servidores de aplicaciones y base de datos
- El hardware de red, que comprende la infraestructura física de la red a la cual se conectan los clientes y servidores. Como ejemplo se tiene a los switches y hubs, routers, access points y tarjetas de red.

2.3.1.1. Clasificación de las redes.

Las redes se pueden clasificar de diferentes maneras. Las principales clasificaciones son: (Telefonica de España, 2006).

a) Por su uso: se clasifican en redes privadas o corporativas y redes públicas.

b) Por su conexión física: se clasifican en redes punto a punto (unicast) y redes multipunto o de difusión (broadcast).

c) Por su técnica de transmisión de datos:

- Líneas dedicadas. Enlace punto a punto permanente y siempre disponible. Se utilizan principalmente en redes WAN[2] con velocidades prefijadas por el proveedor, generalmente simétricas y full-duplex. Otro caso habitual es el radio enlace.
- Modelos de circuito conmutado (Circuit Switching). En ellos las comunicaciones no comparten los medios. Al iniciarse la comunicación se reserva los recursos intermedios necesarios para establecer y mantener el circuito. Si el canal se corta se corta la comunicación. Los dispositivos mantienen información sobre el estado de la comunicación (statusfull).

  Una vez establecido el circuito se comporta como una línea dedicada ofreciendo un transporte físico de bits sobre el que se puede utilizar cualquier protocolo de nivel de enlace. El costo es proporcional al tiempo y la distancia de conexión.
- Modelos de paquetes conmutados (Packet Switching). En ellos las comunicaciones se dividen en paquetes que comparten los medios. Se pueden utilizar varios enlaces

[2] Redes de área extensa (WAN: Wide Area Network)

en cada interfaz físico. Ofrece un medio físico de transmisión de datos para los equipos. Existen dos submodelos:

- Datagramas: Cada paquete debe estar delimitado e identificado y llevar la dirección destino, y cada uno se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo. En este modelo no sabemos si los paquetes van a llegar todos ni si van a llegar por orden (ni si van a llegar sin errores). Los dispositivos no mantienen información sobre el estado de la comunicación (stateless). Es el modelo más sencillo de implementar y el único que soporta multidifusión (multicast). Se puede asimilar al sistema de correo tradicional.
- Circuitos virtuales (VC: Virtual Circuit): Simula un circuito conmutado, pero compartiendo los medios.

  Primero se establece una conexión y los equipos intermedios reservan una parte de sus recursos; después todos los paquetes siguen la misma ruta ordenadamente. Este modelo es utilizado en telefonía digital GPRS y redes como X.25.

d) Por su topología: Según (José María Barceló Ordinas, 2004)se entiende por topología de una red local la distribución física en la que se encuentran dispuestos los ordenadores que la componen. De este modo, existen tres tipos, que pueden llamarse "puros" los cuales son: anillo, bus y estrella.

La topología de una red es el diseño de las comunicaciones entre los nodos de la red, estas pueden ser:

- Red en bus
- Red en estrella
- Red en anillo (o doble anillo)
- Red en malla (o totalmente conexa)
- Red en árbol
- Red mixta (cualquier combinación de las anteriores)

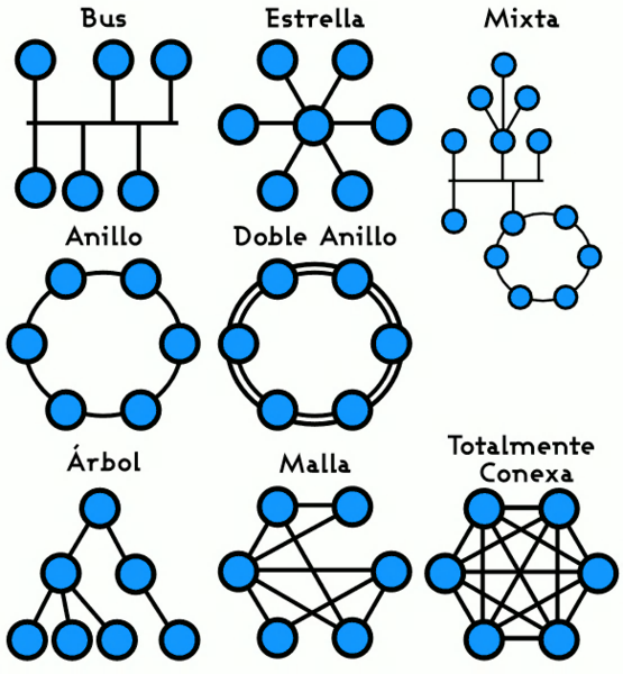


FIGURA 2.2: *Topologías de red*
Fuente: *(Creative Commons, 2009)*

Hay que diferenciar entre la topología física, que define como están conectados físicamente los nodos y la topología lógica que es como tratan los nodos las conexiones.

En este caso para el desarrollo del presente proyecto se toma en cuenta la topología Estrella Extendida que tiene una topología en estrella central, con cada uno de los nodos extremos de la topología en estrella, como se muestra en la Figura 2.3.

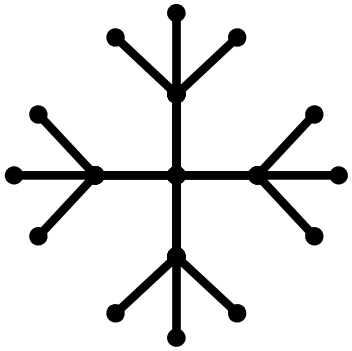


FIGURA 2.3*: Topología de red estrella extendida*
Fuente: *(José María Barceló Ordinas, 2004)*

La ventaja es que hace, que el cableado sea más corto y limita el número de dispositivos necesarios para interconectar cualquier nodo central. Una topología en estrella extendida es jerárquica y se puede configurar (con el equipo apropiado) para "animar" a que el trafico permanezca local.

e) Por su extensión: Redes de área personal (PAN), local (LAN), extensa (WAN), la siguiente tabla ejemplifica de manera clara este tipo de clasificación**.**

TABLA 2.1: *Clasificación de las redes por su extensión*
Fuente: *Modificado (Creative Commons, 2009).*

DIAMETRO	TIPO
< 0,01 m	Paralelismo masivo. Procesadores multi - núcleo
< 0,1 m	Multiprocesadores
< 10 m	Redes de área personal (Pan: Personal Área Network), Redes de infrarrojos o bluetooth
10m – 3 km	Redes de área local (LAN: Local Área Network) y metropolitana (MAN). Ethernet, Wi-Fi.
> 3 km	Redes de área extensa (WAN: Wide Area Network) o redes interconectadas. Frame-Relay, RDSI, ATM, SONet/SDH.

2.3.2. Redes de Área Local.

Dentro de la clasificación de las redes tomaremos a continuación aquella que se relaciona de manera directa al desarrollo del presente proyecto y su extensión geográfica como ser las redes de Área Local LAN.

La cuestión de compartir recursos entre computadoras ha adquirido mayor importancia en la medida en que estas se han convertido en instrumentos cada vez más habituales. Los recursos compartidos incluyen por lo general datos propios o sensibles, impresoras y otros tipos de aplicaciones. Como respuesta a la necesidad de compartir recursos, se ha desarrollado un tecnología de red de área local (LAN) para permitir que múltiples computadoras que se encuentran en una misma habitación o edificio puedan

comunicarse entre sí, en lugar de estar conectada cada computadora individualmente con todas las demás computadoras, todas las que forman parte de una LAN están preparadas para compartir un medio común (es decir, el cable) De este modo cualquier comunicación que se produce en la LAN se transmite inmediatamente a todas las computadoras conectadas a la misma.

Entonces: Una red de área local es un sistema que permite la interconexión de ordenadores que están próximos físicamente. Entendemos por próximo todo lo que no sea cruzar una vía pública: una habitación, un edificio, un campus universitario, etc. (José María Barceló Ordinas, 2004).

El objetivo básico de una red LAN es la de compartir recursos entre diferentes ordenadores próximos (un sistema de almacenamiento masivo, una impresora o un dispositivo de conexión hacia el exterior, por ejemplo). Para este tipo de comunicaciones se propuso una filosofía de diseño basada en la difusión de tramas con medio compartido, de manera que cuando una estación pone una trama en el medio, el resto de estaciones puedan recibirla.

Los receptores reales de la trama se la quedan y el resto, la ignora. Para cumplir con el propósito de difusión de tramas existen dos protocolos LAN que gozan de mayor aceptación para las redes LAN estas son: Ethernet, desarrollado por los ingenieros de la Xerox Corporation y Token Ring, desarrollado por los de la IBM Corporation. Ambos utilizan este método de retrasmisión para comunicarse con otras computadoras; difieren principalmente en el método que emplean para determinar quién puede comunicarse a continuación en la LAN. (Sharp, 2004).

En las LAN Ethernet, las computadoras deben asegurarse de que no existe tráfico antes de transmitir la información; en las LAN Token Ring, las computadoras envían un testigo de acceso especial a lo largo de la red para permitir la transmisión de datos.

Otra mejora importante ha sido la aparición de las redes de área local inalámbricas (wireless LAN), en las que el enlace entre estaciones no se lleva a cabo por medio de cables, sino por medio de enlaces radioeléctricos. Las ventajas de este tipo de enlaces, en cuanto a movilidad y facilidad de instalación, son evidentes.

2.3.2.1. Características de una red local.

Los ordenadores conectados a una red local pueden ser grandes ordenadores u ordenadores personales, con sus distintos tipos de periféricos. Aunque hay muchos tipos de redes locales entre ellas hay unas características comunes:

a) Un medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. Las redes locales están contenidas en una reducida área física: un edificio, un campus, etc.

b) Una velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo. El equipo de la red local puede transmitir datos a la velocidad máxima a la que puedan comunicarse las estaciones de la red, suele ser de un Mb por segundo.

c) Una distancia entre estaciones relativamente corta, entre unos metros y varios kilómetros.

d) La posibilidad de utilización de cables de conexión normales.

e) Todos los dispositivos pueden comunicarse con el resto y algunos de ellos pueden funcionar independientemente.

f) Un sistema fiable, con un índice de errores muy bajo. Las redes locales disponen normalmente de su propio sistema de detección y corrección de errores de transmisión.

g) Flexibilidad, el usuario administra y controla su propio sistema.

h) Los dos tipos básicos de dispositivos que pueden conectarse a una red local son las estaciones de trabajo y los servidores:

- Una estación de trabajo es un ordenador desde donde el usuario puede acceder a los recursos de la red.
- Un servidor es un ordenador que permite a otros ordenadores que accedan a los recursos de que dispone. Estos servidores pueden ser:

  - Dedicados: son usados únicamente para ofrecer sus recursos a otros nodos.
  - No dedicados: pueden trabajar simultáneamente como servidor y estación de trabajo.

En una red es imprescindible identificar los ordenadores que forman parte de la misma. Cuando un ordenador genera una trama para otro, además de los datos que le quiere enviar, le pone el identificador del ordenador (u ordenadores) destino y el suyo, para que quien reciba la trama pueda saber quién se la ha enviado.

Para construir una red local, se precisan básicamente dos cosas: hardware (tarjetas, cables, conectores, etc.) y un software que sea consciente de que existen diferentes máquinas conectadas y ofrezca los servicios necesarios para que las aplicaciones puedan aprovecharlo.

2.3.2.2. Tipos de Redes

La clasificación de redes que se hace de acuerdo al medio de comunicación que utilizan, estas son: redes alámbricas que utilizan medios guiados, como cable coaxial, cable de par trenzado y fibra óptica. Si el tipo de medio que se utiliza es radio, infrarrojo o microondas son llamadas redes inalámbricas. A continuación se dará una breve explicación en qué consisten las redes alámbricas y redes inalámbricas.

a) Redes Alámbricas ó wirednetworks, estas se comunican a través de cables de datos en tecnologías IEEE[3] 803.3 (Ethernet), Los cables de datos conocidos como cables de red conectan computadoras y otros dispositivos que forman parte de las redes, este tipo de red son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades. Entre las ventajas de las redes alámbricas se tiene que, si se planean correctamente, sus costos de instalación son relativamente bajos, ofrecen un buen rendimiento, y cuentan con gran velocidad. En la mayoría de las organizaciones se utiliza este tipo de red. Algunas desventajas que pueden presentar este tipo de redes son el paso de los cables a través del acceso físico, en caso de que no se planeen correctamente pueden tener costos de instalación altos, pueden presentar dificultad en su expansión y se requiere que los dispositivos se encuentren físicamente en un nodo de la red para poder operar. En la figura 2.4 se puede apreciar la conexión entre los dispositivos de una red Alámbrica.

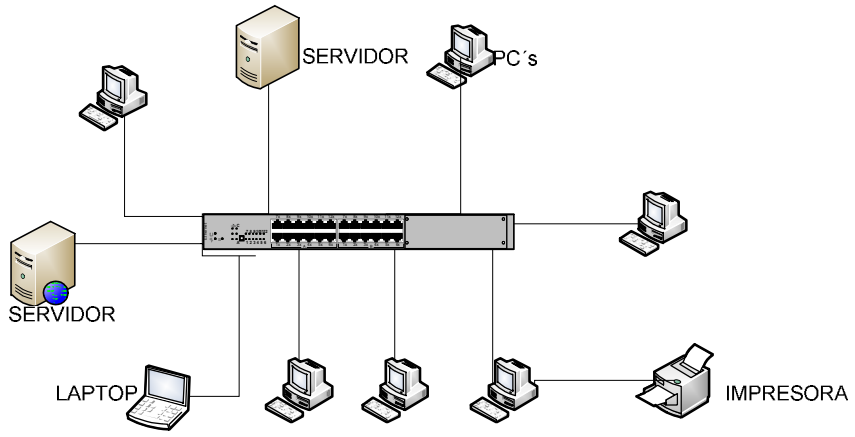


FIGURA 2.4*:* Red Alámbrica

Fuente: Elaboración Propia

b) Redes Inalámbricas o wireless networks, son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediantes ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas. Cuentan con la

[3] Instituto de Ingenieros Eléctricos y Electrónicos

libertad y la flexibilidad de operar dentro y entre edificios, proporciona todas las características y ventajas de la tecnología LAN tradicionales sin limitaciones de los cables. La libertad de moverse manteniendo la conectividad ha ayudado a que las redes inalámbricas alcancen una gran aceptación. Algunas ventajas de este tipo de redes son:

- Rápida instalación de la red sin la necesidad de usar cableado.
- Movilidad, los usuarios pueden permanecer conectados a la red incluso cuando no se encentren en sus mesas.
- Accesibilidad, todos los equipos portátiles y la mayoría de los teléfonos móviles de hoy en día vienen equipados con la tecnología WI-FI necesaria para conectarse directamente de una LAN inalámbrica.
- Productividad, el acceso a la información y a las aplicaciones clave de una empresa ayuda a su personal a realizar su trabajo y fomentar la colaboración.
- Escalabilidad, conforme crecen las operaciones comerciales de una empresa, puede que se necesite ampliar la red rápidamente.

Generalmente, las redes inalámbricas se pueden ampliar con el equipo existente, reduciendo costos, mientras que en una red cableada puede necesitar cableado adicional.

Las redes inalámbricas se clasifican de acuerdo a la cobertura que abarcan en redes de Área Local Inalámbricas, Wireless LANs (Wireless Local Área Networks), redes de Área Metropolitana Inalámbricas, Wireless MANs (Wireless Metropolitan Área Networks) y redes de Área Amplia Inalámbricas, Wireless WANs (Wireless Wide Área Networks), a continuación se hace hincapié en las Wireless LANs, debido que nuestra red de trabajo es de este tipo.

- Wireless LANs. Proporcionan las características de las redes alámbricas y agregan las ventajas de la redes inalámbricas, como la movilidad de usuarios. En estas redes se pueden encontrar tecnologías inalámbricas basadas en WI-FI

(Wireless Fidelity), que es un conjunto de stándares certificados por una alianza independiente llamada WI-FI Alliance.

Los estándares sobre los que trabaja Wi-Fi forman parte de la serie 802.11 del grupo IEEE y actúan sobre las capas uno y dos del modelo OSI. Enseguida se explica de manera general su modo de funcionamiento y sus componentes:

- Punto de Acceso, AP (Access Point). Es el Servidor de Acceso a la Red, NAS (Network Access Server), capaz de trabajar sobre una red de radiofrecuencia, que se utiliza para hacer de intermediario en las comunicaciones inalámbricas entre equipos o para convertir una red cableada en inalámbrica.

  - Identificador de Celda de Servicio, SSID (Service Set IDentifier). Es un nombre de red para definir la red a la que se quiere conectar algún usuario. Este nombre de red se divulga por parte del AP mediante beacons, que son pequeños paquetes, los cuales se utilizan para localizar la red, así como para mostrar sus características.

  - Canal. Dependiendo del tipo de red Wi-Fi y de su normativa, el espectro o espacio radioeléctrico asignado para el desempeño de estas redes se divide en canales. Estos canales definen unas frecuencias fijas de trabajo para los equipos que los utilizan.

  - Cobertura. El área o la zona de cobertura de una AP la determina la potencia de transmisión del equipo y el equipo de antenas que se va a utilizar, además de otros factores externos como las estructuras de las construcciones o el clima.

  - Antenas. Cada antena tiene un diseño diferente, según la direccionalidad de la antena, ésta se puede clasificar en antena isotrópica (que transmite a igual potencia en todos sus ángulos, creando una proyección en forma de

una esfera), antena omnidireccional (parecida a la antena isotrópica, transmite en horizontal hacia todos los ángulos), y antena direccional (enfoca mayoritariamente la señal hacia ángulos más concretos). En la figura 2.5 se pueden apreciar los componentes de una Wireless LAN

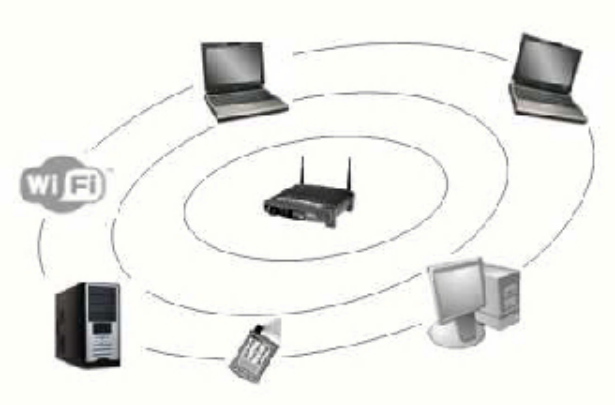


FIGURA 2.5: Componentes de una Wireless LAN
Fuente: (Cordoba Téllez Anabel, 2010)

2.3.3. Administración de redes

La Administración, es la ciencia social y técnica encargada de la planificación, organización, dirección y control de los recursos (humanos, financieros, materiales, tecnológicos, del conocimiento, etc.) de una organización, con el fin de obtener el máximo beneficio posible; este beneficio puede ser económico o social, dependiendo de los fines perseguidos por la organización. (Chiavenato, 2004).

Entonces, de acuerdo a nuestro contexto: El término *administración de redes* es definido como; la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos. (Ontiveros, 2004)

Esto nos lleva a reconocer que una red debe contar con un sistema de administración aun cuando se crea que es pequeña, aunque es cierto que entre mayor sea su tamaño más énfasis se debe poner en esta tarea.

Existen tres dimensiones de la administración de redes, los cuales son:

- Dimensión Funcional. Se refiere a la asignación de tareas de administración por medio de áreas funcionales.
- Dimensión Temporal. Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.
- Dimensión del escenario. Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

Ontiveros en su libro Metodologías de Administración describe un modelo sobre arquitecturas de administración de redes que indica que tanto el modelo TMN de la ITU[4] como el modelo OSI-MN (Nedwork Management) son modelos funcionales que dividen la administración de una red en áreas funcionales (configuración, fallas, desempeño, contabilidad, y seguridad), definiendo de esta forma una estructura organizacional, con funciones bien definidas. De esto deriva el nombre de modelos funcionales

En tal sentido se describe a continuación el modelo funcional con la creación de las siguientes áreas funcionales:

2.3.3.1. Administración de la configuración

Describe actividades ubicadas dentro del proceso de la administración de la configuración los cuales serán:

a) Planeación y diseño de la red.

Su objetivo de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación, contempla varias etapas:

[4] Unión Internacional de Telecomunicaciones

- Reunir las necesidades de la red. Las cuales pueden ser:

  Específicas o generales.

  - Multicast,
  - Calidad de servicio (QoS), etc.

  Cuantitativas:

  - Cantidad de nodos en un edificio
  - Cantidad de switches necesarios para cubrir la demanda de nodos.

Las siguientes etapas solo se adecuaran cuando involucre un rediseño completo de la red o en el caso de alguna necesidad más general que pueda requerir de un cambio total en la red, la cual no viene al caso del presente proyecto de grado.

- Diseñar la topología de la red
- Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
- Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.

b) Selección de la infraestructura de red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta.

Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo. Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red.

c) Instalaciones y Administración del software.

Su objetivo es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red, comprende:

- Instalaciones de hardware.

Contempla, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc.

El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
- Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.
- Documentar el cambio para futuras referencias.

- Administración del software.

Esta actividad es responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos. Menciona las siguientes recomendaciones:

- Antes de realizar una instalación, se debe tomar en cuenta, que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.
- Obtener el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requieren especial cuidado. Estos

respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor de TFTP[5].

d) Provisión

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

e) Políticas y procedimientos relacionados.

Esta actividad recomienda realizar, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.
- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

2.3.3.2. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

[5] (Protocolo de transferencia de archivos trivial)

El proceso de la administración de fallas consiste de distintas fases:

- Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado.
- Localización de fallas. Determinar el origen de una falla.
- Pruebas de diagnóstico. Diseñar y realizar pruebas que apoyen la localización de una falla.
- Corrección de fallas. Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- Administración de reportes. Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

2.3.3.3. Administración de desempeño

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado para optimizar el desempeño de la red.

La optimización de una red es el proceso de medidas para definir las características de la carga de tráfico y hacer modificaciones al esquema de la red, el diseño, y la configuración para mejorar su desempeño. Un proyecto de optimización involucra usar un analizador de protocolos para evaluar la operación de la red por completo, incluye todos los componentes de software y hardware. (Cardenas, 2003).

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

a) Monitoreo.- El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

- Utilización de enlaces. Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.
- Caracterización de tráfico. Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.
- Porcentaje de transmisión y recepción de información. Es encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.
- Utilización de procesamiento. Tarea que permite conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

b) Análisis.- Posterior a la recolección de información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

El proceso de análisis puede detectar comportamientos relacionados a lo siguiente:

- Utilización elevada. Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

- Tráfico inusual. El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

- Elementos principales de la red. Permite conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

- Calidad de servicio. Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

- Control de tráfico. El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

La administración del desempeño se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces.

Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

2.3.3.4. Administración de reportes.

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este

es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

a) Creación de reportes.- Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios.

Cuando se crea un reporte debe contener al menos la siguiente información:

- El nombre de la persona que reportó el problema.
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema
- Comentarios acerca de la problemática.
- Fecha y hora del reporte.

b) Seguimiento a reportes.- La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc., y ésta debe poder ser consultada en cualquier momento por el administrador.

c) Manejo de reportes.- El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte.

d) Finalización de reportes.- Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

2.3.3.5. Administración de contabilidad

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

2.3.3.6. Administración de la seguridad.

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad y el planteamiento de políticas de seguridad.

A continuación se definen las estrategias que ofrece la administración de seguridad, pero en este caso se dará mayor énfasis a los servicios de seguridad y mecanismos de control:

a) Prevención de ataques.- El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

b) Detección de intrusos.- El objetivo es detectar el momento en que un ataque se está llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. Este objetivo se puede lograr mediante un

sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

c) Respuesta a incidentes.- El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

d) Políticas de Seguridad.- La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

   Entre otras, algunas políticas necesarias son:
   - Políticas de uso aceptable
   - Políticas de cuentas de usuario
   - Políticas de configuración de ruteadores
   - Políticas de acceso remoto.
   - Políticas de contraseñas.
   - Políticas de respaldos.
   - Políticas de acceso a la red.

   Este último se detalla más adelante debido a que es un aspecto fundamental del presente proyecto de grado.

e) Servicios de seguridad.- Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad. Identifica el “que”. De acuerdo a la Arquitectura de Seguridad OSI, un servicio de seguridad es una característica que debe tener un sistema para satisfacer una

política de seguridad. La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- No repudio
- Control de acceso

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de seguridad de una organización, en este caso se define a la Autenticación y al Control de Acceso como servicios de seguridad relacionados al presente proyecto, mismos que se detallan en el apartado de seguridad en redes de ordenadores.

f) Mecanismos de seguridad.- Define las herramientas necesarias para implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: Control de acceso, cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras, para el presente proyecto se implementara el Mecanismo de Seguridad Servidor RADIUS o FreeRADIUS.
Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

g) Proceso.- Esta estrategia de la administración de seguridad **p**ara lograr el objetivo perseguido debe, al menos, realizar las siguientes acciones:
- Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.

- Definir, de acuerdo a las políticas de seguridad, los servicios necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.
- Implementar las políticas de seguridad mediante los mecanismos adecuados.

2.3.4. Seguridad en Redes de datos.

La definición de seguridad tiene muchas interpretaciones, por tanto se recurre a algunas definiciones realizadas por Claudia E. Bello en su Manual de Seguridad en Redes.

Seguridad: es "calidad de seguro", y, seguro está definido como "libre de riesgo".
Información: es "acción y efecto de informar".
Informar: es "dar noticia de una cosa".
Redes: es "el conjunto sistemático de caños o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin".

Uniendo estas definiciones:

Seguridad en Redes: es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin. (Bello, 2000).

Entonces: Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en la aplicación de servicios, mecanismos y políticas de acceso que permitan el control.

Para que un sistema se pueda definir como seguro, debe tener estas cuatro características: (Fundacion Codigo Libre Dominicana, 2004)

- Integridad: La información sólo puede ser modificada por quien está autorizado.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Autenticidad: Que no se pueda negar la autoría.

Dependiendo de las fuentes de amenaza y los ataques, la seguridad puede dividirse en seguridad física y seguridad lógica

La seguridad lógica, será a la que se dará mayor énfasis en el desarrollo del presente proyecto.

2.3.4.1. Seguridad física.

La Seguridad Física consiste en la ″aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial″. (Seguridad Corporativa, 2009).

a) Objetivos de la seguridad física.
   - Garantizar la integridad y la recuperación de los datos
   - Sistemas de alimentación ininterrumpida

   En tal sentido la seguridad física hace referencia a la protección frente a las amenazas físicas de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación. Fundamentalmente los factores que protegen serán:
   - Humanos: Corresponde a todos los administradores, usuarios y personal en general que pertenecen a una organización.
   - Tecnológicos: Recursos tecnológicos necesarios para el funcionamiento de los servicios. Ej.: Hardware, software, servidores, Internet, equipos de red y datos, etc.
   - Estructurales: Ej.: Edificios, data centers, oficinas, bodegas, etc.

Sobre estos factores siempre existirán sucesos que amenacen la seguridad (integridad, confidencialidad, disponibilidad) de los mismos, estos sucesos se conocen como amenazas.

2.3.4.2. Seguridad lógica

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. (Universidad Catolica del Peru, 2010)

Toda red de ordenadores puede verse afectado por la falta de seguridad física donde la mayoría de los daños que puede sufrir un sitio de cómputo, no será sobre los medios físicos, sino, contra información por él almacenada y procesada.

Así, la seguridad física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica. (Seguridad Corporativa, 2009).

Los objetivos que se plantean para la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.

A continuación se detallaran aspectos relacionados a la seguridad lógica que están estrechamente interconectados con la administración de redes.

a) Control de acceso a la red.

   Un control de acceso a la red, NAC(Network Access Control), se refiere a la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular. Los mecanismos para el control de acceso pueden ser usados para cuidad recursos físicos, recursos lógicos o recursos digitales. El objetivo del control de acceso es realizar lo que su nombre implica, es decir controlar el acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad

en el usuario final y controles post-admisión sobre los recursos y dispositivos a los que pueden acceder los usuarios y verificar que pueden hacer en la red.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema, estos son: (Borghello, 2001)

b) Tipos de control de acceso a la Red.

Existen diferentes tipos de control de acceso a una red los cuales se explican a continuación:

- Basado en hardware. Tanto si es "in-line" o "out-of-band", esta opción necesita habitualmente de un equipo (appliance) que tendrá que estar instalado en casi cualquier ubicación donde sea preciso contar con un NAC. Algunos de estas aplicaciones han sustituido a los switches de acceso, mientras que otros operan entre la capa de acceso a red y los switches de red.

- Basado en agentes software. El siguiente paso es el basado en pequeños programas residentes en los ordenadores y dispositivos, instalándose estos agentes en cada uno de los sistemas que deban ser controlados por el NAC. Dichos agentes escanean y monitorizan el dispositivo, generalmente enviando los resultados a un servidor central.

Los sistemas que no cumplen con los requisitos no tendrán autorización de acceso a la red, y a menudo se les envía algún tipo de medida correctora para que cumplan las directivas de seguridad.

c) Operación de un Control de Acceso a la Red.

Descripción de la operación de un NAC:

- Detección e Identificación de nuevos dispositivos conectados a la red.
  Esto se lleva a cabo por la identificación de peticiones de autenticación, a través de los switches.
- Autenticación de usuarios y dispositivos. La Autenticación es un procedimiento que consiste en comprobar la identidad de una entidad (persona ó equipo), con vistas a la autorización del acceso de dicha entidad a ciertos recursos (sistemas, redes ó aplicaciones). La autenticación se realiza utilizando el estándar 802.1x y un servidor RADIUS, mismos que se describen más adelante.
- Evaluación o revisión de sistemas finales en cuanto a su cumplimiento y/o vulnerabilidades, se hace una revisión de las condiciones en las que se encuentra el equipo, que busca conectarse a la red en cuanto a su cumplimento con políticas previamente establecidas como son sistema operativo, programas y aplicaciones instalados, actualizaciones de antivirus así como nivel de parcheo. Esto se realiza con el objetivo de que si un equipo de usuario deja de cumplir con las políticas establecidas, éste será redireccionado a la zona de remediación.

- Autorización para usar la red basado en los resultados de la autenticación y evaluación. Como ya se mencionó esta fase depende de los resultados obtenidos previamente, entonces se determina el roll o función que desempeña la estación o equipo final de usuario, y de acuerdo con esto se autoriza el uso de recursos de red.
- Remediación para equipos con problemas de cumplimiento de políticas de seguridad. Aquí se resuelven problemas de cuarentena de sistema finales, y/o usuarios para evitar impacto negativamente en la red.

d) Elementos de un Control de Acceso a la Red.

Los elementos que integran un control NAC son:

- Equipo cliente. En una red, los equipos clientes son empleados por los usuarios de una red tales como PC's, impresoras, servidores, entre otros.
- Autenticador. Entidad en un extremo de un segmento punto a punto de una LAN que facilita la autenticación de la entidad conectada al otro extremo del enlace. Nac Gateway. Es un dispositivo que se encuentra entre el servidor de autenticación y el equipo de usuario final. Este dispositivo permite controlar las acciones de autenticación y autorización mediante la manipulación de los atributos que entrega el servidor de autenticación, a fin de indicar al autenticador la acción a seguir.
- Servidor de autenticación. Entidad que facilita servicio de autenticación al autenticador.

2.3.5. Arquitectura AAA.

El desarrollo tecnológico ha traído como consecuencia la vulnerabilidad a amenazas informáticas que pueden comprometer la operación de una organización, por ello se están adoptando mecanismos que permiten una gestión eficiente de todos los requerimientos de seguridad, asignando roles y privilegios para el acceso a todos los sistemas que consuman los servicios proporcionados, permitiendo una gestión eficiente a fin de mantener la disponibilidad y confidencialidad de la información. (The FreeRADIUS Project, 2013)

La Autenticación + Autorización + Arqueo, AAA (Autentication + Authorization + Accounting) es un estándar para el diseño basado en la autenticación, es una colección y definición de normas para la creación de sistemas. (The FreeRADIUS Project, 2013)

La arquitectura AAA permite la existencia de servidores Proxy para descentralizar peticiones hacia otros servidores, con lo que una petición de autenticación o arqueo podrá ser transferida a otro servidor secundario por el servidor principal, este proceso es independiente para cada una de las tres "aes", por lo que se pueden construir redes complejas que gestionen independientemente la autenticación hacia un servidor, la autorización hacia otro u otros y el arqueo hacia otros. Todo esto proporciona las

características de redundancia, descentralización y balanceo de carga. Esta arquitectura permite la respuesta a las siguientes preguntas.

Autenticación ¿Quién es el solicitante?

Autorización ¿A qué servicios le voy a permitir acceder?

Arqueo ¿Qué hace el cliente con los servicios que presto?

2.3.5.1. Componentes en la arquitectura AAA

La arquitectura de la triple AAA tiene los siguientes componentes:

a) Solicitante. Equipo o usuario que solicita autenticación o entrada.

b) NAS. Es el equipo de red que hace de puerta de entrada física y tramita la autenticación. Este equipo suele ser quien inicia la secuencia de autenticación al detectar una conexión activa, por ello se denomina autenticador.

c) Servidor de autenticación**.** Es el que dirige todo el proceso AAA de los equipos y usuarios que soliciten acceso, puede hacer el papel de Proxy elevando las consultas a otros servidores.

d) Servidor de directorio o servidor de base de datos de usuarios y credenciales. Al cual el servidor de autenticación va a solicitar los datos de autenticación de los solicitantes de acceso. Este puede ser la misma máquina que el servidor de autenticación, un servidor de Directorio Activo, AD (Active Directory), una base de datos SQL (MySQL, Microsoft SQL Server, Oracle,Ldap, etc.), o un servidor UNIX con credenciales de usuario.

e) Proveedor de servicios, SP (Service Provider). Es el propietario de la infraestructura de acceso a la que se conecta el usuario y por lo tanto es el propietario del servidor AAA y del equipo de servicio o NAS.

2.3.5.2. Autenticación.

La autenticación es el proceso de verificación de la identidad de un remitente que hace una petición para conectarse a un sistema. El remitente puede ser una persona que usa un ordenador u otro medio electrónico, un ordenador por sí mismo o programa. La autenticación es un modo de asegurar que los usuarios son realmente quienes dicen ser

y que tienen la autorización para realizar funciones en el sistema. Debe dar una respuesta inequívoca a la pregunta ¿Quién o qué entidad pretende acceder a los servicios que presto?

Los primeros sistemas utilizaban una estructura simple de nombre de usuario y contraseña en texto plano, basando todo este sistema en estos dos datos, que podrían ser interceptados o robados por otra persona. Con el tiempo, este sistema fue mejorando mediante el acceso a través de desafío (Challenge), mediante dicho proceso no hay intercambio de contraseñas durante el transporte de la autenticación, sino mediante la encriptación de mensajes de una misma clave y un mismo algoritmo, evitando el transporte de la contraseña en sí.

Posteriormente se implantan otros métodos, como el acceso a través de equipos telefónicos con identificador (número de teléfono o número de serie), el generador de contraseñas portátil (token), tarjetas de acceso, sistemas biométricos, etc.; hasta llegar en la actualidad a un sistema más seguro basado en certificados llamado Infraestructura de Clave Pública, PKI (Public Key Infraestructure), que es una tecnología o conjunto de protocolos y estándares, que utilizan para su puesta en funcionamiento un conjunto de hardware y software, además de una serie de procedimientos de implementación de seguridad y normativas.

Durante este proceso no es el solicitante quien habla lenguaje AAA con el servidor de Autenticación, sino que el solicitante habla con el NAS o autenticador, y es éste quien traduce o encamina los paquetes hacia el servidor de autenticación. De esta manera no existe un camino abierto entre el solicitante y el servidor de autenticación, con lo que se garantiza bastante la seguridad del servidor de autenticación contra ataques directos, ya que un atacante tendría que estar en el interior de su infraestructura. AAA es versátil, ya que no provee de un único método de autenticación, sino que es considerado un protocolo extensible porque permite cualquier tipo de autenticación que se integre o adapte a su formato. En la fase de autenticación se produce un

mensaje inicial de solicitud de acceso desde el equipo NAS al servidor de autenticación en forma de:

Solicitud de Acceso (Access - Request). El solicitante envía el nombre de usuario y la contraseña cifrada, si procede hacía en NAS. Este envía entonces al servidor de autenticación el mensaje de Access-Request solicitando además el puesto de acceso para el solicitante.

2.3.5.3. Autorización.

La autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que éste ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido. Este proceso contesta a la pregunta: ¿A qué servicios se va a permitir acceder al solicitante, una vez autenticado? En este paso se produce la consulta del servidor de autenticación a la base de datos de usuarios, certificándose en la información del usuario que solicita acceso.

En los registros relacionados con este usuario, se podrá consultar todo tipo de derechos y deberes relacionados con él, de esta manera el servidor conocerá detalles como: si el solicitante está autorizado a acceder a la red en este momento, si le debe asignar la dirección IP concreta, si habrá de configurarle parámetros específicos para su conexión, si deberá concederle un ancho de banda determinado, si debe solicitar otro tipo de credenciales, o simplemente si deberá denegar su acceso. Todas estas reglas son definidas para cada usuario en concreto, para un grupo de usuarios o para todos los usuarios.

En esa fase el servidor de autenticación, tras conocer todos los atributos necesarios para el solicitante, responderá a su solicitud de autenticación mediante un mensaje estándar enviado al equipo NAS para permitir, denegar o volver a preguntar sobre su acceso:

Aceptación de Acceso (Access-Accept). Cuyo fin de la solicitud de autenticación es la aceptación del acceso. Si el mecanismo de acceso ha sido correcto, se envía el mensaje al NAS con los atributos necesarios para regular el acceso del solicitante de forma personalizada.

Denegación de Acceso (Access-Reject). Debido a usuario inexistente, contraseña incorrecta, derechos reservados, se le deniega de forma incondicional el acceso a este solicitante. Se puede incluir en este mensaje el motivo de la denegación del servicio. El NAS que recibe este mensaje no permite el acceso al solicitante, enviando un mensaje (si se incluye) al solicitante.

Solicitud de información adicional para el acceso (Access-Challenge). Se le requiere al solicitante información adicional, como contraclave, tarjeta de acceso, PIN de acceso, o cualquier otro método alternativo o adicional de acceso. El NAS transmite la petición al solicitante.

Este mensaje puede ser intercambiado en múltiples ocasiones dependiendo del tipo de autenticación y de la información.

2.3.5.4. **Accounting**.

Una vez realizado el proceso de autorización se produce la fase de arqueo, proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluida la cantidad de tiempo que permanece conectado, los servicios a los que accede, así como los datos transferidos durante la sesión.

Los datos registrados durante este proceso se utilizan con fines estadísticos. Estos datos correctamente manejados y gestionados nos permiten tomar decisiones en cuanto al uso de recursos por parte de los usuarios, con el fin de denegar conexiones, cambiar anchos de banda, impedir descargas, etc.

La fase de arqueo está limitada por la capacidad del equipo NAS de registrar información de sesiones. Mediante este proceso se podrá facturar a los usuarios los servicios prestados ya sea en forma de tiempo o de flujo de datos; por ejemplo el

acceso a Internet mediante conexiones móviles (UMTS, 3G, etc.), se suele tarifar el servicio por descarga de datos, si no se tiene contratada tarifa plana.

En el área de arqueo se acumula la información de sesiones para posteriormente tarifarlas, de esa manera el Accounting es el responsable de proporcionar los datos necesarios para enlazar con un sistema de tarificación adecuado.

Durante esta fase se producen los siguientes mensajes:

- Solicitud de inicio de arqueo (Accounting - Request [Start]). Solicitud de inicio enviada desde el equipo NAS al servidor, que indica que ha comenzado la fase de arqueo y se comenzarán a registrar los datos de la sesión de usuario.
- Respuesta de asentimiento al inicio de arqueo (Accounting – Response [Start]). Responde a la solicitud inicial. Registrando la información de inicio y enviando este paquete NAS para mostrar su conformidad.
- Solicitud final de arqueo (Accounting - Request [Start]. El NAS comprueba la desconexión del usuario y envía al servidor un mensaje final de la fase de arqueo.

2.3.6. RADIUS.

RADIUS (Remote Authentication Dial-In User Server) es un protocolo que nos permite gestionar la "autenticación, autorización y registro" de usuarios remotos sobre un determinado recurso, a continuación se desarrollara el protocolo relacionándolo al modelo AAA:

2.3.6.1. Autenticación en Radius.

Hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario permite acceder a determinados recursos.

Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

a) Autenticación de sistema (system authentication), típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/passwd;

b) Los protocolos PAP (Password Authentication Protocol), y su versión segura CHAP (Challenge Handshake Authentication Protocol), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;

c) LDAP (Lightweight Directory Access Protocol), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;

d) EAP (Extensible Authentication Protocol), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto; por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

2.3.6.2 Autorización en Radius

Concede servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario.

El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

1.

Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

2.3.6.3 Registro en Radius

A menudo traducido también como contabilidad, se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

2.3.6.4 Métodos de autenticación del protocolo RADIUS.

Los métodos de autenticación son módulos de software sobre los que se basa RADIUS para llevar a cabo el proceso de autenticación de usuario.

Estos módulos son complejas cajas matemáticas encargadas de realizar el cifrado, descifrado y empaquetado de todos los procesos de autenticación.

a) Protocolo de Autenticación mediante Contraseña. PAP (Password Authentication Protocol). hasta los más actuales como algunos tipos nuevos del Protocolo de Extensión de Autenticación, EAP (Extensible Authentication Protocol), la evolución en cuanto a seguridad ha sido notable. PAP y el Protocolo de Autenticación por Desafío Mutuo, CHAP (Challenge Handshake Authentication Protocol) son los métodos nativos de autenticación incluidos en los primeros servidores RADIUS, y por lo mismo los más vulnerables. Todas las versiones de RADIUS tienen soporte nativo para estos métodos.

b) Método EAP que llega a extender la autenticación. EAP. Es un protocolo que se encarga de transportar, encapsular y ofrecer seguridad en la autenticación, y dentro de él se encuentran los métodos de autenticación a utilizar.

Los métodos de autenticación EAP pueden ser de los siguientes tipos:

- Métodos basados en claves compartidas. Estos métodos tienen el problema en su forma de distribución, transporte o almacenamiento de las credenciales, debido a que se da por hecho que cada usuario debe tener bien guardada su clave en un lugar seguro. Métodos basados en certificados. Estos métodos son los más seguros pero también los más difíciles de implantar. Aquí tenemos a los Certificados PKI, los cuales son la clave central en la infraestructura PKI, ya que con ellos se enlaza la clave pública, que es la clave que un solicitante comparte con otras entidades a fin de que puedan leer su información con los datos que permiten identificarlo. Ejemplos de estos métodos son EAP-TLS, EAP-TTLS y EAP-PEAP.

- Métodos no tunelados. En este tipo de métodos el tráfico EAP completo no es cifrado por el solicitante, autenticador y servidor de autenticación, solamente la información de contraseñas de usuario y otra información importante se cifra en el interior de los paquetes que circulan por la red.

Esto hace posible que los paquetes que se generan en el proceso de autenticación se puedan interceptar para obtener las credenciales de los usuarios. Métodos tunelados. Estos métodos utilizan un sistema criptográfico para encapsular el tráfico completo en el proceso de autenticación, autorización y arqueo, incrementando así la seguridad contra la interceptación de tráfico.

En la TABLA 2.2 se muestra una comparación de las características principales de los métodos más comunes de EAP.

TABLA 2.2 : *Comparación de los principales métodos EAP*

Fuente: *(Córdoba Téllez Anabel, 2010)*

	EAP-MD5	EAP-TLS	EAP-TTLS	EAP-PEAP
Basado en claves compartidas	Si	No	No	No

Certificado de servidor	No	Si	Si	Si
Certificado de cliente	No (Usuario y contraseña mediante Chalenge)	Obligatorio	Opcional (credenciales de usuario)	Opcional (credenciales de usuario)
Validación de certificados	No	Si	Si	Si
Autenticación mutua	No (solo cliente)	Si	Si	Si
Tunelamiento	No	Si, TLS	Si, TLS	Si, TLS
Desarrollador	Estándar	Microsoft	Funk y Certicom	Microsoft, Cisco y RSA.
Solicitantes que lo soportan	Microsoft, WPA, MacOS	Microsoft, MacOs, Linux	WPA, MacOs.	Microsoft, MacOs, Linux
Vulnerable Main in the Middle	Si	No	No	No
Vulnerable actualmente	Si	No	No	No
Usos recomendados	Redes cableadas	Alámbrica e Inalambrica, Smartcards	Alambrica e Inalambrica	Alambrica e Inalambrica

c) Autenticación simple y autenticación mutua.

La autenticación simple se basa en que el sistema solicitante (usuario) pide la autenticación al servidor de autenticación, presuponiendo que éste sea el servidor lícito al que se quiere conectar, por lo que le entrega sus credenciales para ser autenticado. En la autenticación mutua, basada en la desconfianza mutua, el

solicitante verifica primero la identidad del servidor al que enviará sus credenciales.

En los casos de autenticación mutua mediante certificados, como en los protocolos EAP tunelados mediante TLS, antes de que se produzca el intercambio de credenciales tunelado entre solicitante y servidor, ambos pasan por un proceso de verificación de identidades, normalmente mediante el uso de un certificado de cliente y otro de servidor. Los protocolos EAP-TLS, EAP-TTLS y EAP-PEAP, se basan en la autenticación mutua, ya sea utilizando certificados de cliente y de servidor o por combinación de certificados de servidor y credenciales de usuario.

d) Tipos de Autenticación.

La manera de almacenar los nombres de usuarios y contraseñas de los solicitantes, puede realizarse de diferentes maneras:

Autenticación contra archivo de usuarios. Esta es la forma más básica utilizada por los servidores de autenticación. Utiliza un fichero de texto en el cual se almacenan las credenciales de los usuarios y los parámetros asociados a estos. Se recomienda sólo para redes con un número reducido de usuarios.

Autenticación contra el sistema operativo. Aquí basta dar los privilegios suficientes para que un módulo del servidor de autenticación pueda leer los usuarios y sus contraseñas almacenadas en las formas nativas que utilizan los sistemas operativos. Por ejemplo, en el caso de Linux sería el fichero passwd o shadow. Al crear un usuario y sus credenciales, éste queda automáticamente disponible para ser usado en el proceso de autenticación.

Autenticación contra bases de datos. En este tipo de autenticación contra una base de datos, generalmente del tipo SQL, como Oracle, Microsoft SQL Server, MySQL y PostGreSQL, los datos de credenciales de usuarios, sus atributos de autorización y la información de arqueo de cuentas se almacenan en bases de datos pudiéndolo hacer de manera cifrada utilizando funciones como MD5 o SHA1, por ejemplo. La administración de los datos se realiza de manera muy sencilla,

pudiendo hacer consultas, edición y eliminación de la información. Adicionalmente se pueden realizar copias de seguridad. Para la administración de un gran número de usuarios la base de datos es la mejor solución, pudiéndose crear scripts automáticos en lenguaje SQL para ejecutar durante los procesos de Autenticación, Autorización y Arqueo.

Autenticación contra servicios de Directorio. Este tipo de autenticación es apropiado para empresas medianas a grandes que quieran autenticar a sus empleados contra sus sistemas internos de gestión de usuarios. Los servicios de directorio son Active Directory mediante Kerberos, LDAP y eDirectory, entre otros. RADIUS realiza las consultas de autenticación y autorización contra las bases de datos almacenadas en los servidores de directorio, en los cuales se gestionan de forma común las políticas de acceso y trabajo en la red corporativa.

e) Reautenticación.

La reautenticación del solicitante se lleva a cabo si se pierde la conexión y necesita volver a autenticarse en el servidor RADIUS. También se puede forzar esta re autenticación en intervalos de tiempo para incrementar la seguridad; sin embargo, se debe tener cuidado para programar este tiempo a fin de evitar saturar al servidor.

2.3.6.5 Estructura de las comunicaciones RADIUS.

A continuación se describe la estructura de un paquete RADIUS estándar y la secuencia de un proceso completo de autenticación.

a) Estructura de un mensaje RADIUS.

Todos los paquetes RADIUS tienen la misma estructura básica, la cual consiste de los campos: código, identificador, tamaño, autenticador y atributos. En la TABLA2.3 se observa esta estructura, así como el tamaño de cada campo.

***TABLA 2.3**: Estructura de un paquete RADIUS*

***Fuente:** (Cordoba Téllez Anabel, 2010)*

Octetos	1	1	2	16	Variable
	Código	**Identificador**	**Tamaño**	**Autenticador**	**Atributos**

Este paquete RADIUS viene encapsulado dentro de un paquete UDP estándar. A continuación se describe cada campo:

- Código. Este campo tiene un octeto de longitud e identifica el tipo de paquete RADIUS. La TABLA 2.4 identifica algunos valores de código y su correspondiente tipo de paquete. Por ejemplo: si el valor del código es "1", el paquete es una solicitud de acceso (RADIUS Access-Request).

TABLA 2.4: *Valores del campo de código*

Fuente: *(Córdoba Téllez Anabel, 2010)*

Código	Tipo de paquete
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting- Request
5	Accounting-Response
6	Accounting-Status
7	Password- Request
8	Password- Reject
9	Password- Reject
10	Access-Challenge

- Identificador. Su tamaño es de un octeto. Es un campo utilizado para relacionar los paquetes que conforman una conversación, por ejemplo: solicitud y respuesta. Este campo hace posible relacionar paquetes del tipo Access-Challenge (solicitud de información adicional para el acceso) con paquetes tipo Access-Request (solicitud de acceso). Por ejemplo, el campo identificador en un paquete Access-Request enviado por el autenticador, puede contener el valor

"00001101". El servidor de autenticación responderá con un paquete Access-Challenge cuyo campo identificador tendrá el mismo valor "00001101".

- Tamaño. El tamaño de este campo es de dos octetos e identifica el número de octetos que forman un paquete RADIUS.

- Autenticador. El campo autenticador es de 16 octetos. Es generado pseudoaleatoriamente, utilizado para validar la legitimidad del servidor RADIUS con el que se está conversando. Es también un sistema de comprobación de la integridad del paquete.

- Atributos. Los atributos contenidos en el paquete RADIUS son datos comunicados entre el NAS y el servidor RADIUS. Estos datos sirven para el funcionamiento de todo el proceso AAA. Existen atributos de todo tipo, como los atributos User-Name y User-Password, que se utilizan en las solicitudes de autenticación y que definen al usuario y a su contraseña. Todos los procesos que realiza RADIUS se realizan mediante atributos, existiendo atributos para la fase de Autenticación, para la de Autorización y para la de Arqueo. Algunos de estos atributos se muestran en la TABLA 2.5, y se incluye el campo código, el cual debe ir en el paquete RADIUS.

***TABLA 2.5**: Atributos RADIUS*

***Fuente:** (Córdoba Téllez Anabel, 2010)*

Código	Atributo
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
46	Acct-Sesion-Time
64	Password-Reject

b) Secuencia de autenticación de RADIUS.

La comunicación entre el solicitante, el NAS y el Servidor de autenticación tiene siete secuencias:

1. La secuencia comienza por un Access-Request, esta solicitud de acceso es un mensaje que contiene atributos como el nombre de usuario, la contraseña, el número de puerto NAS y el ID de cliente. El NAS envía esta solicitud al servidor RADIUS que tenga preestablecido en su lista de servidores, si es que tuviera más de uno. Si no recibiera respuesta en un tiempo determinado, reintentará el envío cierto número de veces.

2. El servidor RADIUS que recibe la solicitud comprueba si proviene de un equipo NAS autorizado, si no es así, la descarta de forma silenciosa. Si el cliente NAS está en su lista y el shared secret es el correcto comprueba en su base de datos el nombre de usuario y la contraseña. El shared secret o secreto compartido de RADIUS es una contraseña con formato alfanumérico de hasta 128 bytes que se define en los dos extremos de un canal RADIUS, esos extremos son el servidor RADIUS y su cliente, el cliente puede ser un equipo NAS, un servidor Web o un Proxy RADIUS. Este secreto se utiliza para encapsular las comunicaciones entre el cliente y el servidor RADIUS.

3. Si el tipo de autenticación está basada en el desafío, se envía al solicitante un mensaje de Access-Challenge con una frase aleatoria que debe calcular. Después de esto, el solicitante enviará este cálculo y el NAS a su vez, enviará nuevamente un Access-Request con los datos calculados.

4. Una vez comprobados todos estos datos de autorización y la base de datos de credenciales, se decidirá si se acepta o deniega la solicitud. Así, se enviará ya sea un mensaje de Access-Accept o uno de Access- Reject al NAS con los atributos necesarios para activar o denegar el servicio.

5. Si el mensaje anterior es un Access-Accept, el NAS abrirá el puerto con los atributos designados y enviará un mensaje de Accounting-Request [Start] al servidor RADIUS, indicándole que ha comenzado el arqueo de la sesión del usuario. El servidor RADIUS confirmará la recepción del inicio de sesión enviando al NAS un mensaje Accounting-ResponseAccounting [Start] y guardará los datos de inicio de sesión de usuario que le envíoinicio el NAS con el AccountingAccounting-Request [Start].

6. Al terminarse la sesión del usuario, por él mismo o por otra razón el NAS envía al servidor un mensaje Accounting-Request [Stop],Accounting indicándole el fin de la sesión del usuario, así como los datos de consumo del usuario.

7. Finalmente el servidor confirma la recepción de esos datos mediante un mensaje AccountingAccounting-Response [Stop], enviándolo al NAS, terminando así el proceso de autenticación.

En la siguiente figura se muestra la secuencia RADIUS.

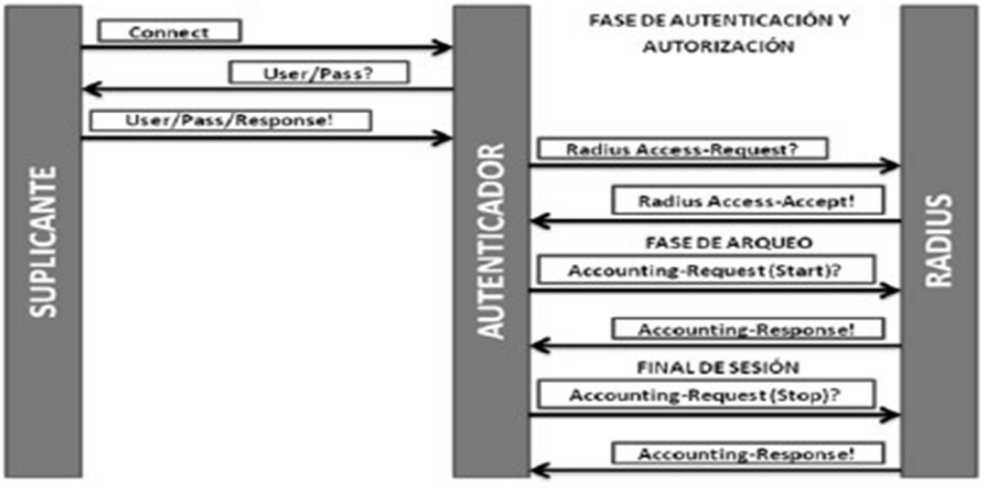


FIGURA. 2.6: *Secuencia AAA de RADIUS*
Fuente: *(Córdoba Téllez Anabel, 2010)*

2.3.7 Políticas de Seguridad.

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de las políticas de seguridad y uso adecuado de los servicios y sitios de su red LAN.

En tal sentido una organización cualesquiera que fuera puede tener muchos sitios, y cada uno contar con sus propias redes. Si la organización es grande, es muy probable que los sitios tengan diferente administración de red, con metas y objetivos diferentes. Si esos sitios no están conectado través de una red interna, cada uno de ellos puede tener sus propias políticas de seguridad de red. Sin embargo si los sitios están conectados mediante una red interna, la política de red debe abarcar a todos los sitios interconectados.

En general, un sitio es cualquier parte de una organización que posee computadoras y recursos relacionados con redes, algunos de ellos pueden ser los siguientes (Siyan, 2002):

- Estaciones de trabajo
- Computadoras hosts y servidores.
- Dispositivos de interconexión: gateways, routers, bridges, repetidores.
- Servidores de terminal
- Software para conexión de red de aplicaciones
- Cables de red
- La información de archivos y bases de datos.

De acuerdo a lo descrito anteriormente, la política de seguridad de un sitio debe tomar en cuenta la protección de esos recursos, debido a que el sitio está conectado con otras redes, la política de seguridad debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas, para ello estas deben ser planteadas.

Entonces se toma como concepto fundamental para el desarrollo de políticas de seguridad informática al "Conjunto de reglas que definen la manera en que una organización maneja, administra, protege y asigna recursos para alcanzar el nivel de seguridad definido como objetivo" (Siyan, 2002).

En tal sentido las políticas de seguridad informática sirven para:

- Definir las decisiones relativas sobre los objetivos de la seguridad de la información.
- Describir claramente de que deseamos protegernos
- Fortalecer el eslabón más débil de la cadena de seguridad de la información.

Se debe hacer también énfasis que las políticas de seguridad deben ser escritas, como lo recomienda la Universidad Nacional de Colombia, que muestra una lista de algunas de estas razones:

- Para cumplir con regulaciones legales o técnicas.
- Como guía para el comportamiento profesional y personal
- Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares.
- Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo.
- Permite encontrar las mejoras prácticas en el trabajo.
- Permiten asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto).

A fin de poder comprender el término política y los vocablos utilizados en la enunciación e implementación de políticas, se muestra una jerarquía entre las definiciones en la siguiente tabla, de acuerdo a la Guía de elaboración de políticas de Seguridad, propuesta por la Universidad Nacional de Colombia (Universidad Nacional de Colombia, 2005):

TABLA 2.6: *Cuadro de jerarquía de los términos utilizados en la enunciación e implementación de políticas.*
Fuente: *Universidad Nacional de Colombia*

POLITICA
Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir, un

número pequeño), deben ser apoyadas y aprobadas por las directivas de la organización, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

ESTANDAR.

Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas: son diseñados para promover la implementación de las políticas de alto nivel de la organización antes de crear nuevas políticas.

MEJOR PRÁCTICA.

Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizadas con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

GUIA.

Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

PROCEDIMIENTO.

Los procedimientos definen específicamente como las políticas, estándares, mejores

prácticas y guías serán implementadas en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema. Los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

2.3.7.1 Planteamiento de la política de seguridad.

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra perdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente (Karanjit Siyan, 2002):

¿Qué recursos se está tratando de proteger?
¿De quienes se necesita proteger los recursos?
¿Qué tan posibles son las amenazas?
¿Qué tan importante es el recurso?
¿Qué medidas se puede implementar para proteger sus bienes de forma económica y oportuna?

Examinar periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

A fin de canalizar las ideas conforme a los lineamientos propuestas se desarrollan hojas de trabajo para la identificación de recursos de la red y su análisis de riesgos.

2.3.7.2 Etapas en el desarrollo de una política.

La vida de una política de seguridad informática comprende once etapas y agrupadas en 4 fases.

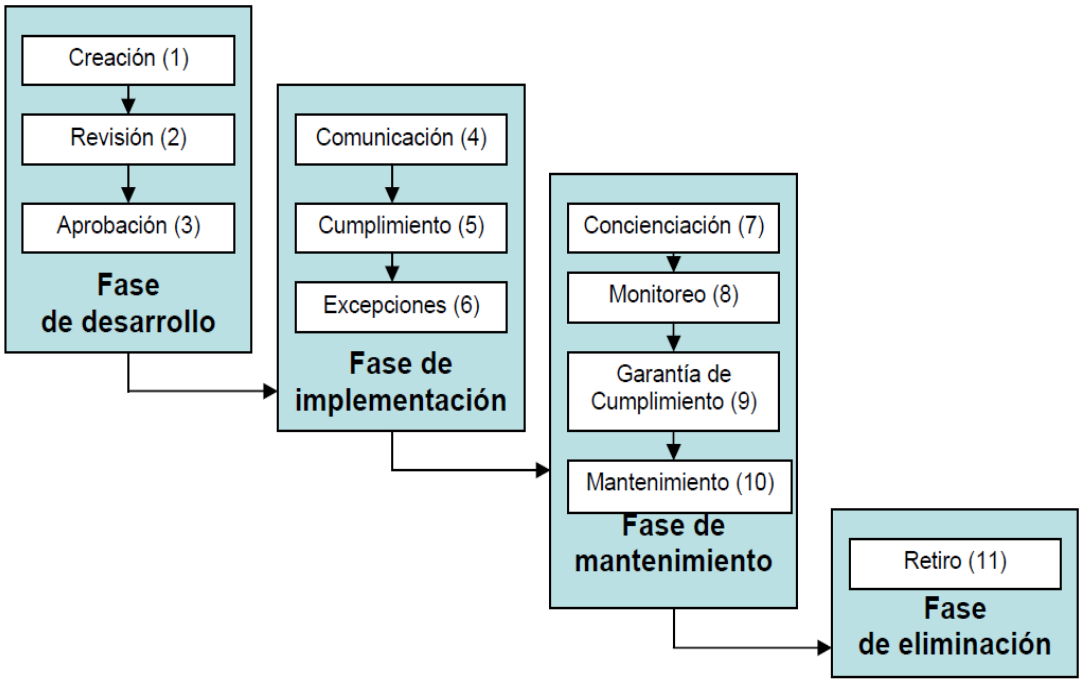


FIGURA 2.7: *Etapas en el desarrollo de una política*
Fuente: *Universidad Nacional de Colombia- 2003*

A continuación se realiza una descripción sucinta de las etapas del desarrollo de una política, enfatizando especialmente en la primera fase.

a) Fase de desarrollo: durante esta fase la política es creada, revisada y aprobada.

– Creación: Planificación, investigación, documentación y coordinación de la política.

El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política o, tomando todo junto, la creación. La creación de una política implica identificar por qué se necesita la política, determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la

factibilidad de su implementación la creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar políticas (es decir, que autoridades deben aprobarlas, con quien se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la organización para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares del Gobierno Municipal de Cobija, al igual que la coordinación con entidades internas y externas que la política afectara, para obtener información y su aceptación.

- Fase de Implementación: en esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).
- Fase de mantenimiento: los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).
- Fase de eliminación: La política se retira cuando no se requiera más.

2.4 MARCO TECNOLÓGICO.

2.4.1 Herramienta para el análisis de vulnerabilidades de red.

Las herramientas utilizadas para la ejecución de Análisis de vulnerabilidades proveen los fundamentos de seguridad para una infraestructura de red desde una base de datos de vulnerabilidades conocidas, la cual se actualiza periódicamente. Existen tres tipos de herramientas de Análisis de Vulnerabilidades:

- Escaneo de red activo. Conocido como Análisis de Vulnerabilidades de Red, estos escanean de forma remota los dispositivos conectados a la red sin requerir la instalación de agentes; una más profunda evaluación de los dispositivos puede ser realizada utilizando credenciales de administrador.
- Observación del tráfico de red pasivo. En este caso, no se escanea de forma activa a los sistemas, sino que se captura el tráfico entre dispositivos de la red para determinar su estado basado en sus patrones de tráfico. Aunque la Observación Pasiva puede

brindar información acerca de dispositivos que no pueden ser activamente escaneados (por ejemplo, equipos con Firewall Personales activados), esta técnica por sí sola no provee de suficiente información para las actividades de remediación.

- Basado en agentes. Están basados en agentes que residen en los dispositivos a analizar, coleccionando información del estado de los dispositivos en tiempo real. Estos pueden determinar aspectos de los dispositivos que no pueden ser determinados de forma remota, tal como aplicaciones y servicios que están instalados pero que no se están ejecutando.

2.4.2 Escaneo de Red y Vulnerabilidades

A continuación se presentan los escaneos a realizar utilizando como herramienta el ZENMAP.

2.4.2.1 ZenMap.

Es una interfaz gráfica para NMap. En lugar de tener que teclear comandos repletos de parámetros, ZenMap presenta una serie de pestañas con botones radiales, casillas y campos rellenables.

El resultado del escaneo se muestra en el panel inferior, mientras que la barra de estado de ZenMap contiene la sintaxis completa del comando lanzado. Un cuadrado de colores indica si el proceso está en marcha o no.

ZenMap puede verse como un asistente para construir comandos complejos, o también como una herramienta de aprendizaje. Aunque incluya el binario de NMap, es recomendable instalar NMap aparte: la versión instalada por ZenMap es anticuada

2.4.3 Herramienta para el análisis de tráfico de red.

2.4.3.1 Wireshark

Wireshark es un Capturador/Analizador de paquetes de red, comúnmente llamado sniffer, nos ofrece un nivel muy alto y detallado de que está pasando en tu red, es Open Source y multiplataforma, una excelente opción al momento de Analizar nuestra red.

2.4.4 Servidores en una Red

Un servidor dentro de una red LAN, sirve para proporcionar información a los demás ordenadores que se encuentran conectados a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información que se encuentre almacenado en él mismo.

2.4.4.1 Tipos de servidores.

Se puede categorizar los diversos tipos de servidores del mercado actual, algunos de ellos son:

- Servidor de Correo electrónico
- Servidor FTP
- Servidor de Pagina Web
- Servidor Proxy
- Servidor de autenticación
- Y otros, etc.

a) Servidor de autenticación.

- Autenticador
- Suplicante

FIGURA 2.8: *Estructura de control de acceso y autenticación*

Fuente: *Universidad Politécnica de Madrid*

b) Servidor FreeRadius.

Es un software de dominio público que identifica usuarios que acceden de forma remota a un servidor, permite el control total sobre cada llamada y la

monitorización y generación de estadísticas. (Universidad Catolica del Peru, 2010).

El servidor RADIUS utiliza el puerto 1813 UDP para establecer sus conexiones. Cuando se realiza la conexión con un ISP mediante módem, DSL, cable, módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS (FreeRadius) sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP. (The FreeRADIUS Project, 2013)

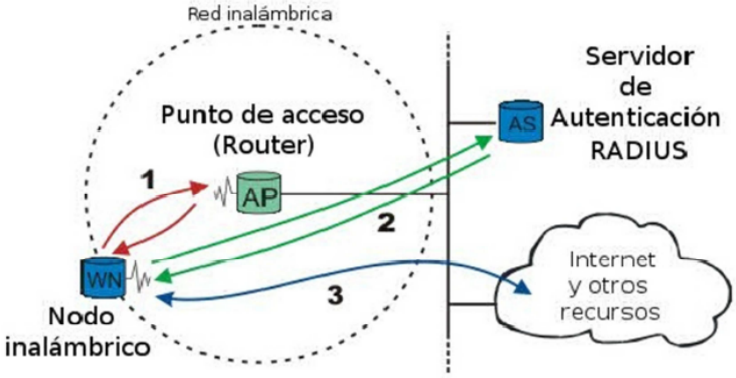


FIGURA 2.9: *Servidor Radius*
Fuente: *Raúl Espinosa Soriano*

2.4.5 Punto de acceso inalámbrico.

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos

conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming".

Por otro lado, en una red donde los dispositivos cliente se administran a sí mismos sin la necesidad de un punto de acceso, se convierten en una red ad-hoc.

Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. Los puntos de acceso (AP) son dispositivos que permiten la conexión inalámbrica de un equipo móvil de cómputo (ordenador, tableta, smartphone) con una red. Generalmente los puntos de acceso tienen como función principal permitir la conectividad con la red, delegando la tarea de ruteo y direccionamiento a servidores, ruteadores y switches. La mayoría de los AP siguen el estándar de comunicación 802.11 de la IEEE lo que permite una compatibilidad con una gran variedad de equipos inalámbricos. Algunos equipos incluyen tareas como la configuración de la función de ruteo, de direccionamiento de puertos, seguridad y administración de usuarios. Estas funciones responden ante una configuración establecida previamente. Al fortalecer la interoperabilidad entre los servidores y los puntos de acceso, se puede lograr mejoras en el servicio que ofrecen, por ejemplo, la respuesta dinámica ante cambios en la red y ajustes de la configuración de los dispositivos. Los AP son el enlace entre las redes cableadas y las inalámbricas. El uso de varios puntos de acceso permite el servicio de roaming. El surgimiento de estos dispositivos ha permitido el ahorro de nuevos cableados de red. Un AP con el estándar IEEE 802.11b tiene un radio de 100 m aproximadamente.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores situados en sus equipos (ordenador, tableta, smartphone, smart TV, radio por Internet...). Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica.

2.5 MARCO METODOLÓGICO.

Se presenta a continuación el método de diseño de la investigación denominado "BASADO EN ACCIONES", utilizado por la Escuela Militar de Ingeniería EMI (Ingenieria, 2006), que emerge de la inclusión del concepto de la planificación académica donde las acciones son los instrumentos que permiten arribar a los objetivos. Este enfoque facilita el desarrollo del Proyecto de Grado debido a que explica la relación de los principales componentes del Proyecto en comparación con el método tradicional empleado para el desarrollo del trabajo de grado que establece las siguientes etapas:

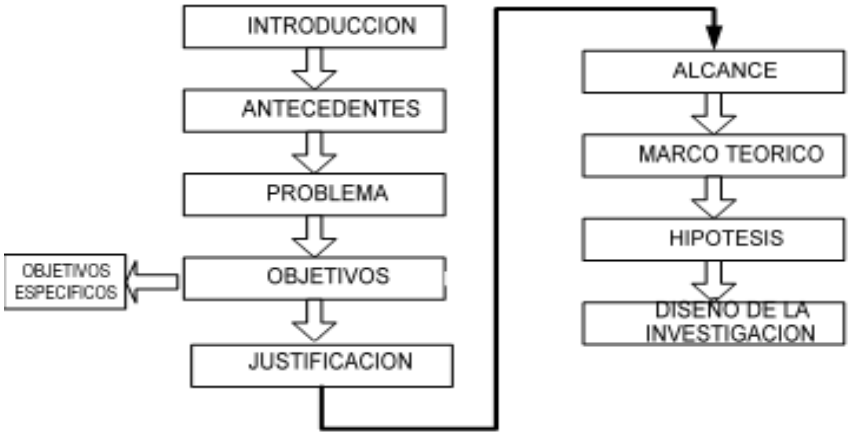


Figura Nro 1: Método tradicional de trabajos de Grado
Fuente: EMI

Entonces, de acuerdo al enfoque tradicional se observa que no se relacionan adecuadamente los elementos de los sucesivos pasos a desarrollar en el proyecto de grado en función del objetivo general. Lo que hace el método basado en acciones es explicitar la relación de los elementos del diseño con el objetivo general a través de las acciones que permiten lograr cada objetivo especifico logrando sin dificultad el contenido del marco teórico, el diseño de la investigación y

la redacción del temario tentativo en función de las acciones, este ultimo para el presente trabajo se obviara debido a que no presentaremos una hipótesis debido a que la presente es un trabajo de investigación aplicada.

La siguiente figura detalla en un esquema el Método de Diseño de Investigación Basada en Acciones:

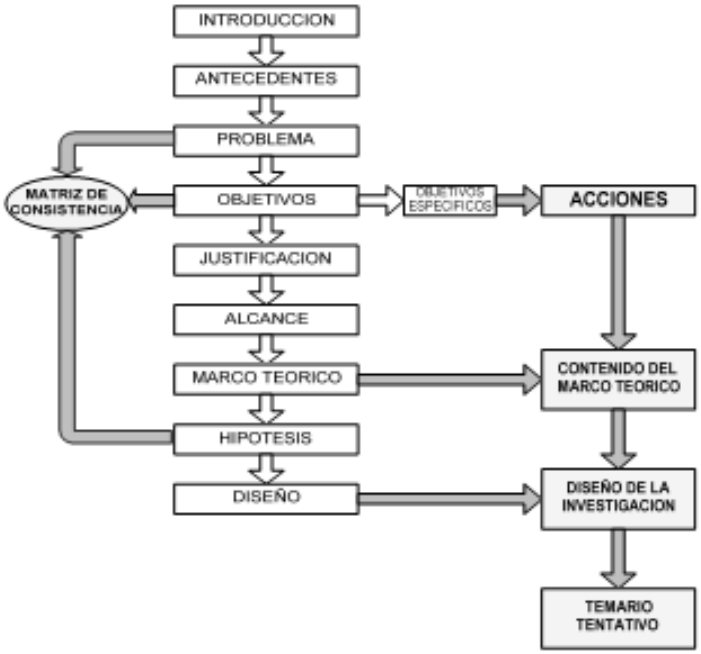


Figura Nro 3: Método de Diseño de Investigación Basado en Acciones

Fuente: EMI

Objetivos específicos y acciones.

El método propuesto comienza por definir, junto con los objetivos específicos, las actividades que deben desarrollarse para lograr cada uno de estos respetando el concepto de que los objetivos son situaciones deseadas mientras que las acciones son actividades. Se toma como ejemplo los objetivos específicos propuestos en el presente trabajo de grado y las acciones a desarrollar para el cumplimiento de los mismos:

TABLA 2.7: *Cuadro de objetivos específicos y acciones.*
Fuente: *Elaboración propia*

OBJETIVOS ESPECIFICOS	ACCIONES
Investigar los antecedentes de la red LAN, para identificar las vulnerabilidades.	• Averiguar los antecedentes de la red LAN, para identificar las vulnerabilidades. • Identificar aquellos recursos con mayor probabilidad de ataques internos y externos para salvaguardarlos contra pérdidas y daños
Analizar el desempeño de la red, a través de la "Metodología para la medición y evaluación del desempeño de redes LAN".	• Escaneo de la red con el software Wireshark • Interpretación de la información. • Elaboración de cuadros estadísticos de tráfico en la red.
Diseño del sistema de control de acceso a la red informática.	• Desarrollar el diseño lógico de la ubicación física del servidor Freeradius
Implementar el mecanismo de seguridad de control de acceso, para operabilizar los recursos de la red de datos.	• Configuración del servidor FreeRadius
Desarrollar políticas de acceso a los recursos de la red.	• Elaborar la propuesta de políticas de acceso a los recursos de la red

2.5.1 Contenido del marco teórico.

Como el proyecto surge de la necesidad de dar solución a un problema real a través de una investigación científica, entonces las acciones deben surgir del conocimiento existente (Ingenieria, 2006), entonces el método permite que el contenido del marco teórico surja al determinar la teoría necesaria para el desarrollo de cada acción en la columna Marco Teórico, mismo que se deberá llenar con la pregunta: "¿En qué asignatura o teoría se aprende a desarrollar esta acción?".

TABLA 2.8: *Cuadro de contenido del Marco Teórico.*
Fuente: *Elaboración propia*

BJETIVOS ESPECIFICOS	ACCIONES	MARCO TEORICO
Investigar los antecedentes de la red LAN, para identificar las vulnerabilidades.	• Averiguar los antecedentes de la red LAN. • Identificar aquellos recursos con mayor probabilidad de ataques internos y externos para salvaguardarlos contra pérdidas y daños	• Seguridad en redes de datos - Redes de datos - Clasificación de las redes. - Tipos de redes – Alámbricas – Inalámbricas - Seguridad en las redes de datos – Seguridad física. – Seguridad lógica - Control de acceso a la red - Administración de redes
Analizar el desempeño de la red, a través de la "Metodología para la medición y evaluación del desempeño de redes LAN".	• Escaneo de la red con el software Wireshark • Interpretación de la información. • Elaboración de cuadros estadísticos de tráfico en la red.	

Diseño del sistema de control de acceso a la red informática.	• Desarrollar el diseño lógico de la ubicación física del servidor Freeradius	- Arquitectura AAA – Autenticación – Autorización – Accounting - Seguridad en redes cableadas e inalámbricas - Introducción a radius • Políticas de seguridad.
Implementar el mecanismo de seguridad de control de acceso, para operabilizar los recursos de la red de datos.	• Configuración del servidor FreeRadius	
Desarrollar políticas de acceso a los recursos de la red.	• Elaborar la propuesta de políticas de acceso a los recursos de la red	

2.5.2 Diseño de la investigación.

Las acciones definen lo que se debe hacer en el marco practico por lo que el método propuesto sirve también para definir el diseño de la investigación que surge de seleccionar un instrumento que propone la teoría, asignatura o el fundamento teórico definido anteriormente, para desarrollar las acciones establecidas. La pregunta que colabora a identificar el instrumento es: "¿Qué técnica o instrumento me enseña esta teoría para desarrollar esta acción?"

TABLA 2.9: *Cuadro de Diseño de la Investigación.*
Fuente: *Elaboración propia*

OBJETIVOS ESPECIFICOS	ACCIONES	MARCO TEORICO	INSTRUMENTOS
Investigar los antecedentes de la red LAN, para identificar las vulnerabilidades.	• Averiguar los antecedentes de la red LAN, para identificar las vulnerabilidades. • Identificar aquellos recursos con mayor probabilidad de ataques internos y externos para salvaguardarlos contra pérdidas y daños	• Seguridad en redes de datos - Redes de datos - Clasificación de las redes. - Tipos de redes – Alámbricas – Inalámbricas - Seguridad en las redes de datos – Seguridad física. – Seguridad lógica - Control de acceso a la red - Administración de redes - Arquitectura AAA – Autenticación – Autorización – Accounting - Seguridad en redes cableadas e inalámbricas - Introducción a radius • Políticas de seguridad.	• Hoja de trabajo para desarrollar un planteamiento de seguridad. • Hoja de trabajo para el análisis de riesgo de seguridad en la red. • Hoja de trabajo para otorgar acceso a los recursos de sistema y red • Software ZENMap.
Analizar el desempeño de la red, a través de la "Metodología para la medición y evaluación del desempeño de redes LAN".	• Escaneo de la red con el software Wireshark • Interpretación de la información. • Elaboración de cuadros estadísticos de tráfico en la red.		Software: • Wireshark • Cuadros estadísticos
Diseño del sistema de control de acceso	• Desarrollar el diseño lógico de la		

a la red informática.	ubicación física del servidor Freeradius		
Implementar el mecanismo de seguridad de control de acceso, para operabilizar los recursos de la red de datos.	• Configuración del servidor FreeRadius		Protocolo RADIUS Servidor RADIUS
Desarrollar políticas de acceso a los recursos de la red.	• Elaborar la propuesta de políticas de acceso a los recursos de la red		• Guía de elaboración de políticas de seguridad para una red

Lo característico del método utilizado, es que en la práctica para toda investigación requiere de una combinación de diferentes métodos, técnicas e instrumentos, lo que se diferencia con lo que proponen, en lo que denominan diseño metodológico, donde definen un solo método para toda la investigación.

CAPÍTULO III
IMPLEMENTACIÓN

El presente capitulo, tiene la finalidad de documentar el desarrollo del proyecto en base a cada uno de las acciones sugeridas en el diseño metodológico, planteado de forma clara y específica, a fin de cumplir con el objetivo general del presente proyecto de grado. Las mismos que fueron ejecutadas en cincos acciones, que contempla la primera acción en los antecedentes de la red, segunda acción análisis de desempeño de la red, tercera acción diseño del control de acceso a la red, cuarta acción implementación del mecanismo de seguridad de control de acceso y quinta acción desarrollo de política de acceso a los recursos de la red.

3.1 INTRODUCCIÓN

El desarrollo de este capítulo, está basado en la implementación del control de acceso a la red LAN del predio central del Gobierno Autónomo Municipal de Cobija, basándose en la metodología adoptada cada objetivo específico involucra acciones es en este sentido que para cada objetivo específico se obtiene un producto.

Para el cumplimiento del objetivo específico se tiene las siguientes acciones:

3.1.1 Acción 1: Identificación de las vulnerabilidades de la red LAN del GAMC a través de la investigación de sus antecedentes, comprende las siguientes sub-acciones:

Sub-**acción 1.1.** Análisis histórico de antecedentes de los diseños de la red LAN del GAMC.

TABLA 3.1: *Cronología de los diseños de la red LAN del GAMC.*
Fuente: *Elaboración propia*

	ANALISIS
DISEÑO LÓGICO DE LA RED DE DATOS DEL GOBIERNO MUNICIPAL DE COBIJA PREDIO CENTRAL. GESTIÓN	Se verifica que la red LAN solo comprende las unidades que funcionan en el predio central del GAMC, donde la conexión del servicio de Internet a todas estas unidades se realiza a través de un modem y switch principal.

2010 ANEXO A	
DISEÑO LOGICO DE LA RED DE DATOS DEL GOBIERNO MUNICIPAL DE COBIJA PREDIO CENTRAL. GESTIÓN 2011 ANEXO B	Se verifica que la red LAN solo comprende las unidades que funcionan en el predio central del GAMC, donde se implementa un servidor proxy.

Sub-acción 1.2. Recopilación de información documental de la red de acuerdo al siguiente cuadro:

TABLA 3.2: *Cuadro de control de documentos de la Unidad de Sistemas*
Fuente: *Elaboración propia*

DOCUMENTO	OBSERVACIONES
Políticas de uso de la red de datos Gobierno Municipal de Cobija.	Desarrollado en 2010, elaborado por Ing. Daniel Torrico
Manual de funciones de la unidad de sistemas del Gobierno Municipal de Cobija	Desarrollado en 2012 en coordinación entre la Unidad de Sistemas del Gobierno Municipal de Cobija y la Unidad Organizacional.

Sub-acción 1.3. Análisis de Infraestructura física y recursos de la red.

TABLA 3.3: *Cuadro de la infraestructura física de la red*
Fuente: *Elaboración propia*

DESCRIPCIÓN	CARACTERISTICAS	CANTIDAD
Tipos de conectores	Rj11(modem),Rj45	155 +-10
Medios utilizados	cable UTP CAT5e, Señal inalámbrica	126,26
Topología en la que están ubicados los elementos de la red	En estrella extendida	-
Sistemas operativos que se están ejecutando.	Linux	4
	Windows Server 2003	1
	Windows 7	105
	Windows8	2
	Windows XP	45

Aplicaciones instaladas en los ordenadores	Office2007	76
	Antivirus Avast8	150
	Autocad Argis	26 6
	Otros.	-
Tecnología utilizada	Ethernet, Fast Ethernet, Giga Ethernet conmutada o Tokeng Ring	152
Terminales	Portatiles y Pc´s	131 (Lista de control de Usuarios Anexo C)
Servidores	Dedicados (Tramites, Seguimiento financiero)	3
Conexiones	Switch , modem y router	22 switch, 2 router y un modem.

TABLA 3.4: *Cuadro recursos de la red.*
Fuente: *Elaboración propia*

RECURSOS	OBSERVACIONES
Impresoras	12 Conectas en red
Sistemas	Sistemas de seguimiento de trámites, sistema de seguimiento financiero, registro de personal interno.
Conexión a internet	Actualmente se cuenta con el servicio de internet ADSL de 256 Kbps.

Sub-acción 1.4. Identificar los recursos con mayor probabilidad de ataques internos y externos para identificar su vulnerabilidad, a través de las siguientes sub-acciones:

Monitoreo de los equipos de la red utilizando wireshark filtrando consultas de los equipos que se conectan mediante el protocolo ARP.

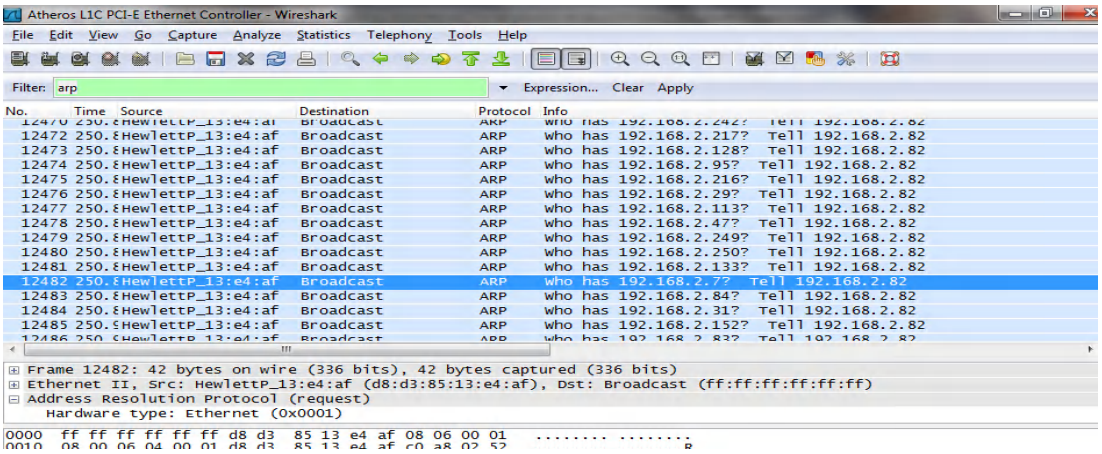


FIGURA 3.1: *Filtros de conexiones mediante ARP.*
Fuente: *Elaboración propia*

De acuerdo al monitoreo de la red se desarrolla la tabla de identificación de recursos con mayor importancia dentro de la red de acuerdo a la mayor cantidad de solicitudes por parte de los usuarios.

TABLA 3.5: *Hoja de trabajo de identificación de recursos de red*
Fuente: *Elaboración propia*

RECURSO DE RED			Tipo de equipo
Numero	**Nombre**	**Importancia de recurso**	
192.168.2.7	Sistemas de seguimiento de tramites	8	Servidor de sistemas
192.168.2.28	Servidor Sincon	5	Equipo dedicado al Sincon
192.168.2.40	Sistema interno de Registro	4	Servidor de Sistema de registro interno de catastro

Sub-acción 1.5. Estimación del riesgo de pérdida del recurso.

Escaneo con el software ZNMAP para identificar vulnerabilidades de los recursos de la red.

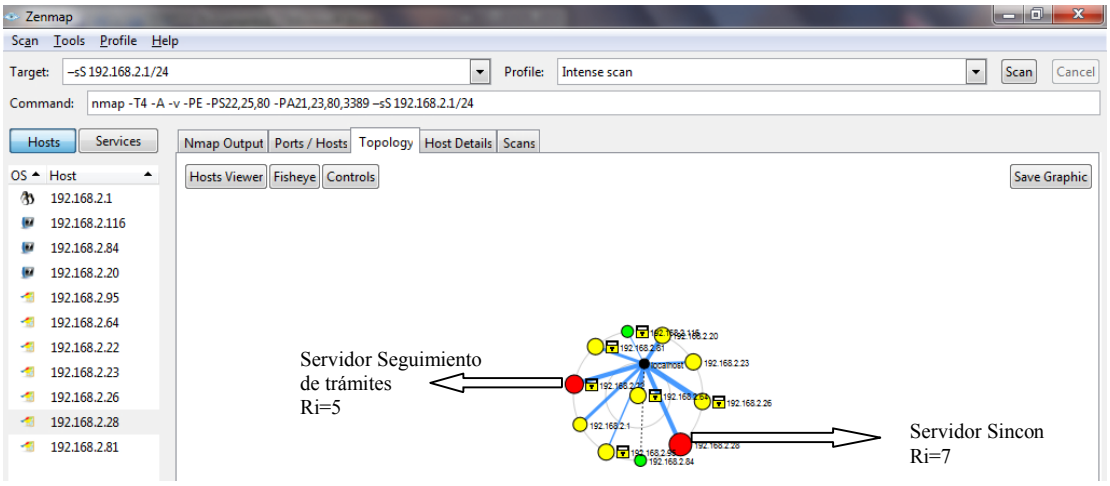


Figura 3.2: *Estimación de riesgo de pérdida del recurso*
Fuente: *Elaboración Propia.*

Descripción de los puertos de la terminal (Sincom)

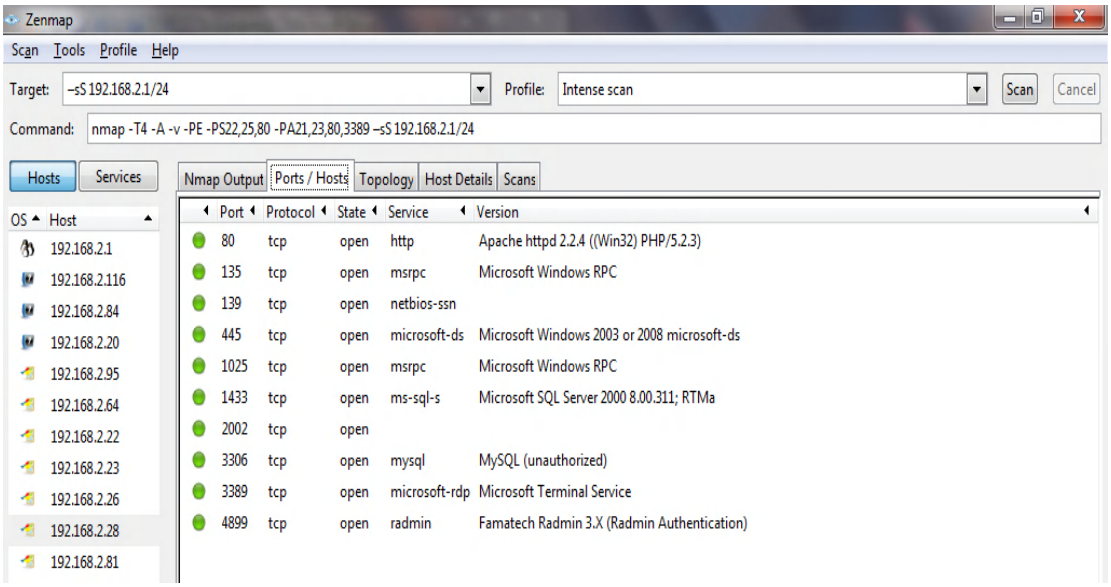


FIGURA 3.3: *Descripción de los puertos de la terminal (Sincom)*
Fuente: *Elaboración propia.*

Se aprecia que los puertos 80,135,139,445,1025,1433,2002,3306,3389,4899 se encuentran abiertos se verifica que el puerto 2002 es un troyano de acceso remoto lo que nos indica una evidencia de vulnerabilidad en este servidor.

TABLA 3.6: *Servidores del GAMC*
Fuente: *Elaboración propia*

RECURSO DE RED		Riesgo del recurso *Ri*
Numero	**Nombre**	
192.168.2.7	Sistemas de seguimiento de tramites	5
192.168.2.28	Servidor Sincon	7
192.168.2.240	Sistema interno de Registro	3

Sub-acción 1.6. Cálculo de los riesgos generales de los recursos de la red, de acuerdo a la siguiente formula.

- Estimación del riesgo de perder el recurso (*Ri*)
- Estimación de la importancia del recurso (*Wi*)

Dónde: Wri=Ri*Wi

TABLA 3.7: *Hoja de trabajo de evaluación de riesgo de los recursos de la red.*
Fuente*: Elaboración propia*

RECURSO DE RED		Riesgo del recurso *Ri*	Peso (importancia) del recurso *Wi.*	Riesgo evaluado (*Ri*Wi*)
Numero	**Nombre**			
192.168.2.7	Sistemas de seguimiento de tramites	5	8	40
192.168.2.28	Servidor Sincon	7	5	35
192.168.2.240	Sistema interno de Registro	3	4	12

De acuerdo al análisis desarrollado se establece que los recursos con mayor importancia en la red son vulnerables a ataques internos y externos.

PRODUCTO ACCION 1:

De acuerdo al análisis de las sub-acciones a través de la investigación de sus antecedentes se establece la existencia del siguiente tipo de vulnerabilidad:

TABLA 3.8: *Tipo de vulnerabilidad existente en la red LAN GAMC*
Fuente: *Elaboración propia*

TIPO DE VULNERABILIDAD EN LA RED	DESCRIPCION
RED	• Trafico de red, identificación de cada dirección ip con puertos abiertos, que provoca a ser víctima de atacante internos como externos. • Recursos compartidos en Windows sin restricciones de usuarios ni password.
HARDWARE	• Limitación institucional de tecnologías de seguridad. • Equipos de red limitados con probabilidad de que fallen y dejen el sistema inoperable.

.

3.1.2 Acción 2: Analizar el desempeño de la red, con el software wireshark de acuerdo a las fases que propone la Metodología para la medición y evaluación del desempeño de redes LAN.

Sub-acción 2.1 Acercamiento del entorno de la red, de acuerdo a la Tabla:

TABLA 3.9: *Infraestructura física de red.*
Fuente: *Elaboración propia*

DESCRIPCIÓN	CARACTERISTICAS	CANTIDAD
Tipos de conectores	Rj11(modem),Rj45	155 +-10
Medios utilizados	cable UTP CAT5e, Señal inalámbrica	126,26
Topología en la que están ubicados los elementos de la red	En estrella extendida	-
Sistemas operativos que se están ejecutando	Linux Windows Server 2003 Windows 7 windows8 Windows XP.	4 1 105 2 45
Aplicaciones instaladas en los ordenadores	Office2007 Antivirus Avast8 Autocad Argis,etc.	76 150 26 6
Tecnología utilizada	Ethernet	152
Terminales	Portatiles y Pc´s	28, 124 (Lista de control de Usuarios Anexo C)
Servidores	Dedicados (Tramites, Seguimiento	3

	financiero)	
Conexiones	Switch , modem y router	22 switch, 2 router y un modem.

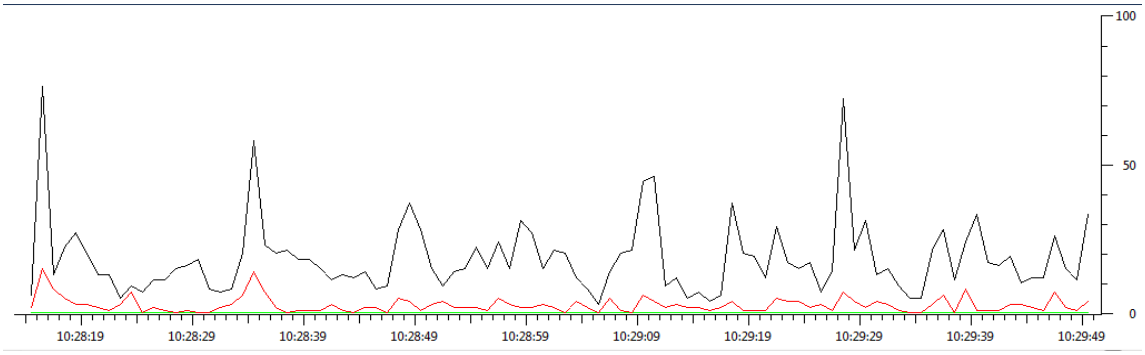
Sub-acción 2.2 Planeación de la estrategia para la realización de las pruebas, de acuerdo al siguiente detalle:

TABLA 3.10: *Planeación de estrategia para la realización de pruebas del desempeño de red.*
Fuente: *Elaboración propia*

<table>
<tr><th colspan="2">Tipo de prueba</th></tr>
<tr><td>Parámetros de evaluación</td><td>Tipos de prueba.</td></tr>
<tr><td>– Tiempo de Respuesta.</td><td>– Pruebas en el ambiente real de trabajo en ciertos periodos de la jornada laboral (entrada y salida).</td></tr>
<tr><th colspan="2">Ambiente de pruebas</th></tr>
<tr><td colspan="2">Ambiente de evaluación de acuerdo al tráfico</td></tr>
<tr><th colspan="2">Herramientas de análisis.</th></tr>
<tr><td colspan="2">Wireshark, Zenmap</td></tr>
<tr><th colspan="2">Determinación de los subsistemas a evaluar</th></tr>
<tr><td>Cuadro de Ip’s y recursos de la red que deberán ser sujetos a monitoreo</td><td>
<table>
<tr><th colspan="2">RECURSO DE RED</th></tr>
<tr><th>Numero</th><th>Nombre</th></tr>
<tr><td>192.168.2.7</td><td>Sistemas de seguimiento de tramites</td></tr>
<tr><td>192.168.2.28</td><td>Servidor Sincon</td></tr>
<tr><td>192.168.2.240</td><td>Sistema interno de Registro</td></tr>
</table>
</td></tr>
</table>

Sub-acción 2.3. Ejecución.- Generación y captura de tráfico de acuerdo al tipo de pruebas.

a) Paquetes capturados con filtro al protocolo arp y puerto 80



b) Paquetes capturados con filtro al protocolo arp y puerto 80

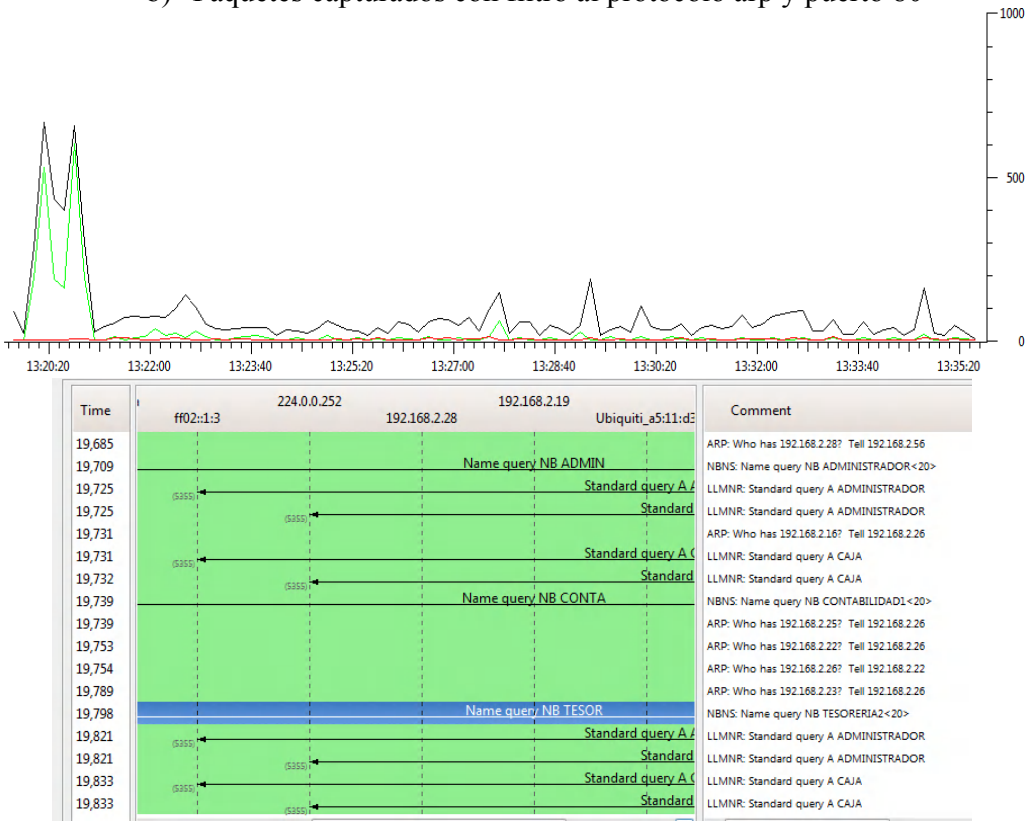


FIGURA 3.4.: *Paquetes capturados con filtro al protocolo arp y puerto 80*
Fuente: *Elaboración propia*

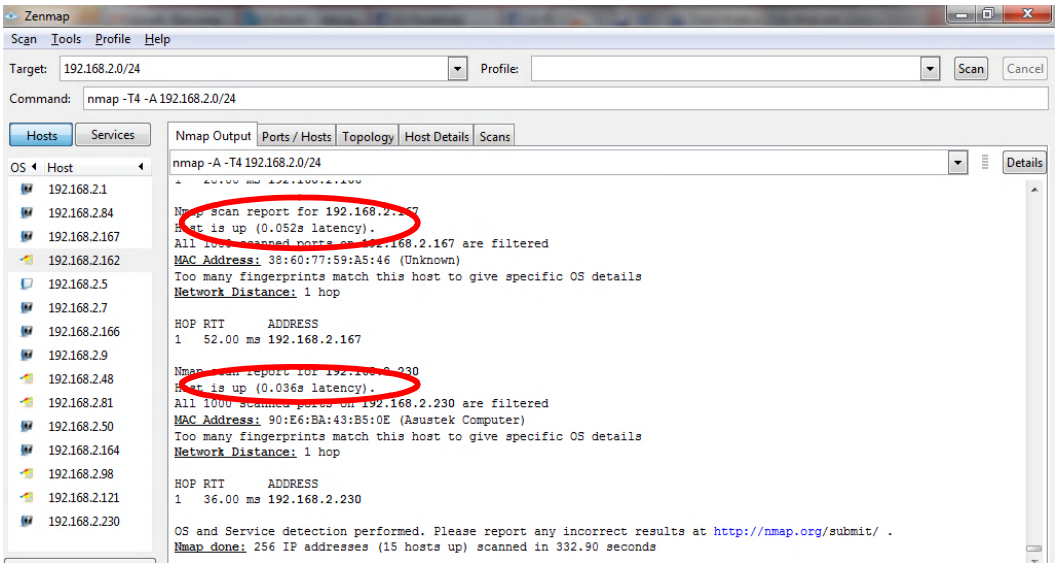


FIGURA. 3.5: *Tiempo de respuesta por terminal*
Fuente: *Elaboración propia*

Sub-acción 2.4. Análisis de los datos obtenidos de las pruebas realizadas.

TABLA 3.11*: Tiempo de respuesta para el protocolo ARP.*
Fuente: *Elaboración propia*

CANTIDAD DE TERMINALES	PROTOCOLO	TIEMPO DE RESPUESTAS	FECHA
5	ARP	1ms	31/05/2013 8:00 a.m. 18:40
8	ARP	1ms	03/06/2013 8:00 a.m. 18:40
16	ARP	2ms	04/06/2013 8:30 a.m. 18:40
30	ARP	1ms	05/06/2013 9:30 a.m. 16:40
34	ARP	1ms	06/06/2013 9:30 a.m. 16:40
32	ARP	2ms	07/06/2013 9:30 a.m. 16:40
45	ARP	2ms	10/06/2013 9:30 a.m.

			16:40

Producto Acción 2: Se verifica que en el desempeño total y parcial de la red existe gran tráfico ARP que genera problemas en la red en horario de trabajo evidenciándose que existen aplicaciones como virus, gusanos, troyanos que congestionan o bloquean la red.

3.1.3 Acción 3: Diseño del control de acceso a la red informática. De acuerdo al producto del análisis se diseñó la arquitectura de red, la cual posee control de acceso a la red y su ubicación.

Sub-acción 3.1. Diagrama de flujo de procedimiento de acceso a la red

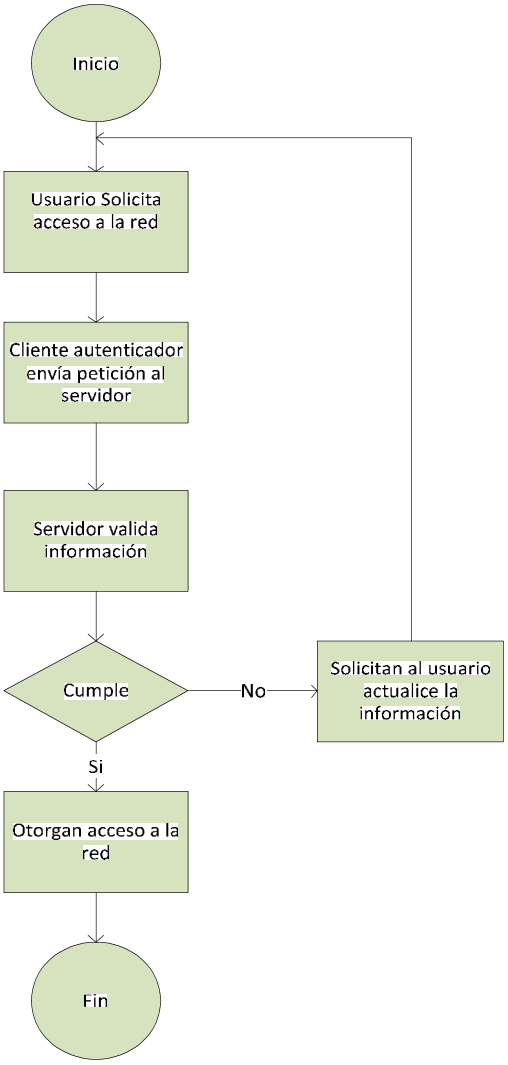


FIGURA. 3.6: Diagrama de flujo de procedimiento de acceso a la red

Fuente: Elaboración propia

Sub-acción 3.2. Diseño de la arquitectura del control de acceso a la red, de acuerdo al manual utilizado para validar los equipos de los usuarios que requieran integrarse a la red local.

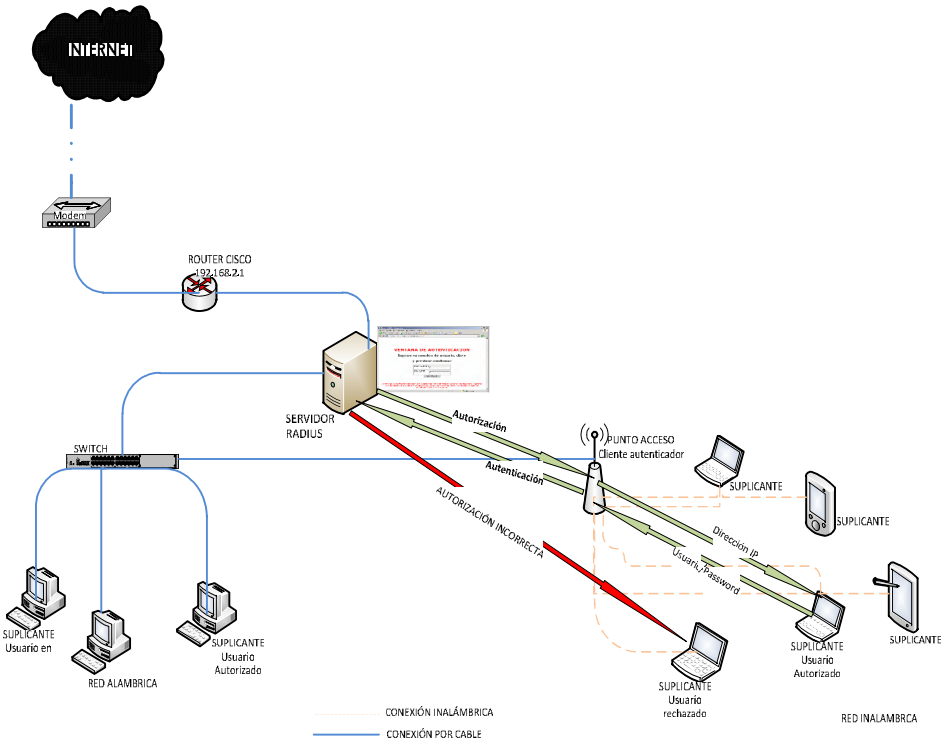


FIGURA. 3.7: Arquitectura de control de acceso.
Fuente: Elaboración propia

En la figura Muestras el Diseño de la solución que consta de cuatro fases:

Detección: El proceso de detección, se realiza por medio de la identificación de peticiones "request", de autenticación, entre el suplicante y cliente con el objeto de obtener acceso a la red.

Autenticación: El proceso de autenticación de usuarios se realiza a través del protocolo 802.1 X, el cual se validara ante el servidor Radius

Evaluación: Para la evaluación de los equipos se establece que cualquier que requiere ingresar a la red requerirá tener asignado permiso mediante su ip/mac el cual se identificara si es parte de la red GAM.

Autorización: La autorización de acceso a la red se efectúa posterior a la evaluación del equipo donde dependiendo de los resultados obtenidos se asigna el rol de privilegios al usuario.

Sub-acción 3.3. Diseño Lógico de la red predio central del Gobierno Autónomo Municipal de Cobija.

Para la interconexión de las diferentes oficinas de la institución, se cuenta con una red de datos, estructurada físicamente de acuerdo a la topología estrella en cascada con cobertura en todas las direcciones y jefaturas administrativas de la institución, la misma presenta las siguientes características, que se especifican a continuación:

- Once switch marca D-link no gestionable misma que no cuentan con la característica de la herramienta a utilizar como servidor cliente estas se encuentran distribuidos estratégicamente en las áreas del predio central del Gobierno Autónomo Municipal como ser Unidad de Bienes y Servicios, Unidad de Recursos humanos, Unidad de activos fijos, Dirección Jurídica, Dirección Financiera, Financiera, Unida de Seguimiento Financiero, Oficialía Mayor Financiera, unidad de sistemas, Despacho.
- Puntos de acceso inalámbrico Wi-Fi, con priorización a la autenticación con acceso a los usuarios de la planta alta y planta baja del predio central.
- Acceso a internet mediante conexión ADSL.
- Sesenta Equipos de computación les treces manejan la red inalámbrica.

De acuerdo a las características existentes en la red de datos del Gobierno Autónomo Municipal de Cobija, esta nos permite centralizar los puntos de acceso a los recursos que utiliza el Municipio como son el sistema Sincon, a los servidores de impresión como se demuestra en la siguiente **FIGURA 3.8.**

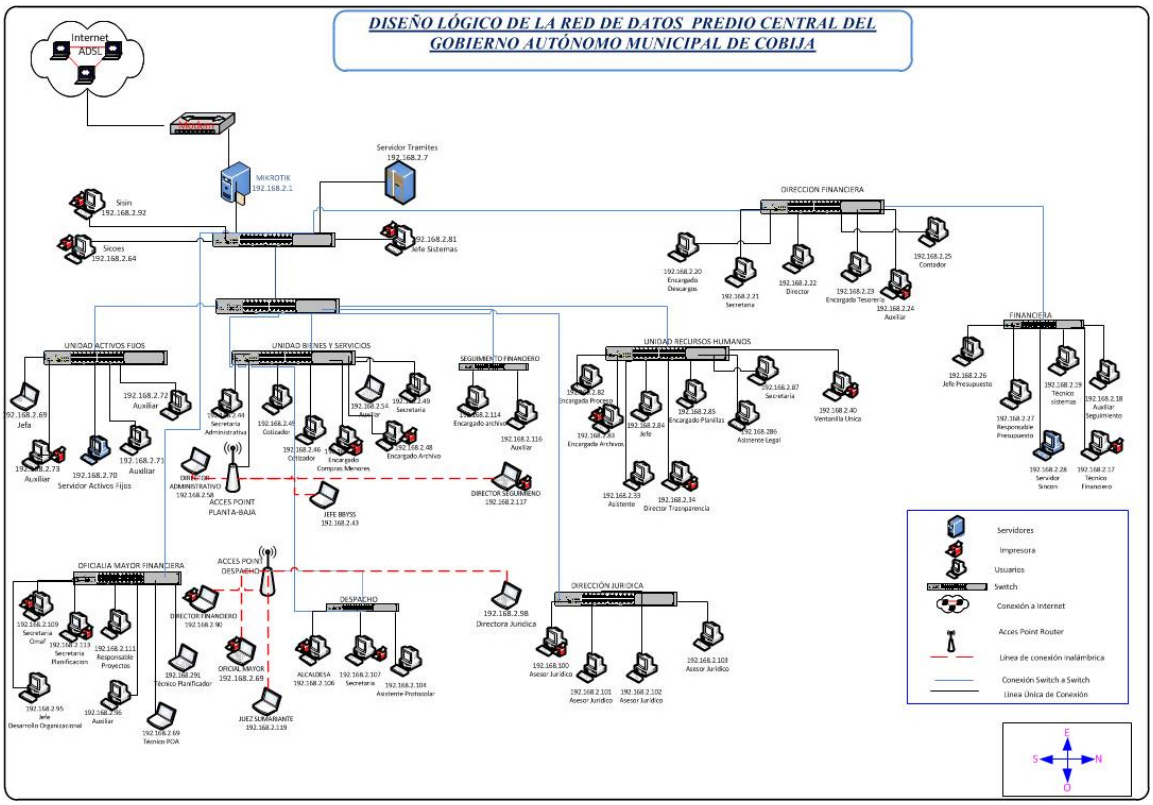


FIGURA 3.8.*Diseño lógico de Red Actual*

Fuente: *Elaboración propia*

Producto acción 3: Diseño lógico de la red de datos del gobierno municipal de cobija predio central, con la implementación de un servidor de autenticación.

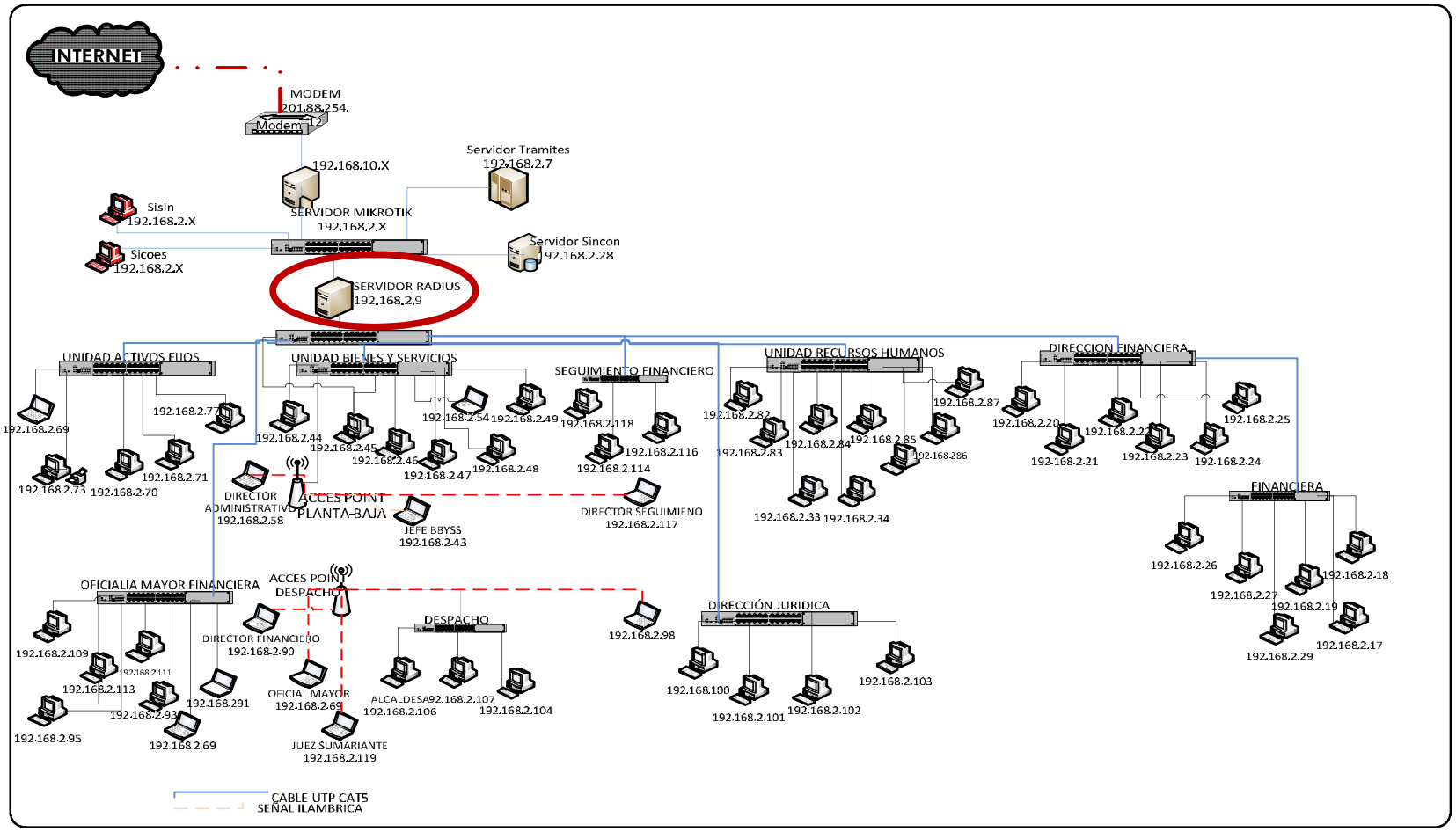


FIGURA 3.9: Diseño Lógico con la implementación del servidor radius
Fuente: Elaboración propia

3.1.4 Acción 4: Implementar el mecanismo de seguridad de Control de Acceso.

Sub-acción 4.1 **instalación de servidor Radius**

a) Determinación de Hardware/Software

Los requerimientos mínimos de hardware y software que fueron utilizados para el servidor Radius, se detalla en la siguiente tabla.

***TABLA 3.12**: Característica técnica para la instalación del servidor*
***Fuente:** Elaboración propia*

Nº	HARDWARE	SOFTWARE
1	PC Pentium 4, 512 MB de memoria, disco de 500 GB.	Distribución: Linux Ubuntu 10.0
2	AP DWL 7100AP	Freeradius 2.1.12 Base de datos LDAP(OpenLDAP) PhpLdapAdmin

La instalación del servidor radius se desarrolla de acuerdo a los siguientes pasos:

***TABLA 3.13**: Datos Técnicos de instalación de Freeradius*
***Fuente:** Elaboración propia*

Nº	Herramientas para la compilación	Instalación de Freeradius
1	#apt-get install libssl-dev	./configure –without-rlm_smb –without-rlm_perl –without-rlm_ldap –without-rlm_krb5
2	#apt-get install build-essential	#make #make install

Sub-acción 4.2 **Configuración del servidor Radius**

Para la configuración del servidor RADIUS, Freeradius cuenta con diversos archivos, estos archivos serán modificados mediante un editor de texto nano y los

archivos son los siguientes: | radiusd.conf | users | clients.conf | eap.conf , mediante la directiva "$INCLUDE", que se encuentran en /usr/local/etc/raddb/

TABLA 3.14: *Datos técnicos de la configuración del Freeradius*
Fuente: *Elaboración Propia*

Nº	Archivos	Configuración	Observación
1	radiusd.conf	"with_ntdomain_hack = yes"	Es el principal archivo a configurar la en él se encuentra las directivas más importantes a configurar para hacer funcionar correctamente el servidor RADIUS.
2	users	"usuario" Cleartext-Password := "usuario1"	En este fichero daremos de alta los nombres de usuario y contraseña que podrán ser usados para autenticarse frente al servidor Radius. Donde usuario es el usuario a autenticar y usuarios1 elsy corresponde a la contraseña
3	eap.conf	default_eap_type=peap	Este archivo se utiliza para configurar los procesos de autenticación basados en los métodos EAP.

4	clients.conf	client 192.168.2.X {
		secret = secreto
		shortname = pa
		}
			En este archivo se configuran todos los clientes que se desee que interactúen con el servidor RADIUS. Se configura el punto de acceso para esto se escribe la IP del Access Point y el secreto.

Sub-acción 4.3 Configuración del Cliente- Punto de acceso para autenticar con radius.

La configuración del punto de acceso se hace mediante interfaz de Web. Además, que el punto de acceso esté en la misma red que el servidor RADIUS, conectados ambos directamente por un cable de red.

TABLA 3.15: *Datos técnicos de la configuración del Cliente Punto de acceso*
Fuente: *Elaboración Propia*

Nº	Actividad	Configuración	Observación
1	Configuración un punto de acceso- AP DWL 7100AP	accedemos a su dirección IP (192.168.2.XV)	Una vez en su panel de configuración, accedemos a la sección de configuración
		Wireless/Wireless Security Modo Seguridad RADIUS	

A continuación accederemos a la pantalla de configuración del punto de acceso, usando un cliente de Web. La configuración completa lo vemos en (Anexo D).

FIGURA 3.10: *Ventana la configuración del Cliente Punto de acceso*
Fuente: *Elaboración Propia*

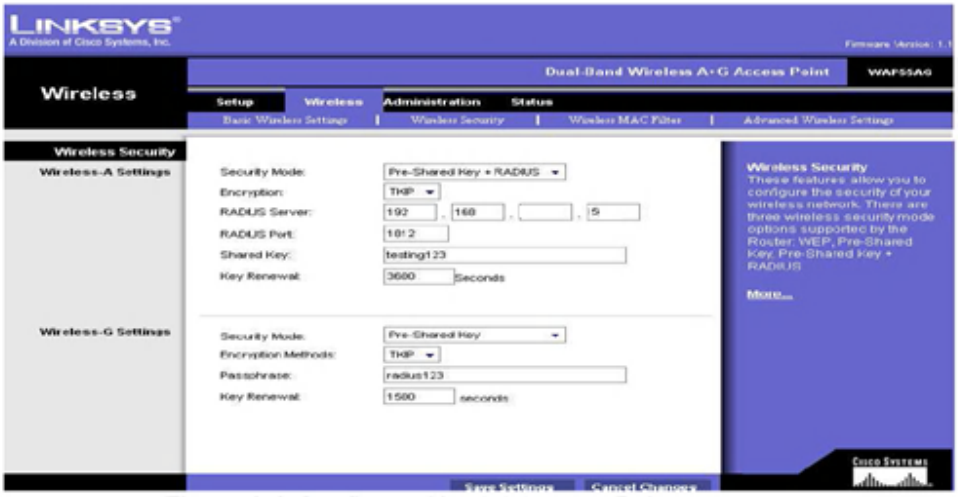


FIGURA 3.11: *Configuración del Punto de acceso*
Fuente: *Elaboración Propia*

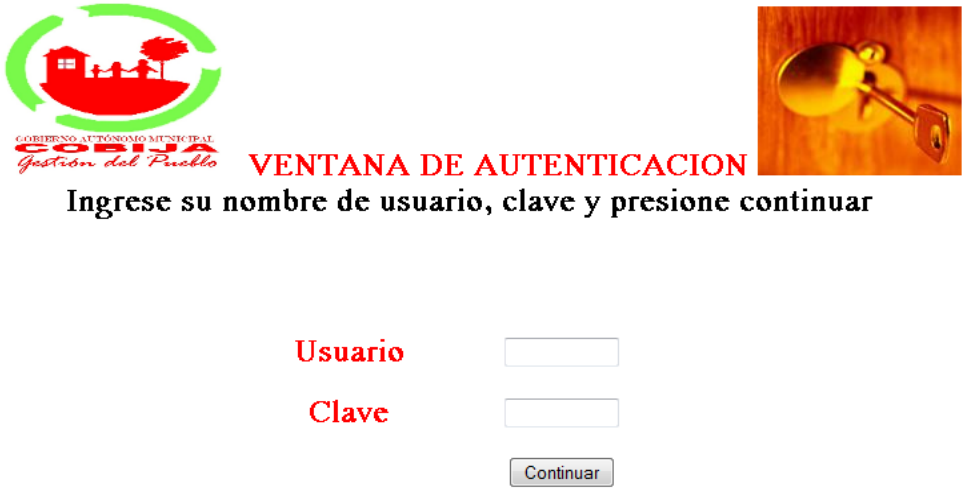


Figura 3.12.: *Ventana de autenticación de los usuarios*
Fuente: *Elaboración Propia*

FIGURA. 3.13*: Administración de los usuarios mediante la base de datos LDAP*
Fuente: *Elaboración Propia*

FIGURA 3.14: *Autenticación a la base de datos LDAP*
Fuente: *Elaboración Propia*

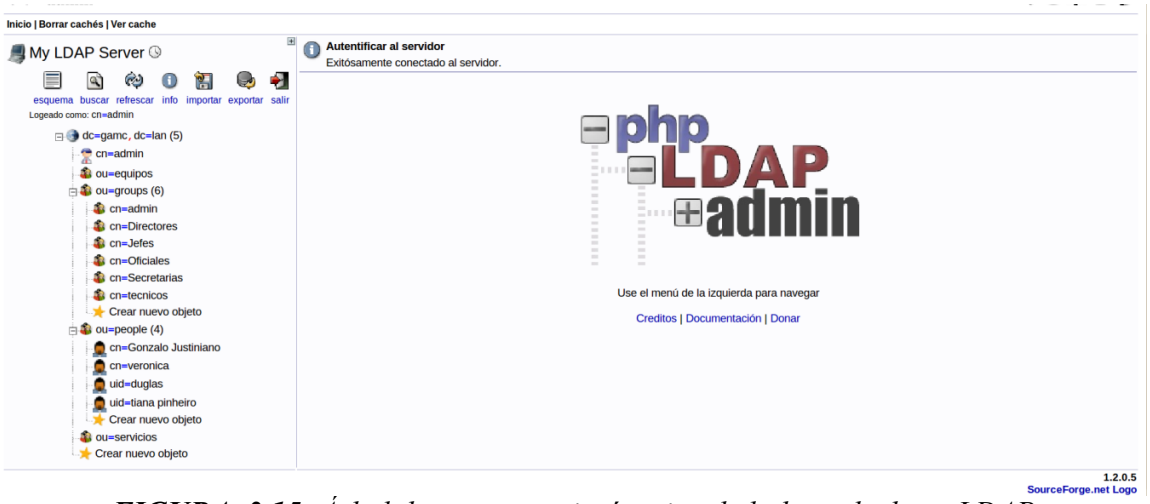


FIGURA. 3.15: *Árbol de estructura jerárquica de la base de datos LDAP*
Fuente: *Elaboración Propia*

Después de realizar la autenticación del administrador del sistema vemos el árbol jerárquico de la base de datos de acuerdo a cada categorización de los usuarios, el cual procedió a la conformación de grupos jerárquicos como ser el de Oficialía, Directores, jefes, Secretarias y Técnicos, a los que le es asignado usuarios de acuerdo a su función administrativa donde trabaja, mediante esta clasificación se procedió a establecer que existirán dos tipos de usuarios.

1. Usuarios con autorización acceder a impresión dentro de la red LAN.

2. Usuarios con acceso acceder a servidores dentro de la red LAN.

Se procede a dar la autorización correspondiente de esta forma estamos validando la conectividad entre cada uno de los usuarios registrados en el servidor Radius, dicho efecto observamos en la FIGURA 3.16

FIGURA 3.16: *Asignación de recursos de la red*
Fuente: *Elaboración Propia*

Para la planeación de la asignación de los recursos, se procedió a la determinación de los puntos que se encuentran cada uno de los equipos que se encuentran conectados a la red que funcionan como servidor de impresión para cada unidad, dirección u oficialía del predio central del Gobierno Autónomo Municipal de Cobija, para lo cual se utilizó el un diseño lógico de la red de cada una de los ambientes donde están funcionando las diferentes oficinas, esto permitió determinar con precisión la ubicación de cada uno de los servidores a los que los usuarios están conectados a la red de datos y que tendrán acceso al servicio, de acuerdo al plano se realizó el plan de asignación que se observa más detalladamente en el Anexo E, que se resume de acuerdo a la siguiente TABLA 3.16.

TABLA 3.16: *Plan de asignación de recursos por tipo de usuario*

Fuente: *Elaboración Propia*

	PLAN DE ASIGNACION POR TIPOS DE SERVICIOS		
Nivel / Cargo	**Servicios impresión**	**Servidor información**	**Privilegios**
Oficial	si	no	
Director	si	no	
Jefe	si	No	
Secretarias	no	No	De acuerdo a su función restringido
Técnicos	no	Si	De acuerdo a su función restringido

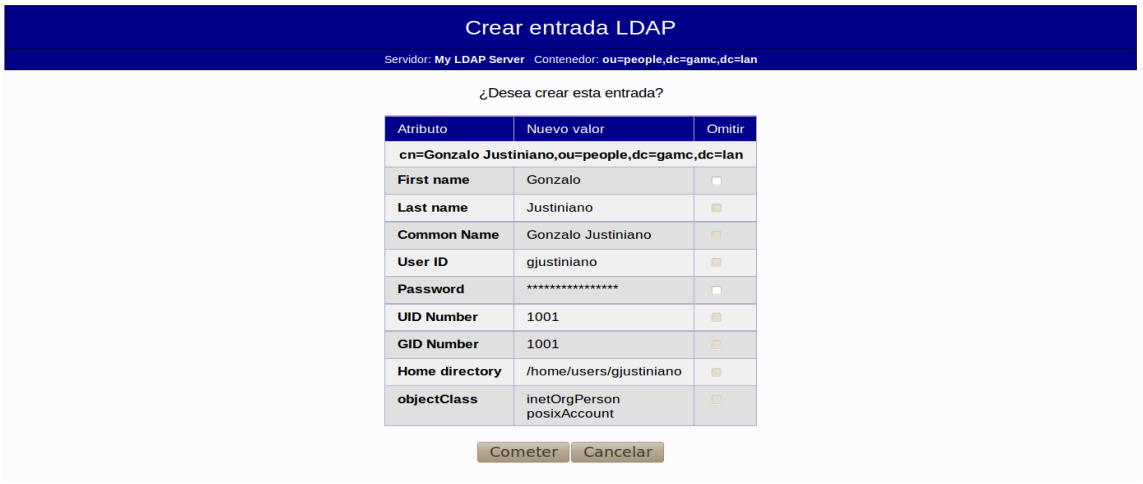


FIGURA 3.17: *Creación de la cuenta de usuarios.*
Fuente: *Elaboración Propia*

TRANSACIONES DE ALTAS Y BAJAS
INGRESO:

usuario.ldif

```
dn: uid=usuario,ou=          ,dc=!          ,dc=
uid: usuario
cn: usuario
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {CRYPT}0tw0q504FSU3I
shadowLastChange: 15624
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/usuario
gecos: usuario
```

FIGURA 3.18: *Contenido de Archivo LDIF de openldap*
Fuente: *Elaboración Propia*

MODIFICACIONES

ldapmodify –xvWD “cn=admin,dc=gamc,dc=lan” –f /etc/ldap/frontend.gamc.lan.ldif

```
dn: uid=duglas,ou=people,dc=gamc,dc=lan
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: duglas
sn: antequeira
givenName: duglas
cn: Duglas Antequeira
displayName: Duglas Antequeira
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: Duglas Antequeira
loginShell: /bin/bash
homeDirectory: /home/duglas
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: duglas.antequeira@example.com
postalCode: 31000
l: Toulouse
o: gamc
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: DA
replace loginShell:
        /bin/bash
replace uidNumber:
        500
replace gidNumber:
        500
replace homeDirectory:
        /home/
replace gecos:
        usuario
replace telephoneNumber:
        0984722963
modifying entry "uid=
                  o,ou=People,dc=
                                  ,dc=
                                      "
modify complete
```

FIGURA 3.19: *Comando de modificación y actualización de la BDLDAP*
Fuente: *Elaboración Propia*

PRODUCTO ACCION 4

Una vez implementado el sistema se observa como resultado lo siguiente:

Los paquetes capturados muestran el protocolo UDP como el más utilizado por los usuarios que circulan en la red inalámbrica y posterior a la implementación del sistema de autenticación se observa su disminución.

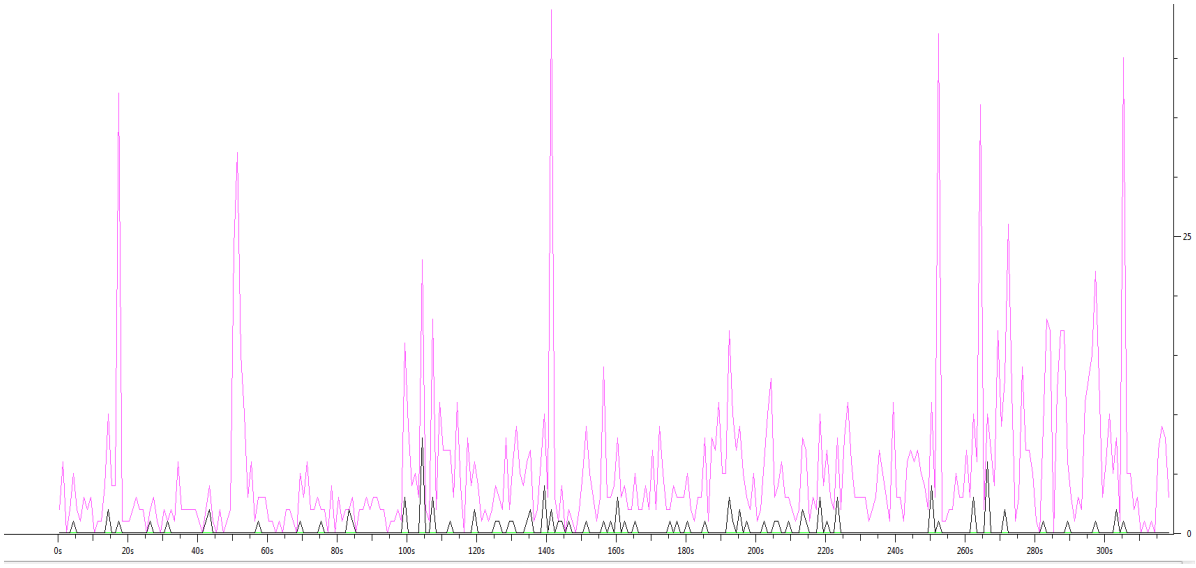


FIGURA 3.20: *Protocolo UDP utilizado sin el sistema de autenticación*

Fuente: *Elaboración propia*

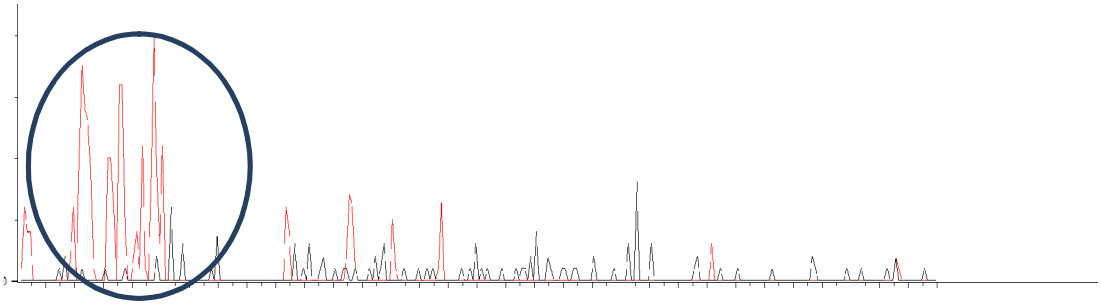


FIGURA 3.21: *Protocolo UDP utilizado con el sistema de autenticación*

Fuente: *Elaboración propia*

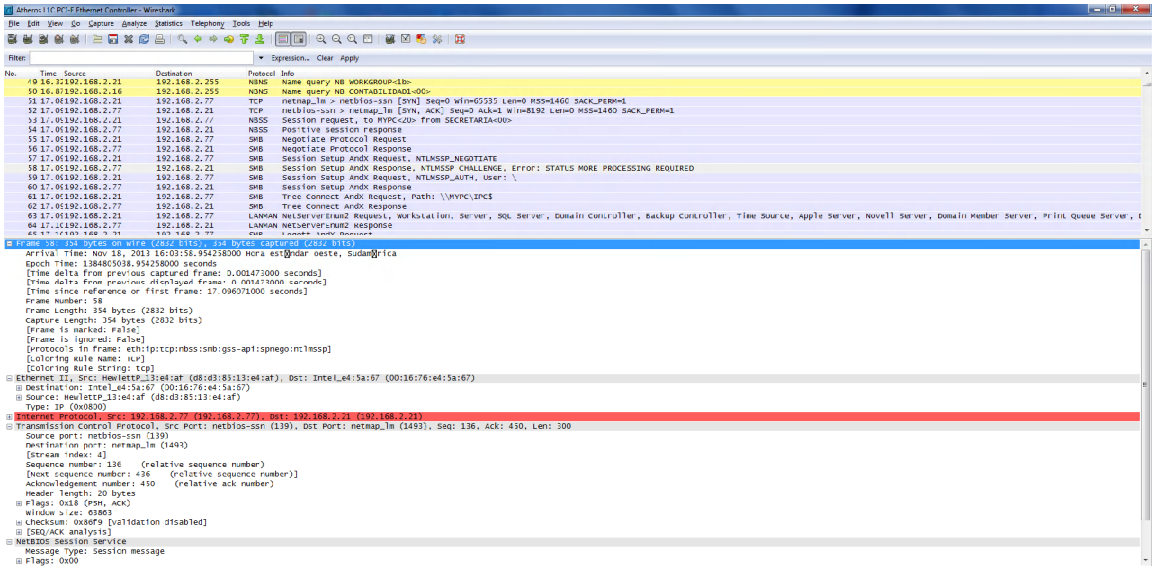


***FIGURA 3.22: C**aptura del suplicante al sistema de autenticación*

***Fuente:** Elaboración propia*

3.1.5 **ACCIÓN 5:** Desarrollar políticas de acceso a los recursos de la red.

La administración del sistema de AAA gestionado por Freeradius/Ldap, del cual es responsable el administrador del sistema, tiene como principal objetivo desarrollar, establecer y hacer cumplir políticas de administración y de uso del sistema logrando de esta forma establecer una administración que garantice la integridad, privacidad y la disponibilidad de los recursos cuando estas sean requerido.

Dentro de las normas y políticas, existe una propuesta de la jefatura de la unidad de sistemas del Gobierno Autónomo Municipal de Cobija, la cual debe ser corregida y aprobada por instancias superiores de la institución, los puntos más importantes está el buen uso de la red de datos, se propone que el sistema sea utilizada únicamente en la red inalámbrica siendo que la red alámbrica no cuenta con recursos de red administrable para la verificación de todo los puntos a detalle sobre la propuesta de política de seguridad para el acceso a los recursos de la red LAN del gobierno autónomo municipal de cobija, ver (anexo F).

CAPÍTULO IV
CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

De acuerdo al proyecto de grado desarrollado se tiene las siguientes conclusiones, que:

- Durante el análisis de la investigación de los antecedentes se identificó que los recursos de la red son los más expuestos a ataques internos y externos.
- Durante el análisis del desempeño de la red se evidencio que el 80% de las peticiones realizadas son generados por virus, troyanos, script dañinos que provocan la saturación de la red.
- La implementación de un servidor RADIUS integrado con OpenLDAP permite contar con un sistema de seguridad que solo permite el acceso a la red a usuarios validados.
- La aplicación de la política propuesta por la administración de redes, garantiza el buen funcionamiento y el adecuado uso de la red.

4.2 RECOMENDACIONES

En base a lo desarrollado se recomienda:

- Integrar con herramientas de administración de red para brindar una gestión de seguridad en la red de datos del Gobierno Autónomo Municipal de Cobija, a fin de garantizar la confidencialidad y la disponibilidad de los recursos.
- Que las políticas de control de acceso deberán ser actualizadas de acuerdo a los requerimientos de la institución así como la actualización de los roles para garantizar que los usuarios accedan a los recursos requerido.
- Realizar gestión de seguridad para garantizar la integridad, la fiabilidad y la confidencialidad de la información que fluye en la red de datos.

REFERENCIAS BIBLIOGRÁFICAS

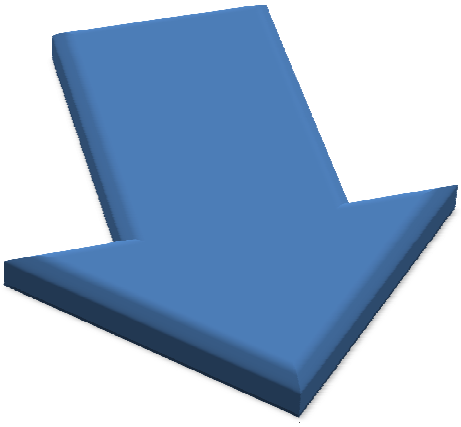
FUENTES ELECTRÓNICAS DE INFORMACIÓN

- **Bello, C. E. (Diciembre de 2000)**. Manual de Seguridad en Redes. Mexico.
- **Borghello, C. F. (2001).** *Seguridad Informatica: Sus Implicancias e Implementacion.*
- **Cardenas, A. A. (2003).** *Metodologia para la medicion y evaluacion del desempeño de redes de area local.* Bogota D.C.
- **Chiavenato, I. (2004).** *Introduccion a la Teoria General de la Administracion.* Mexico: McGraw-Hill Interamericana.
- **Cordoba Téllez Anabel, D. M. (Abril de 2010).** Diseño de un sistema de seguridad de control de acceso con Radius configurado en un sistema operativo Linux para una LAN inalambrica. Mexico,DF, México.
- **Creativecommons.org. (2006).** *Redes Inalámbricas en los paises en desarrollo.* Limehouse Book Sprint Team.
- **Fundacion Codigo Libre Dominicana. (2004)**. Guia de administracion de redes con Linux. Santo Domingo, Republica Dominicana.
- **Ingenieria, E. M. (2006).** *Metodologia de la Investigacion.* La Paz.
- **José María Barceló Ordinas, J. Í. (2004)**. *Redes de Computadores.* Barcelona - España: Fundació per a la Universitat Oberta de Catalunya.
- **Karanjit Siyan, P. D. (2000).** *Internet y Seguridad en Redes.* España: PRENTICE-HALL HISPANOAMERICANA, S.A.
- **Ontiveros, S. (2004).** *Metodologias par Administrar Redes.*
- **Piloña, A. J. (9 de Julio de 2002).** Metodologia para el diseño de redes de area local. Guatemala, Guatemala.
- **red hat Enterprise Linux 4. (2005).** *Introduccion a la Administracion de Sistemas*. Recuperado el 10 de Mayo de 2013, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/index.html
- **Seguridad Corporativa. (2009).** *seguridadcorporativa.org.* Recuperado el Lunes de Mayo de 2013, de http://www.seguridadcorporativa.org/info/Seguridad-online.html?ses=Y3JlPTEzNjg0NzU1MjEmdGNpZD13d3cuc2VndXJpZGFkY29ycG9yYXRpdmEub3JnNTE5MTQ3ODE0OGQwZjAuMzI3MjYwOTUmZmtpPTg4MDIz

ODA0JnRhc2s9c2VhcmNoJmRvbWFpbj1zZWd1cmlkYWRjb3Jwb3JhdGl2YS5vcmc
mcz04NDkyZTUwMmI5

- **Sharp, E. A. (2004).** *Seguridad en Internet e Intranet.* Madrid-España: Prentice hall.
- **Telefonica de España. (2006).** *Introduccion a la Telematica y a las Redes de datos.* Madrid España.
- **The FreeRADIUS Project. (2013).** *FreeRADIUS The world's most popular RADIUS Server.* Recuperado el Lunes de Mayo de 2013, de http://freeradius.org/
- **Torres, A. A. (2003).** Metodologia para la medicion y evaluacion del desempeño de redes de area local. Bogota D.C., Colombia.
- **Universidad Catolica del Peru. (2010)**. *Seguridad en sistemas informaticos.* Recuperado el 9 de Mayo de 2013, de http://biblioteca.pucp.edu.pe/docs/elibros_pucp/alcocer_carlos/24_Alcocer_2000_Redes_Cap_24.pdf
- **Universidad de Sevilla Departamento de Tecnologia Electronica. (2006).** Introduccio a la Seguridad en Redes de Computadores. Sevilla, España.
- **Universidad Nacional de Colombia. (2003).** Guia para elaboracion de politicas de seguridad. Bogota, Colombia.
- **Universidad Rey Juan Carlos. (2004).** Internet y Teleinformatica. Madrid, España.

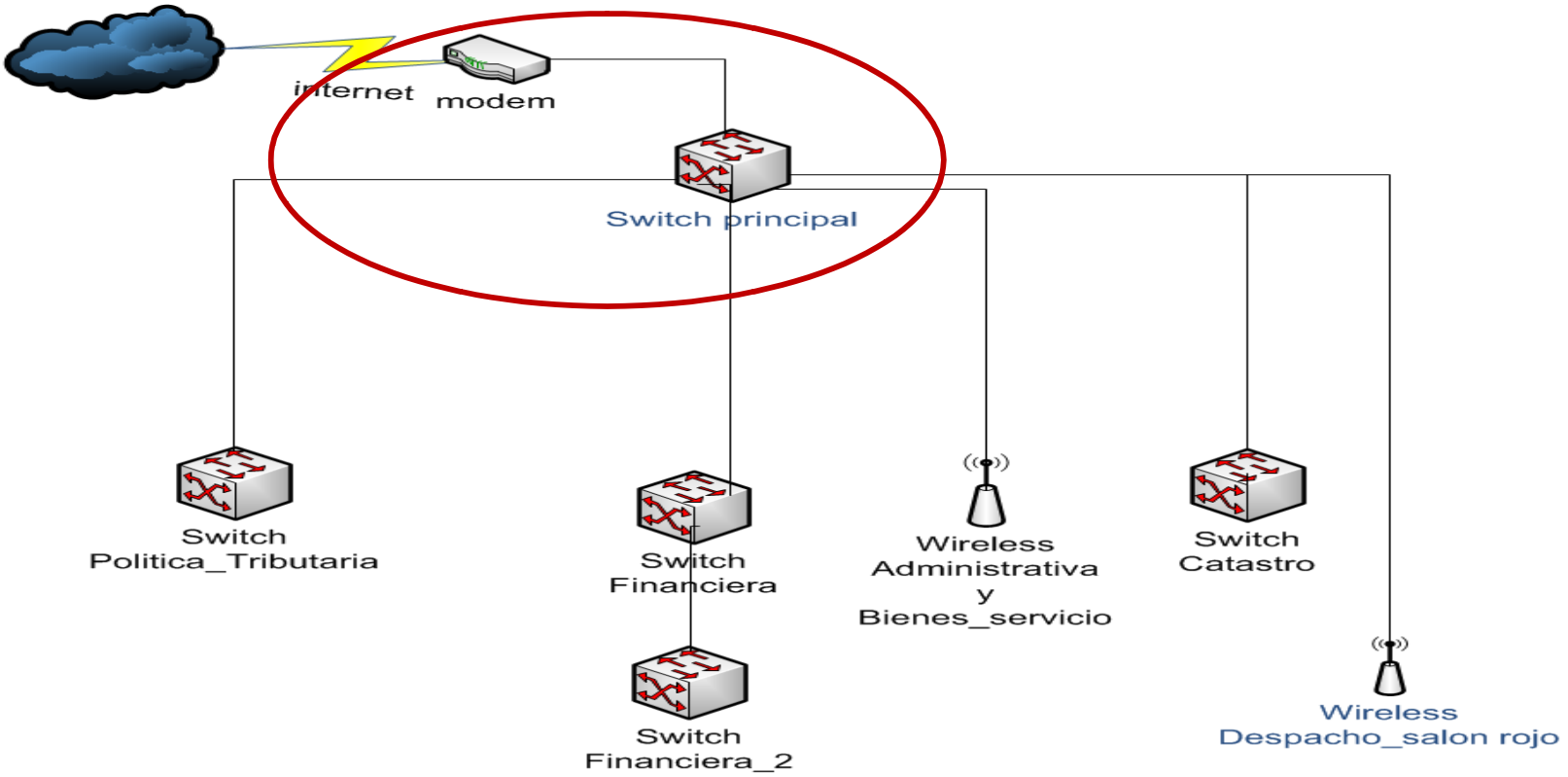
ANEXOS

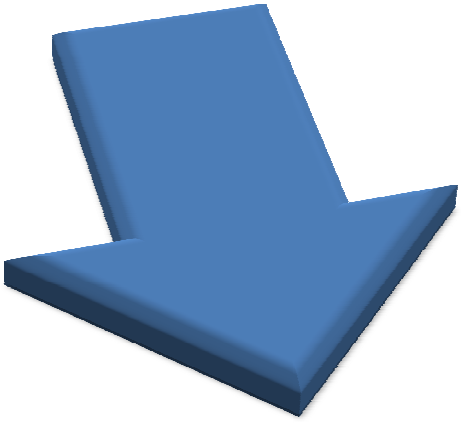


ANEXO A

DISEÑO LÓGICO DE LA RED LAN DEL GAM GESTIÓN 2010

DISEÑO LOGICO DE LA RED DE DATOS DEL GOBIERNO MUNICIPAL DE COBIJA GESTIÓN 2010

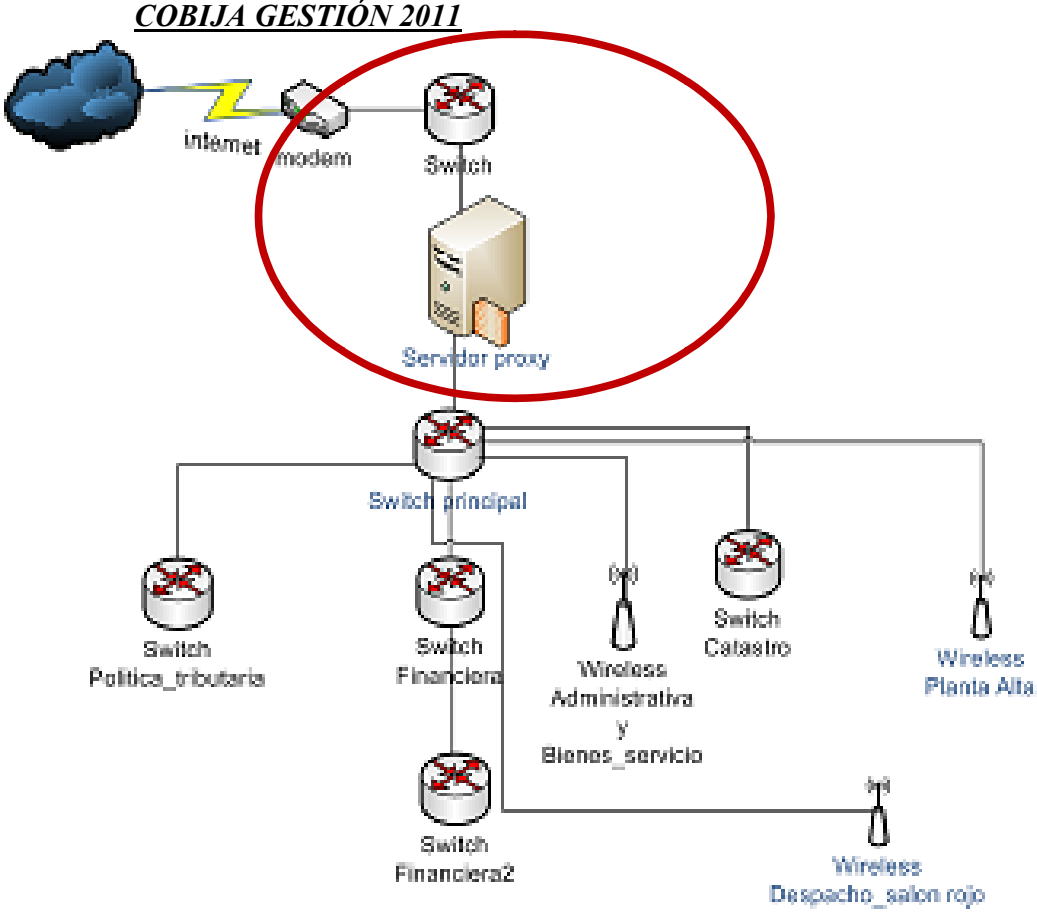


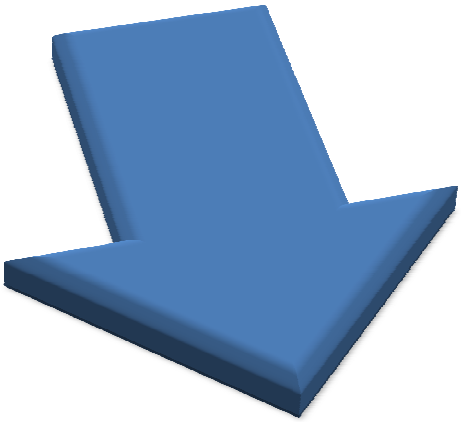


ANEXO B

DISEÑO LÓGICO DE LA RED LAN DEL GAM GESTIÓN 2011

DISEÑO LOGICO DE LA RED DE DATOS DEL GOBIERNO MUNICIPAL DE COBIJA GESTIÓN 2011





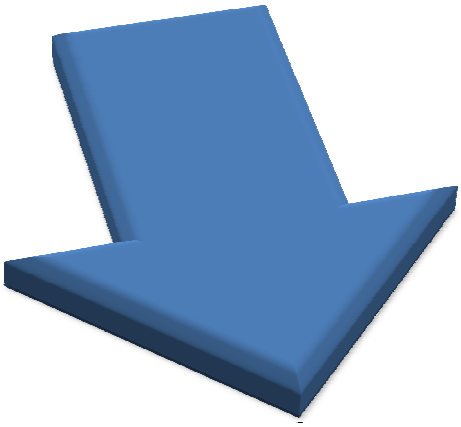
ANEXO C

LISTA DE CONTROL DE USUARIOS DE LA RED GAMC

LISTA DE CONTROL DE USUARIOS DE LA RED GOBIERNO MUNICIPAL DE COBIJA

Nº	GRUPO TRABAJO	IP	CARGO	USUARIO	TIPO/EQUIPO
1	FINANCIERA	192.168.2.16	CAJERA GENERAL	AIDE SUAREZ	Pc-Escritorio
2	FINANCIERA	192.168.2.17	TECNICO FINANCIERO	JHONNY	Pc-Escritorio
3	FINANCIERA	192.168.2.18	AUXILIAR SEGUIMIENTO	CASUMI NAKASHIMA	Pc-Escritorio
4	FINANCIERA	192.168.2.19	TECNICO SISTEMAS	DUGLAS ANTEQUEIRA	Pc-Escritorio
5	FINANCIERA	192.168.2.20	ENCARGADI DESCARGO	LILIANA A	Pc-Escritorio
6	FINANCIERA	192.168.2.21	SECRETARIA	KATIANA FLORES	Pc-Escritorio
7	FINANCIERA	192.168.2.22	DIRECTOR	WILSON VIDAURRE	Pc-Escritorio
8	FINANCIERA	192.168.2.23	ENCARAGADO TESORO Y CP	PAULA	Pc-Escritorio
9	FINANCIERA	192.168.2.24	AUXILIAR CONTABLE	KENIA ZABALA	Pc-Escritorio
10	FINANCIERA	192.168.2.25	CONTADOR	MILTON SORIA	Pc-Escritorio
11	FINANCIERA	192.168.2.26	JEFE PRESUPUESTO	SANABRIA	Pc-Escritorio
12	FINANCIERA	192.168.2.27	AUXILIAR PRESUPUESTO	ABIGAIL AYUVIRI	Pc-Escritorio
13	FINANCIERA	192.168.2.28	SERVIDOR SINCON	DIRECCION FINANCIERA	Pc-Escritorio
14	TRANSPARENCIA	192.168.2.33	ASESOR LEGAL DE INFORME	YOVANA	Pc-Escritorio
15	TRANSPARENCIA	192.168.2.34	DESCARGO	MEDARDO	Pc-Escritorio
16	TRANSPARENCIA	192.168.2.35	DIRECTOR TRANSPARENCIA	LIBERTAD AGUADA	Portatil
17	VENTANILLA	192.168.2.40	VENTANILLA UNICA	SANDRA	Pc-Escritorio
18	BIENES Y SERVICIOS	192.168.2.43	JEFE BIENES Y SERVICIOS	INES APAZA	Portatil
19	BIENES Y SERVICIOS	192.168.2.44	AUXILIAR BYS	ARIEL JUSTINIANO	Pc-Escritorio
20	BIENES Y SERVICIOS	192.168.2.45	COTIZADOR	GABRIELA/YULI	Pc-Escritorio
21	BIENES Y SERVICIOS	192.168.2.46	SECRETARIA BYS	DANIELA	Pc-Escritorio
22	BIENES Y SERVICIOS	192.168.2.47	COTIZADOR COMPRAS MEN	LEO	Pc-Escritorio
23	BIENES Y SERVICIOS	192.168.2.48	ENCARGADO DE ARCHIVOS BIENES Y SERVICIOS	ENRIQUE	Pc-Escritorio
24	BIENES Y SERVICIOS	192.168.2.49	COTIZADOR	DANIELA	Pc-Escritorio
25	DIRECCION ADMINNISTRATIVA	192.168.2.58	DIRECTOR ADMIN	VERONICA DOMINGUES	Portatil
26	DIRECCION ADMINNISTRATIVA	192.168.2.59	SECRETARIA	VIRGINIA CHIGUANTO	Pc-Escritorio
27	DIRECCION ADMINNISTRATIVA	192.168.2.60	ENCARGADO PAGO SERVICIOS BASICOS	FREDDY	Pc-Escritorio
28	SICOES	192.168.2.64	ENCARGADA DE SICOES	LISETH BENITEZ	Pc-Escritorio
29	SEGUIMFINANACIERO	192.168.2.66	RESP.SEGUMIENTO DE ARCHIVOS	TANIA	Pc-Escritorio
30	SEGUIMFINANACIERO	192.168.2.67	JEFE SEGUIMIENTO FINANCIERO	YONNER REYES	PORTATIL
31	SEGUIMFINANACIERO	192.168.2.68	AUXILIAR	FABIOLA	Pc-Escritorio
32	ACTIVO_FIJOS	192.168.2.69	JEFA ACTIVOS FIJOS	AMANDA	Portatil
33	ACTIVO_FIJOS	192.168.2.70	REPONSABLE SISTEMA	ROLANDO CHIPANA	Portatil
34	ACTIVO_FIJOS	192.168.2.71	ASISTENTE ACTIVO FIJOS	SILVESTRE	Pc-Escritorio
35	ACTIVO_FIJOS	192.168.2.72	AUXILIAR	GROVER	Pc-Escritorio
36	ACTIVO_FIJOS	192.168.2.74	AUXILIAE ACTIVO FIJOS	CRISTINA RIBEIRO	Pc-Escritorio
37	ACTIVO_FIJOS	192.168.2.75	AUXILIAR	YOVANA	Pc-Escritorio
38	ACTIVO_FIJOS	192.168.2.76	AUXILIAR ACTFIJOS	IVAN ROJAS	Pc-Escritorio
39	SISTEMAS	192.168.2.77	RESP.REDES E INTERNET	RENELSY ROJAS	Portatil
40	SISTEMAS	192.168.2.78	DESARROLLADOR SISTEMAS	JORGE CHIPANA-YOR	Portatil
41	SISTEMAS	192.168.2.80	RESP-HARDWARE SOFTWARE	EDGAR EDWIN NINA CHURA	Portatil
42	SISTEMAS	192.168.2.81	JEFE UNIDAD SISTEMA	SILVIA CARABALLO	Pc-Escritorio
43	RRHH	192.168.2.82	ENCARGADA DE PROCESOS	FIRUTTE SADAFI	Pc-Escritorio
44	RRHH	192.168.2.83	ENCARGADA DE ARCHIVOS	NOEMI	Pc-Escritorio
45	RRHH	192.168.2.84	JEFE	GONZALO JUSTINIANO	Pc-Escritorio

46	RRHH	192.168.2.85	ENC.PLANILLAS	FERNANDO PELAES	Pc-Escritorio
47	RRHH	192.168.2.86	SECRETARIA	NATALY	Pc-Escritorio
48	RRHH	192.168.2.87	ASESOR JURIDICO	MILENKA	Pc-Escritorio
49	RRHH	192.168.2.88	RESPONSABLE MANEJO FILE	DEILY	Pc-Escritorio
50	PLANIFICACION	192.168.2.90	TECNICO PLANIFICADOR	ROY ROJAS	Portatil
51	PLANIFICACION	192.168.2.91	POA-PLANIFICADOR	CLAVEL	Portatil
52	PLANIFICACION	192.168.2.92	RESPONSABLE SISIM	ARISTOFANIS COCA	Pc-Escritorio
53	PLANIFICACION	192.168.2.93	JEFE DESARROLLO ORGANIZACIONAL	ERWIN MACUAPA	Pc-Escritorio
54	PLANIFICACION	192.168.2.94	DIRECTOR	LUIS ALBERTO CORDERO	Portatil
55	PLANIFICACION	192.168.2.95	AUXILIAR	PEDRO	Pc-Escritorio
56	JURIDICA	192.168.2.98	DIRECTOR-JURIDICA	TIANA PINHEIRO	Portatil
57	JURIDICA	192.168.2.100	ASESOR JURIDICO	JACINTO CONDORI TORRES	Pc-Escritorio
58	JURIDICA	192.168.2.101	ASESOR JURIDICO	ALEXANDER CASTEDO	Pc-Escritorio
59	JURIDICA	192.168.2.102	ASESOR JURIDICO	DINA VACA CARAICA	Pc-Escritorio
60	JURIDICA	192.168.2.103	ASESOR JURIDICO	VICTOR RENGEL AREVALO	Pc-Escritorio
61	JURIDICA	192.168.2.104	AUXILIAR	EDWIN	Pc-Escritorio
62	GABINETE	192.168.2.105	RELACIONES PUBLICAS	BRENDA	Pc-Escritorio
63	GABINETE	192.168.2.106	ALCALDESA	ANA LUCIA REIS	Pc-Escritorio
64	GABINETE	192.168.2.107	ASISTENTE DESPACHO	JUAN CARLOS	Pc-Escritorio
65	OMAF	192.168.2.108	OFICIAL MAYOR	RENATO APURI	Portatil
66	OMAF	192.168.2.109	SECRETARIA OMAF	LETICIA	Pc-Escritorio
68	OMAF	192.168.2.111	ASISTENTE OMAF	ADOLFO	Pc-Escritorio
69	PLANIFICACION	192.168.2.113	SECTRARIA PLA IFICACION	DIOLY	Pc-Escritorio
70	DESPACHO	192.168.2.118	JUEZ SUMARIANTE	CICERO	PORTATIL
72	DESPACHO	192.168.2.120	ALCALDESA		PORTATIL



ANEXO D

INSTALACIÓN Y CONFIGURACIÓN DE FREERADIUS

INSTALACION DE FREERADIUS

Instalamos todas las herramientas que nos hacen falta para la compilación y posterior instalación de Freeradius.

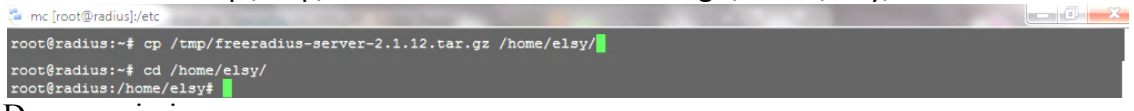
Para ello, desde el terminal, como administrador (superusuario), tecleamos:

#apt-get install libssl-dev

#apt-get install build-essential

Copiamos el fichero descargado a nuestra carpeta de trabajo (/home/"usuario"), y lo descomprimimos haciendo uso de tar:

root@radius:~# cp /tmp/freeradius-server-2.1.12.tar.gz /home/elsy/



Descomprimimos:

Vemos la carpeta ya descomprimida

```
root@radius:/home/elsy# ls
Descargas   Escritorio                freeradius-server-2.1.12.tar.gz  MÃºsica     PÃºblico
Documentos  freeradius-server-2.1.12  ImÃ¡genes                        Plantillas  VÃdeos
root@radius:/home/elsy#
```

Copiamos la carpeta correspondiente a la raíz (/).

```
root@radius:/home/elsy# cp -r freeradius-server-2.1.12 /
root@radius:/home/elsy# cd
root@radius:~# /
-bash: /: es un directorio
root@radius:~# cd /
root@radius:/# ls
bin   dev  freeradius-server-2.1.12  initrd.img  lost+found  mnt  proc  sbin     srv  tmp  var
boot  etc  home                     lib         media       opt  root  selinux  sys  usr  vmlinuz
root@radius:/#
```

Luego nos vamos a la carpeta raíz de freeradius-server:

```
root@radius:~# cd /
root@radius:/# ls
bin   dev  freeradius-server-2.1.12  initrd.img  lost+found  mnt  proc  sbin     srv  tmp  var
boot  etc  home                     lib         media       opt  root  selinux  sys  usr  vmlinuz
root@radius:/# cd /freeradius-server-2.1.12/
root@radius:/freeradius-server-2.1.12#
```

Procedemos a la configuración e instalación:

./configure –without-rlm_smb –without-rlm_perl –without-rlm_ldap –without-rlm_krb5

#Make

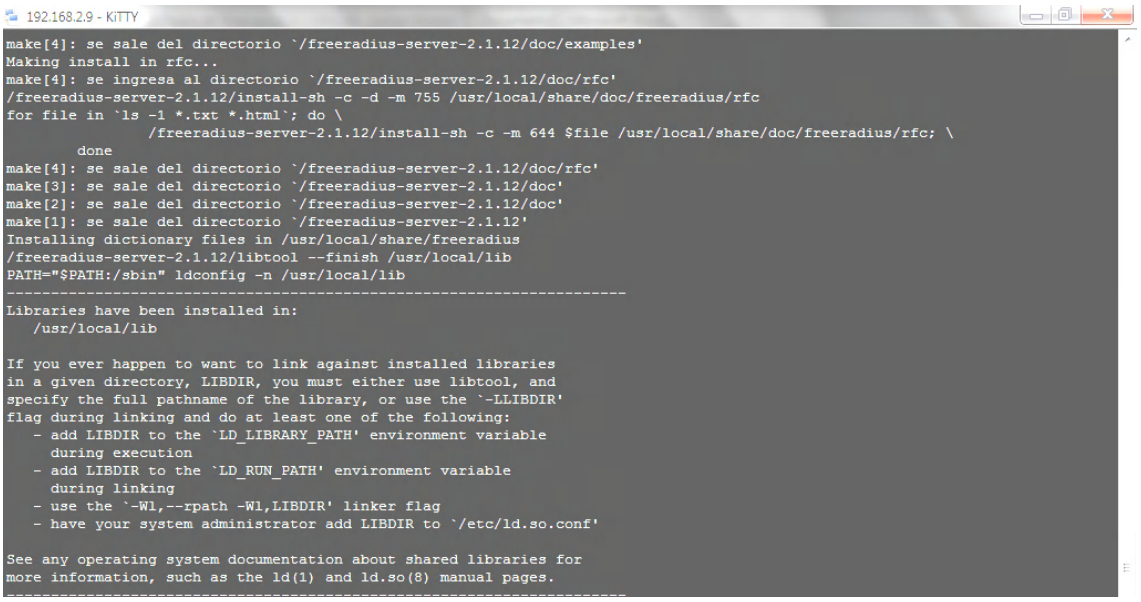
Una ves finalizado el make seguimos con el siguiente comando:

192.168.2.9 - KiTTY

```
"i686-pc-linux-gnu\" -DRADIUSD_VERSION=\"2.1.12\" -DOPENSSL_NO_KRB5 -c radconf2xml.c  -fPIC -DPIC -o .libs/radconf2xml.o
 gcc -g -O2 -Wall -D_GNU_SOURCE -D_REENTRANT -D_POSIX_PTHREAD_SEMANTICS -DNDEBUG -I/freeradius-server-2.1.12/src -DHOSTINFO=\
"i686-pc-linux-gnu\" -DRADIUSD_VERSION=\"2.1.12\" -DOPENSSL_NO_KRB5 -c radconf2xml.c -o radconf2xml.o >/dev/null 2>&1
/freeradius-server-2.1.12/libtool --mode=link gcc   -o radconf2xml radconf2xml.lo /freeradius-server-2.1.12/src/lib/libfreera
dius-radius.la util.lo log.lo conffile.lo -lnsl -lresolv  -lpthread
gcc -o .libs/radconf2xml .libs/radconf2xml.o .libs/util.o .libs/log.o .libs/conffile.o  /freeradius-server-2.1.12/src/lib/.li
bs/libfreeradius-radius.so -lnsl -lresolv -lpthread
creating radconf2xml
make[4]: se sale del directorio `/freeradius-server-2.1.12/src/main'
make[3]: se sale del directorio `/freeradius-server-2.1.12/src'
make[2]: se sale del directorio `/freeradius-server-2.1.12/src'
Making all in raddb...
make[2]: se ingresa al directorio `/freeradius-server-2.1.12/raddb'
make[2]: se sale del directorio `/freeradius-server-2.1.12/raddb'
Making all in scripts...
make[2]: se ingresa al directorio `/freeradius-server-2.1.12/scripts'
make[2]: No se hace nada para `all'.
make[2]: se sale del directorio `/freeradius-server-2.1.12/scripts'
Making all in doc...
make[2]: se ingresa al directorio `/freeradius-server-2.1.12/doc'
make[3]: se ingresa al directorio `/freeradius-server-2.1.12/doc'
Making all in examples...
make[4]: se ingresa al directorio `/freeradius-server-2.1.12/doc/examples'
make[4]: No se hace nada para `all'.
make[4]: se sale del directorio `/freeradius-server-2.1.12/doc/examples'
Making all in rfc...
make[4]: se ingresa al directorio `/freeradius-server-2.1.12/doc/rfc'
make[4]: No se hace nada para `all'.
make[4]: se sale del directorio `/freeradius-server-2.1.12/doc/rfc'
make[3]: se sale del directorio `/freeradius-server-2.1.12/doc'
make[2]: se sale del directorio `/freeradius-server-2.1.12/doc'
make[1]: se sale del directorio `/freeradius-server-2.1.12'
root@radius:/freeradius-server-2.1.12#
```

#make install

```
root@radius:/freeradius-server-2.1.12# Make install
```



De esta forma ya tenemos instalado nuestro servidor FreeRadius.

CONFIGURACION DE FREERADIUS

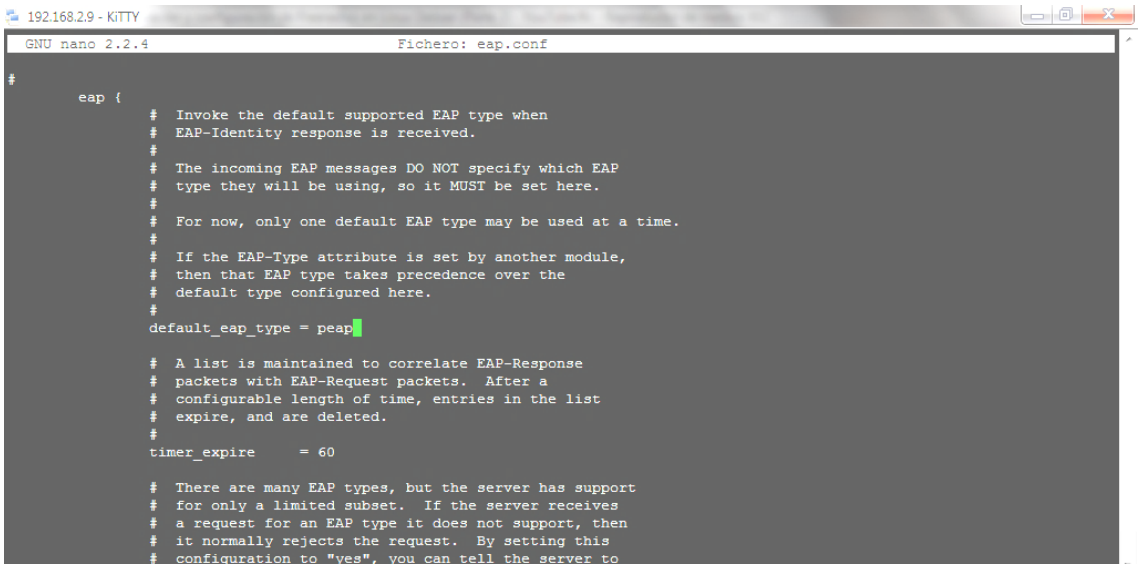
Procederemos a realizar la configuración de Freeradius. Los ficheros de configuración del servidor Radius, se encuentra en /usr/local/etc/raddb. Para configurar el servidor modificamos ciertos parámetros de los ficheros de configuración del servidor Radius: eap.conf

Lo primero que hacemos es movernos hasta el directorio donde se encuentran los ficheros
de configuración (/usr/local/etc/raddb):

Luego sacamos una copia del fichecho eap.conf el comando:

Luego editamos el fichero:

Modificamos default_eap_type: Cambiamos el valor md5 (por defecto) a peap.



Modificamos el ficheros de los usuarios que van a tener acceso al servidor

Users

Realizamos una copia del fichero users a users1.

En este fichero daremos de alta los nombres de usuario y contraseña que podrán ser usados para autenticarse frente al servidor Radius.

Editamos el fichero users con un editor de texto, como per ejemplo nano:

En este fichero añadiremos al final del mismo, tantos usuarios como queramos, con el formato:

Guardamos y salimos del fichero

El siguiente fichero que se modificar es el:

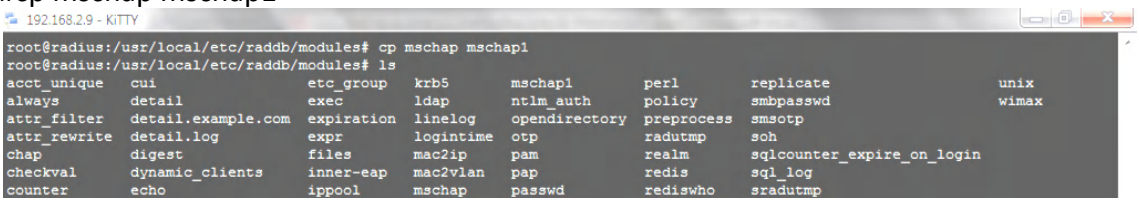
Mschap

Accedemos a la carpeta modules:

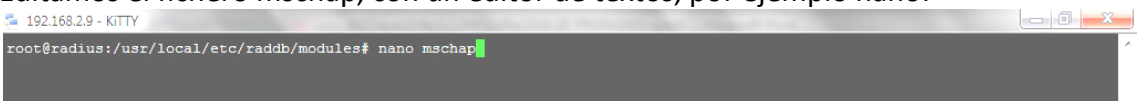
#cd modules

Realizamos una copia de seguridad del fichero mschap a mschap1:

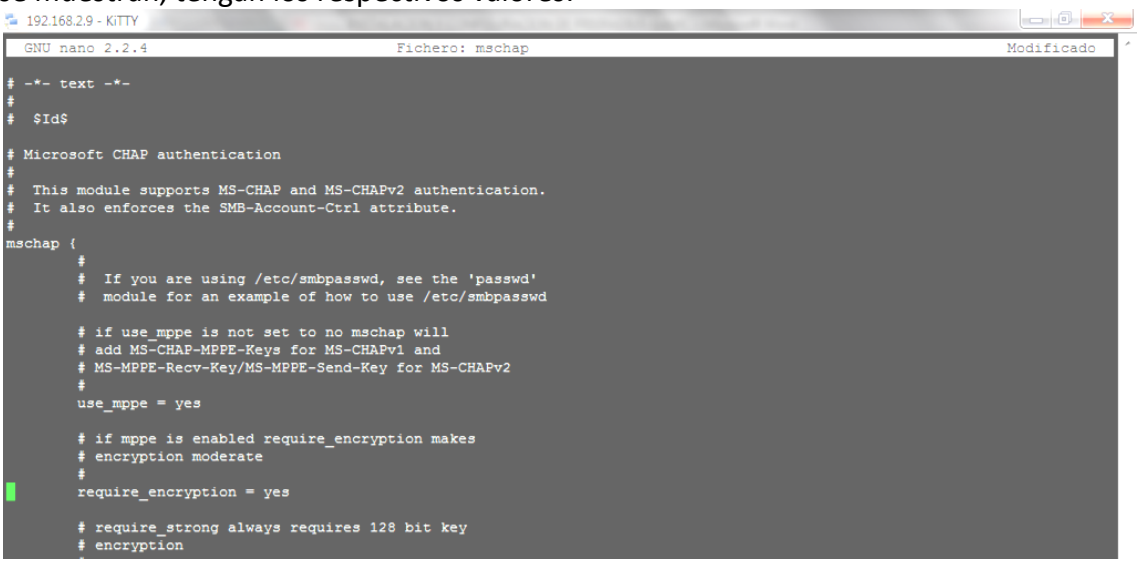
#cp mschap mschap1



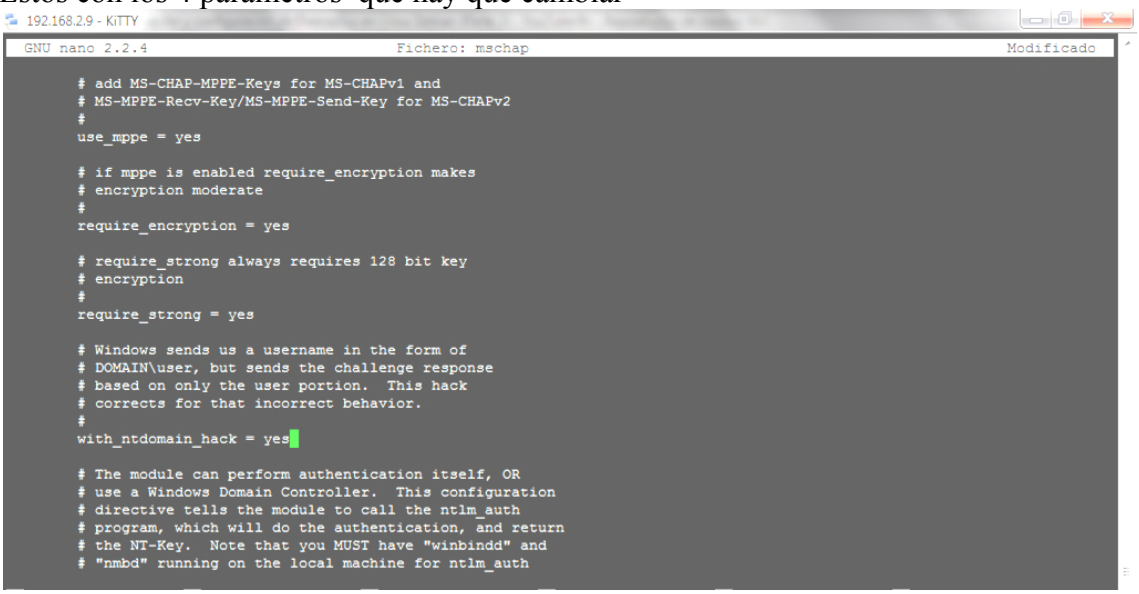
Editamos el fichero mschap, con un editor de textos, por ejemplo nano:



Y realizamos los cambios adecuados para que las distintas variables que a continuación se muestran, tengan los respectivos valores:



Estos con los 4 parametros que hay que cambiar



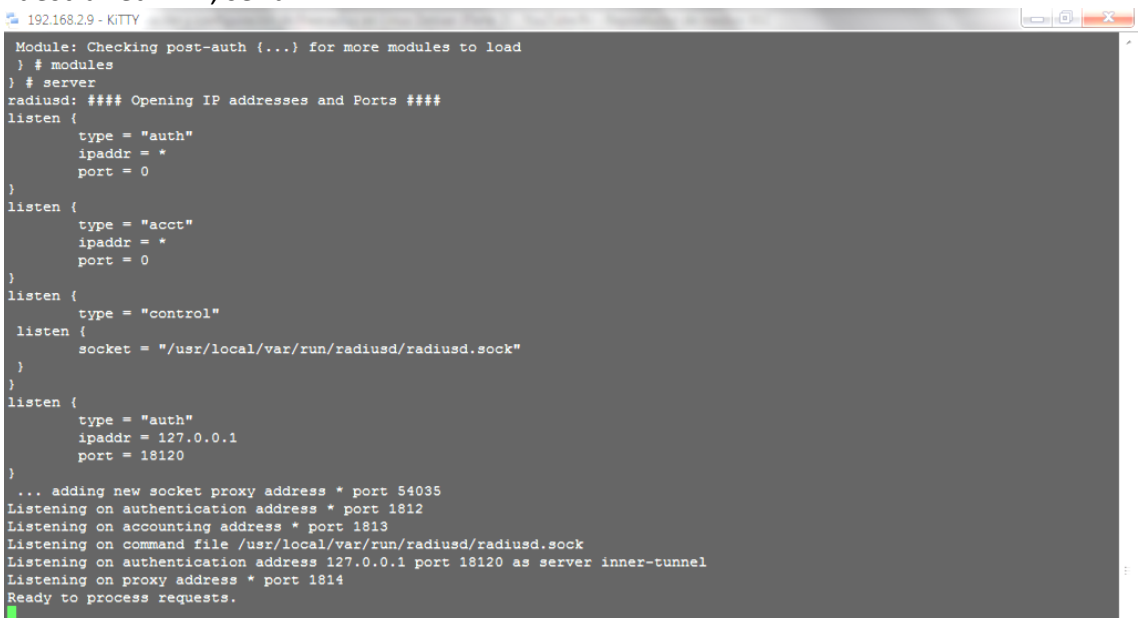
Una vez realizados los cambios, guardamos y salimos.

Para que los cambios realizados en la configuración sean cargados en radius, pasaremos a

ejecutar el siguiente comando:

Prueba del funcionamiento del servidor Radius FREERADIUS

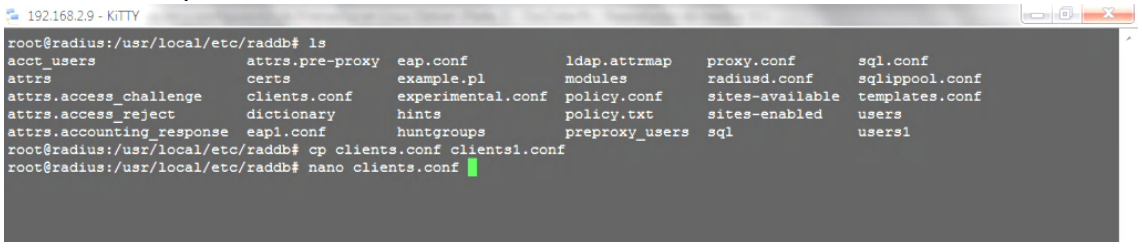
Para poner en funcionamiento nuestro servidor, ejecutaremos:
#/usr/local/sbin/radiusd –f –X
El aspecto de la pantalla, de Freeradius, a la espera que algún cliente se intente conectar a
nuestra red Wifi, sería:

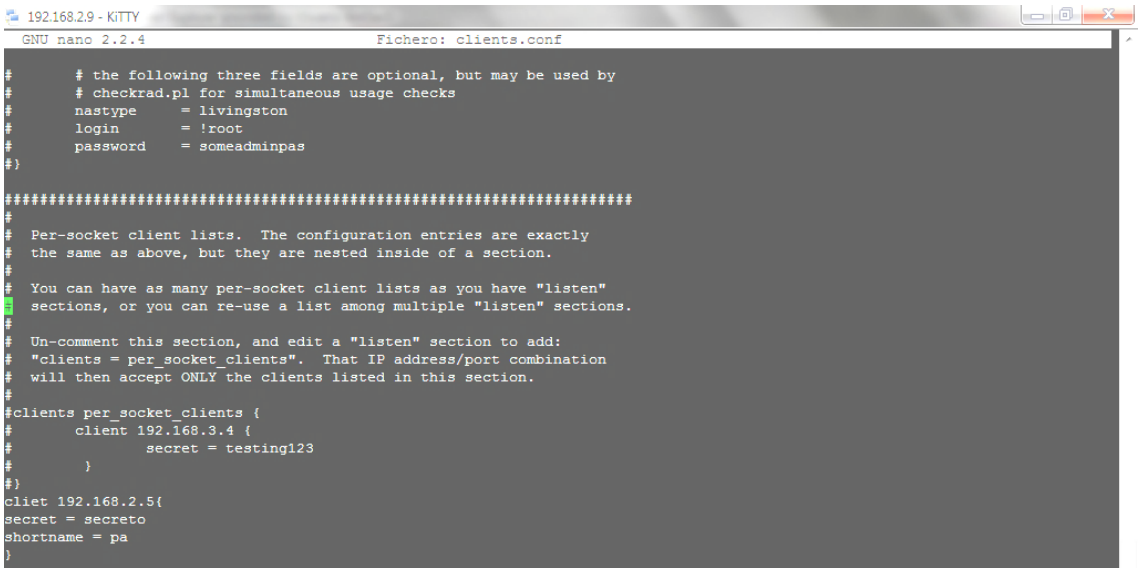


Con lo que se lanza el demonio de Freeradius.

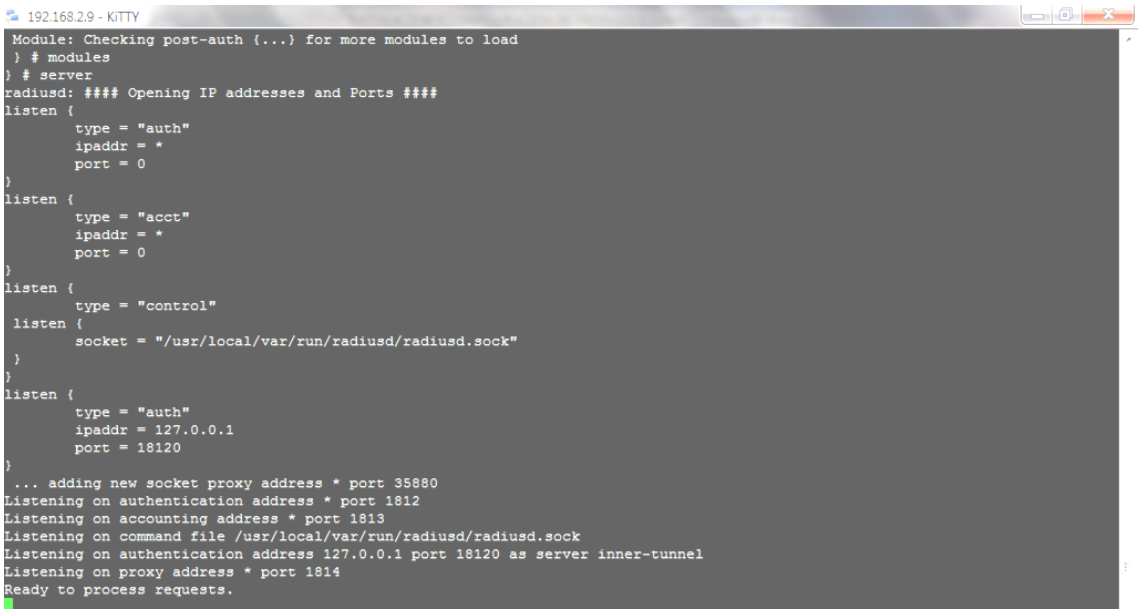
Configuración del cliente en nuestro servidor Radius Freeradius

Solo nos queda en este momento, en lo que se refiere a la configuración de nuestro servidor
Radius Freeradius, el configurar el cliente (punto de acceso) que va a hacer uso de sus servicios.
Para ello, accedemos a /usr/local/etc/raddb, hacer una copia del fichero clients.conf a clients1.conf, y añadir el cliente:



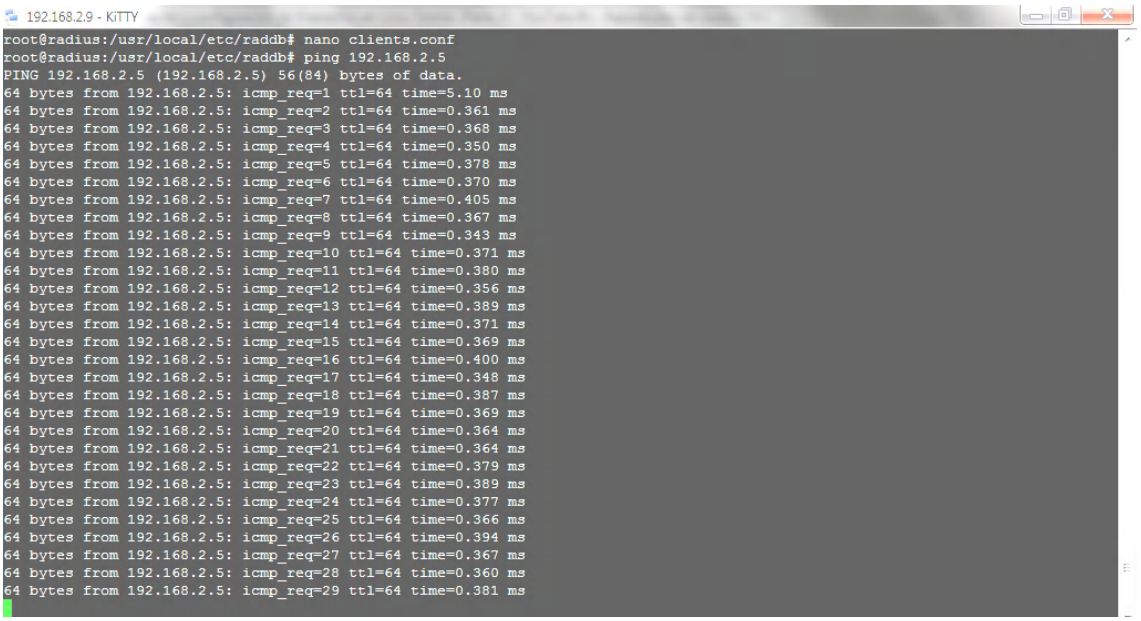


Una vez dado de alta el cliente, paramos Radius y volvemos a levantar.



Configuración de nuestro Punto de Acceso Wifi

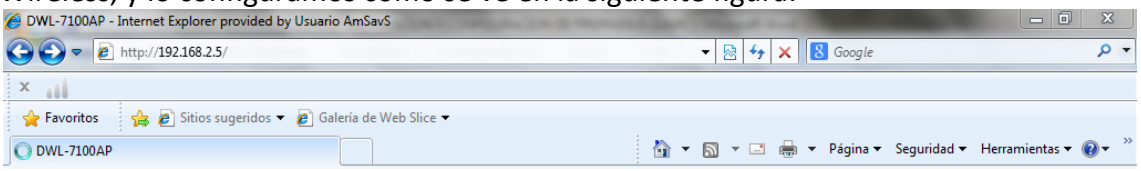
Verificamos que nuestro punto de acceso este activado

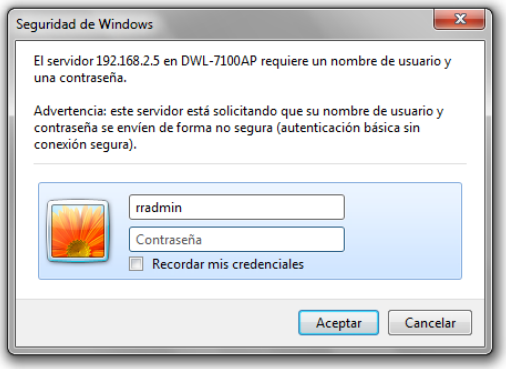


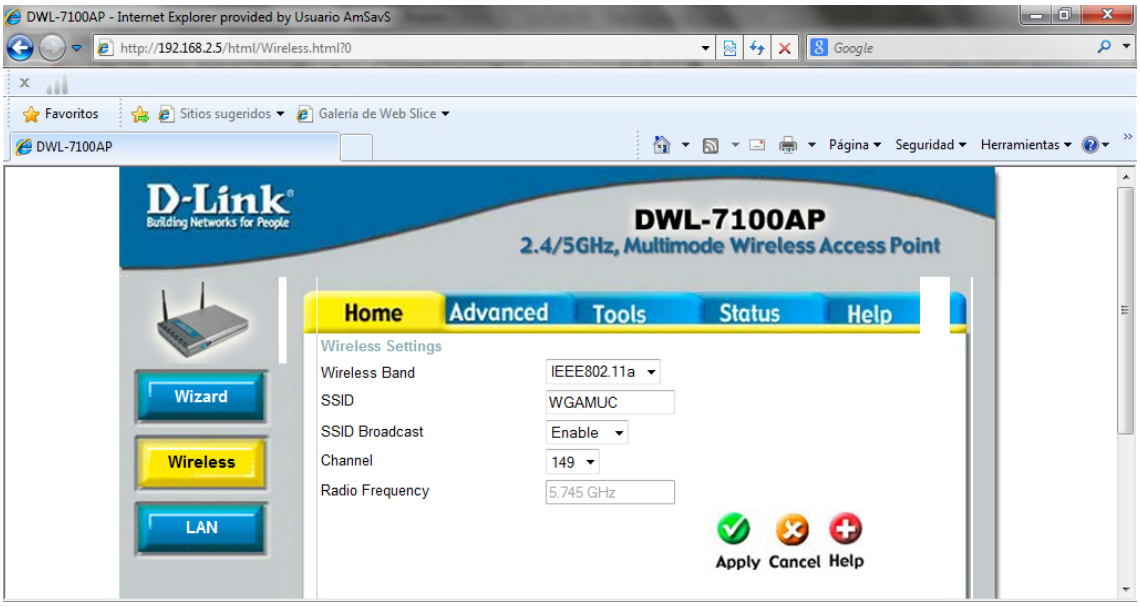
Configuraremos un punto de acceso. En concreto vamos a utilizar un punto de acceso AP DWL 7100AP

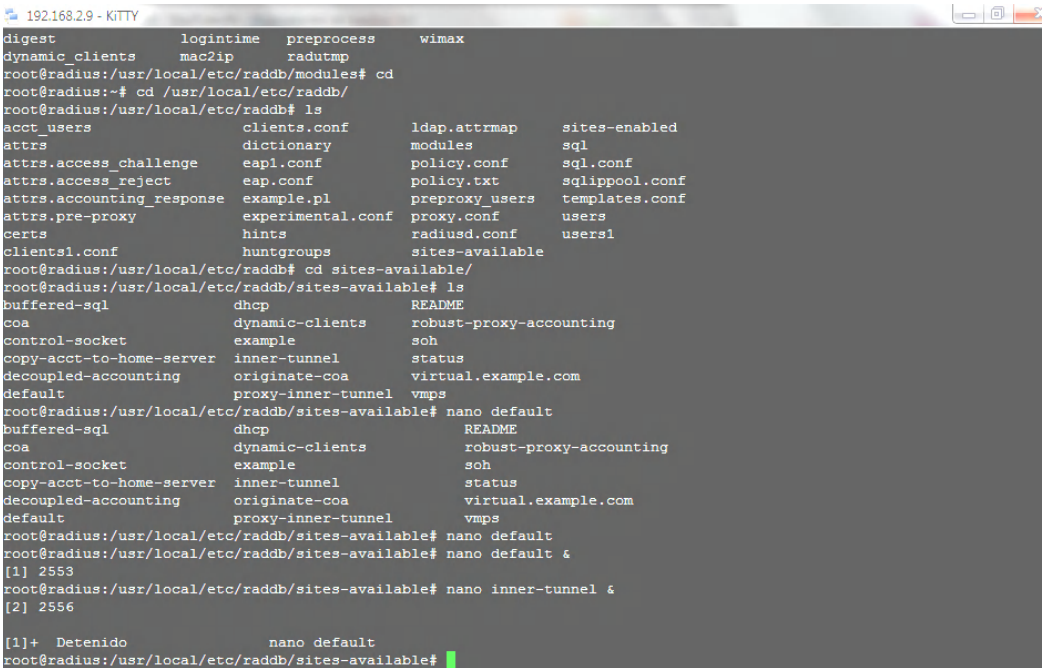
Lo conectamos a nuestro servidor Radius, y accedemos a su dirección IP (192.168.2.5) desde un navegador. Una vez en su panel de configuración, accedemos a la sección de configuración

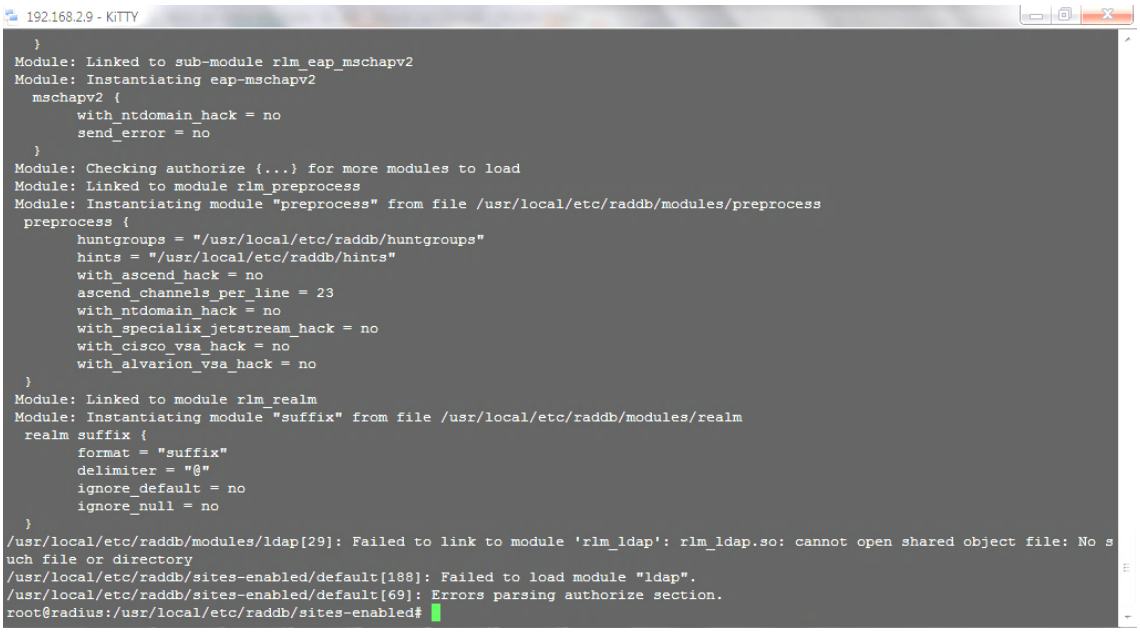
Wireless, y lo configuramos como se ve en la siguiente figura:

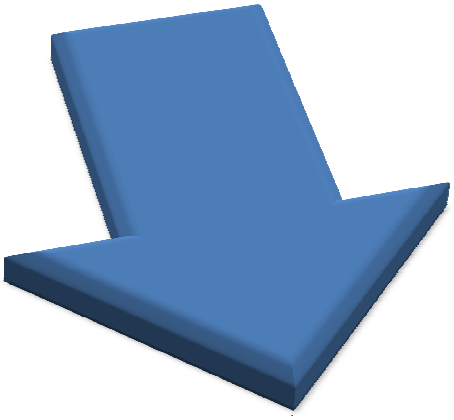





DWL-7100AP - Internet Explorer provided by Usuario AmSavS
http://192.168.2.5/html/Wireless.html?0
Favoritos
Sitios sugeridos
Galería de Web Slice
DWL-7100AP
Página
Seguridad
Herramientas
D-Link
Building Networks for People
DWL-7100AP
2.4/5GHz, Multimode Wireless Access Point
Home
Advanced
Tools
Status
Help
Wizard
Wireless
LAN
Wireless Settings
Wireless Band
IEEE802.11a
SSID
WGAMUC
SSID Broadcast
Enable
Channel
149
Radio Frequency
5.745 GHz
Apply
Cancel
Help


192.168.2.9 - KiTTY
digest logintime preprocess wimax
dynamic_clients mac2ip radutmp
root@radius:/usr/local/etc/raddb/modules# cd
root@radius:~# cd /usr/local/etc/raddb/
root@radius:/usr/local/etc/raddb# ls
acct_users clients.conf ldap.attrmap sites-enabled
attrs dictionary modules sql
attrs.access_challenge eap1.conf policy.conf sql.conf
attrs.access_reject eap.conf policy.txt sqlippool.conf
attrs.accounting_response example.pl preproxy_users templates.conf
attrs.pre-proxy experimental.conf proxy.conf users
certs hints radiusd.conf users1
clients1.conf huntgroups sites-available
root@radius:/usr/local/etc/raddb# cd sites-available/
root@radius:/usr/local/etc/raddb/sites-available# ls
buffered-sql dhcp README
coa dynamic-clients robust-proxy-accounting
control-socket example soh
copy-acct-to-home-server inner-tunnel status
decoupled-accounting originate-coa virtual.example.com
default proxy-inner-tunnel vmps
root@radius:/usr/local/etc/raddb/sites-available# nano default
buffered-sql dhcp README
coa dynamic-clients robust-proxy-accounting
control-socket example soh
copy-acct-to-home-server inner-tunnel status
decoupled-accounting originate-coa virtual.example.com
default proxy-inner-tunnel vmps
root@radius:/usr/local/etc/raddb/sites-available# nano default
root@radius:/usr/local/etc/raddb/sites-available# nano default &
[1] 2553
root@radius:/usr/local/etc/raddb/sites-available# nano inner-tunnel &
[2] 2556
[1]+ Detenido nano default
root@radius:/usr/local/etc/raddb/sites-available#


192.168.2.9 - KiTTY
}
Module: Linked to sub-module rlm_eap_mschapv2
Module: Instantiating eap-mschapv2
mschapv2 {
with_ntdomain_hack = no
send_error = no
}
Module: Checking authorize {...} for more modules to load
Module: Linked to module rlm_preprocess
Module: Instantiating module "preprocess" from file /usr/local/etc/raddb/modules/preprocess
preprocess {
huntgroups = "/usr/local/etc/raddb/huntgroups"
hints = "/usr/local/etc/raddb/hints"
with_ascend_hack = no
ascend_channels_per_line = 23
with_ntdomain_hack = no
with_specialix_jetstream_hack = no
with_cisco_vsa_hack = no
with_alvarion_vsa_hack = no
}
Module: Linked to module rlm_realm
Module: Instantiating module "suffix" from file /usr/local/etc/raddb/modules/realm
realm suffix {
format = "suffix"
delimiter = "@"
ignore_default = no
ignore_null = no
}
/usr/local/etc/raddb/modules/ldap[29]: Failed to link to module 'rlm_ldap': rlm_ldap.so: cannot open shared object file: No s
uch file or directory
/usr/local/etc/raddb/sites-enabled/default[188]: Failed to load module "ldap".
/usr/local/etc/raddb/sites-enabled/default[69]: Errors parsing authorize section.
root@radius:/usr/local/etc/raddb/sites-enabled#

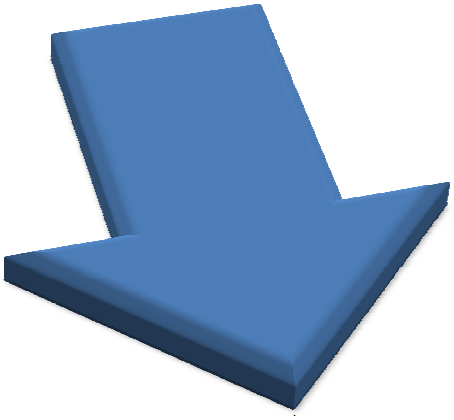


ANEXO E

LISTA DEASIGNNACIÓN DE SERVICIOS DE LA RED CENTRAL G.A.M.C

LISTA DE ASIGNACIÓN DE SERVICIOS DE LA RED PREDIO CENTRAL DEL GAMC

Nº	GRUPO DE TRABAJO	IP	CARGO	USUARIO	ESTADO
			OFICIALIA MAYOR FINANCIERA		
			OFICIAL MAYOR		
1	MAE	192.168.2.xx	ALCALDESA	ANA LUCIA REIS	IMPRESORA
2	OMAF	192.168.2.xxx	OFICAL MAYOR FINANCIERA	RENATO APURI	IMPRESORA
			DIRECTORES		
3	FINANCIERA	192.168.2.22	DIRECTOR FINANCIERO	WILSON VIDAURRE	IMPRESORA
4	ADMINISTRATIVA	192.168.2.58	DIRECTOR ADMINISTRATIVA	VERONICA DOMINGUES	IMPRESORA COMPARTIDA
5	PLANIFICACION	192.168.2.94	DIRECTOR PLANIFICACION	LUIS ALBERTO CORDERO	IMPRESORA
6	JURIDICA	192.168.2.98	DIRECTOR-JURIDICA	TIANA PINHEIRO	IMPRESORA COMPARTIDA
7	TRANSPARENCIA	192.168.2.35	DIRECTOR TRANSPARENCIA	LIBERTAD AGUADA	SERVICIO DE IMPRESORA
			JEFES		
8	FINANCIERA	192.168.2.26	JEFE PRESUPUESTO	SANABRIA	IMPRESORA COMPARTIDA
9	SEGUIMIENTO FINANC	192.168.2.67	JEFE SEGUIMIENTO FINANCIERO	YONNER REYES	IMPRESORA COMPARTIDA
10	ACTIVOS FIJOS	192.168.2.69	JEFA ACTIVOS FIJOS	AMANDA	IMPRESORA COMPARTIDA
11	SISTEMAS	192.168.2.81	JEFE UNIDAD SISTEMA	SILVIA CARABALLO	SERVICIO DE IMPRESORA
12	RECURSOS HUMANOS	192.168.2.84	JEFE DE RECURSOS HUMANOS	GONZALO JUSTINIANO	IMPRESORA COMPARTIDA
13	BIENES Y SERVICIOS	192.168.2.43	JEFE BIENES Y SERVICIOS	INES APAZA	IMPRESORA COMPARTIDA
14	FINANCIERA	192.168.2.27	JEFE PRESUPUESTO	ABIGAIL AYUVIRI	IMPRESORA COMPARTIDA
15	PLANIFICACION	192.168.2.93	JEFE DESARROLLO ORGANIZACIONAL	ERWIN MACUAPA	IMPRESORA COMPARTIDA
			SECRETARIAS/AUXILIARES		
16	BIENES Y SERVICIOS	192.168.2.46	SECRETARIA BIENES Y SERVICIOS	DANIELA	IMPRESORA COMPARTIDA
17	FINANCIERA	192.168.2.21	SECRETARIA FINANCIERA	KATIANA FLORES	IMPRESORA COMPARTIDA
18	ADMINISTRATIVA	192.168.2.59	SECRETARIA ADMINISTRATIVA	VIRGINIA CHIGUANTO	IMPRESORA COMPARTIDA
19	RECURSOS HUMANOS	192.168.2.86	SECRETARIA RECURSOS HUMANOS	NATALY	IMPRESORA COMPARTIDA
20	OMAF	192.168.2.109	SECRETARIA OMAF	LETICIA	IMPRESORA
21	PLANIFICACION	192.168.2.113	SECTRARIA PLA IFICACION	DIOLY	SERVICIO DE IMPRESORA
22	DESPACHO	192.168.2.105	SECRETARIA DESPACHO	FATIMA CAMPOS	IMPRESORA
23	BIENES Y SERVICIOS	192.168.2.44	AUXILIAR BYS	ARIEL JUSTINIANO	IMPRESORA COMPARTIDA
24	FINANCIERA	192.168.2.24	AUXILIAR CONTABLE	XENIA ZABALA	IMPRESORA COMPARTIDA
25	BIENES Y SERVICIOS	192.168.2.68	AUXILIAR	FABIOLA	IMPRESORA COMPARTIDA
26	BIENES Y SERVICIOS	192.168.2.72	AUXILIAR	GROVER	IMPRESORA COMPARTIDA
27	ACTIVOS FIJOS	192.168.2.74	AUXILIAE ACTIVO FIJOS	CRISTINA RIBEIRO	SERVICIO DE IMPRESORA
28	ACTIVOS FIJOS	192.168.2.75	AUXILIAR	YOVANA	NO AUTORIZADA
29	ACTIVOS FIJOS	192.168.2.76	AUXILIAR ACTFIJOS	IVAN ROJAS	IMPRESORA COMPARTIDA
30	SEGUIMIENTO FINANC	192.168.2.18	AUXILIAR SEGUIMIENTO	CASUMI NAKASHIMA	IMPRESORA COMPARTIDA
31	FINANCIERA	192.168.2.95	AUXILIAR	PEDRO	NO AUTORIZADA
32	JURIDICA	192.168.2.104	AUXILIAR	EDWIN	NO AUTORIZADA
			TÉCNICOS ADMINISTRADORES		
33	SEGUIMIENTO FINANC	192.168.2.33	ASESOR LEGAL DE INFORME	YOVANA	IMPRESORA COMPARTIDA
34	FINANCIERA	192.168.2.16	CAJERA GENERAL	AIDE SUAREZ	NO AUTORIZADA
35	FINANCIERA	192.168.2.17	TECNICO FINANCIERO	JHONNY	NO AUTORIZADA
36	FINANCIERA	192.168.2.19	TECNICO SISTEMAS	DUGLAS ANTEQUEIRA	SERVICIO DE IMPRESORA
37	FINANCIERA	192.168.2.20	ENCARGADI DESCARGO	LILIANA A	IMPRESORA COMPARTIDA
38	FINANCIERA	192.168.2.23	ENCARAGADO TESORO Y CP	PAULA	IMPRESORA
39	FINANCIERA	192.168.2.25	CONTADOR	MILTON SORIA	IMPRESORA COMPARTIDA
40	FINANCIERA	192.168.2.28	SERVIDOR SINCON	DIRECCION FINANCIERA	TECNICO SISTEMAS
41	TRANSPARENCIA	192.168.2.34	DESCARGO	MEDARDO	IMPRESORA COMPARTIDA
42	VENTANILLA UNICA	192.168.2.40	VENTANILLA UNICA	SANDRA	IMPRESORA
43	BIENES Y SERVICIOS	192.168.2.45	COTIZADOR	GABRIELA/YULI	IMPRESORA COMPARTIDA
44	BIENES Y SERVICIOS	192.168.2.47	COTIZADOR COMPRAS MEN	LEO	SERVICIO DE IMPRESORA
45	BIENES Y SERVICIOS	192.168.2.48	ENCARGADO DE ARCHIVOS BIENES Y SER	ENRIQUE	SERVICIO DE IMPRESORA
46	BIENES Y SERVICIOS	192.168.2.49	COTIZADOR	DANIELA	IMPRESORA COMPARTIDA
47	BIENES Y SERVICIOS	192.168.2.60	ENCARGADO PAGO SERVICIOS BASICOS	FREDDY	IMPRESORA COMPARTIDA
48	BIENES Y SERVICIOS	192.168.2.64	ENCARGADA DE SICOES	LISETH BENITEZ	SERVICIO DE IMPRESORA
49	SEGUIMIENTO FINANC	192.168.2.66	RESP.SEGUIMIENTO DE ARCHIVOS	TANIA	NO AUTORIZADA
50	SISTEMAS	192.168.2.70	REPONSABLE SISTEMA	ROLANDO CHIPANA	IMPRESORA COMPARTIDA
51	SISTEMAS	192.168.2.77	RESP.REDES E INTERNET	RENELSY ROJAS	IMPRESORA COMPARTIDA
52	SISTEMAS	192.168.2.78	DESARROLLADOR SISTEMAS	JORGE CHIPANA-YOR	AUTORIZADO SISTEMA INFROM
53	SISTEMAS	192.168.2.80	RESP-HARDWARE SOFTWARE	EDGAR EDWIN NINA CHURA	IMPRESORA COMPARTIDA
54	RECURSOS HUMANOS	192.168.2.82	ENCARGADA DE PROCESOS	FIRUTTE SADAFI	IMPRESORA COMPARTIDA
55	RECURSOS HUMANOS	192.168.2.83	ENCARGADA DE ARCHIVOS RECURSOS HU	NOEMI	SERVICIO DE IMPRESORA
56	RECURSOS HUMANOS	192.168.2.85	ENC.PLANILLAS	FERNANDO PELAES	IMPRESORA
57	RECURSOS HUMANOS	192.168.2.87	ASESOR JURIDICO	MILENKA	IMPRESORA COMPARTIDA
58	RECURSOS HUMANOS	192.168.2.88	RESPONSABLE MANEJO FILE	DEILY	IMPRESORA COMPARTIDA
59	PLANIFICACION	192.168.2.90	TECNICO PLANIFICADOR	ROY ROJAS	IMPRESORA COMPARTIDA
60	PLANIFICACION	192.168.2.91	POA-PLANIFICADOR	CLAVEL	IMPRESORA COMPARTIDA
61	PLANIFICACION	192.168.2.92	RESPONSABLE SISIM	ARISTOFANIS COCA	IMPRESORA
62	JURIDICA	192.168.2.100	ASESOR JURIDICO	JACINTO CONDORI TORRES	IMPRESORA
63	JURIDICA	192.168.2.101	ASESOR JURIDICO	ALEXANDER CASTEDO	IMPRESORA COMPARTIDA
64	JURIDICA	192.168.2.102	ASESOR JURIDICO	DINA VACA CARAICA	IMPRESORA COMPARTIDA
65	JURIDICA	192.168.2.103	ASESOR JURIDICO	VICTOR RENGEL AREVALO	IMPRESORA COMPARTIDA
66	DESPACHO	192.168.2.105	RELACIONES PUBLICAS	BRENDA	IMPRESORA COMPARTIDA
67	DESPACHO	192.168.2.107	ASISTENTE DESPACHO	JUAN CARLOS	IMPRESORA COMPARTIDA
68	OMAF	192.168.2.111	ASISTENTE OMAF	ADOLFO	IMPRESORA COMPARTIDA
69	DESPACHO	192.168.2.118	JUEZ SUMARIANTE	CICERO	IMPRESORA COMPARTIDA



ANEXO F

PROPUESTA DE POLITICA DE SEGURIDAD PARA EL ACCESO A LOS RECUROS DE LA RED LAN DEL GOBIERNO AUTONOMO MUNICIPAL DE COBIJA

PROPUESTA DE POLITICA DE SEGURIDAD PARA EL ACCESO A LOS RECURSOS DE LA RED LAN DEL GOBIERNO AUTONOMO MUNICIPAL DE COBIJA

Introducción:

Las siguientes políticas servirán como referencia, y en ningún momento pretenden constituirse como normas absolutas. Todos aquellos actos que se consideren como violaciones a las normativas vigentes en este documento, están prohibidas.

Al utilizar la red LAN del Gobierno Autónomo Municipal de Cobija GAMC, se espera que el usuario (Personal que desarrolla actividades en el predio central del GAMC conectada a la red) use los recursos con respeto, cortesía y responsabilidad, en procura de no vulnerar los derechos de los demás usuarios de la red.

Las autoridades administrativas del GAMC y en particular la unidad de sistemas, se comprometen a publicar y difundir estas políticas de uso para los usuarios de los recursos provistos a través de la red.

Los casos no provistos por el presente reglamento serán resueltos por la unidad de sistemas, si la situación lo amerita, procederán en conjunto con las autoridades competentes del GAMC.

PROPOSITO:
El propósito de este documento es definir la política administrativa y proveer una guía respecto al uso responsable de los ordenadores, servidores y redes que permiten de forma eficiente el acceso y distribución de información.

Además, ya que estas tecnologías nos permiten la posibilidad de acceder, copiar y compartir información con fuentes remotas, nuestros usuarios deben ser conscientes de los derechos de los otros, tales como su privacidad. Finalmente también se hará una enumeración de las responsabilidades que supone el uso de estos recursos y las consecuencias de su abuso

Definiciones de Términos:

1. **Red LAN del GAMC**: Es el nombre dado al conjunto de instalaciones y recursos informáticos del Gobierno Autónomo Municipal de Cobija, que hacen parte de la infraestructura de telecomunicaciones y los recursos que se encuentren bajo la supervisión del mismo.

2. **Usuario:** Se entiende por usuario de la red, todo ente que reciba o provea información a través de la red GAMC; caben bajo esta denominación las personas que tengan algunas vinculación laboral con el Gobierno Municipal de Cobija y cumplan con los requerimientos de acceso a la red. Las presentes políticas serán aplicadas a todos los usuarios.
   La Unidad de Sistemas divide en dos tipos de usuarios:

USUARIOS CON PRIVILEGIOS: Alcaldesa, Asambleístas, Oficialía Mayor, Directores y Jefes.
USUARIOS SIN PRIVILEGIOS: Secretarias, personal auxiliar y técnicos.

3. **Recurso:** Se entiende por recurso, al conjunto de hardware y software que apoyan la labor de gestión administrativa de los usuarios que requieran y/o proveen información a través de la Red.

Personal Autorizado:

Están autorizados a utilizar los recursos de la Red, todo el personal administrativo del GAMC.

I.- Control de acceso a la Red

Objetivos:

a) Impedir el acceso no autorizado a los sistemas de información y recursos.
b) Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
c) Controlar la seguridad en la conexión en la red.
d) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
e) Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
f) Garantizar la seguridad de la información cuando se utiliza instalaciones de trabajo remoto.

1. **Administración de Accesos de Usuarios**

Con el objetivo de impedir el acceso no autorizado a los recursos y a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y recursos.

1.1. Registración de Usuarios

El Responsable de la red de datos definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a los sistemas y recursos.

1.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido.

2. **Administración de Contraseñas de Usuario**

La asignación de contraseñas se controlará a través de un proceso de administración por parte del responsable de redes.

3. **Administración de Contraseñas Críticas**

Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser habilitación de servicios, actualización de software, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

El Responsable de redes definirá procedimientos para la administración de dichas contraseñas críticas.

4. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y recursos de la red, el propietario de la Información de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

5. Responsabilidades del Usuario

5.1. **Uso de Contraseñas**

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.
Los usuarios deben cumplir las directivas que se impartan a tal efecto.

5.2. **Equipos Desatendidos en Áreas de Usuarios**

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
El Responsable de la red de datos debe coordinar con la unidad de Recursos Humanos las tareas de concientización a todos los usuarios, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

6. Política de utilización de los Recursos de la Red

Se controlará el acceso a los recursos de red tanto internos como externos. El Responsable de la Red e Internet tendrá a cargo el otorgamiento del acceso a los recursos de red, únicamente de acuerdo al pedido formal del titular de cada dirección o jefatura que lo solicite para personal de su competencia

7. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de redes de datos definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

8. Control de Acceso a las Aplicaciones

8.1. Restricción del Acceso a la Información

Solo tendrán acceso a la información y a las funciones de los sistemas de aplicación el responsable de sistema de conformidad con la política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación.

8.2. Aislamiento de los Servidores de Sistemas de información

Los Servidores deben de estar en un ambiente informático dedicado (aislado).

Debe ejecutarse en una equipo dedicado, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones.

9. Monitoreo del Acceso y Uso de los Sistemas de información

9.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

9.2. Monitoreo del Uso de los Sistemas de información

9.3. Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas

II. Derechos y responsabilidades de los usuarios de la Red

Derechos:

- Los usuarios dispondrán de pleno acceso a los recursos de la red y de los recursos previa autentificación y de acuerdo a lo consignado en el presente documento y en las normativas asociadas.

- Los usuarios gozan de la privacidad del servicio y su información, salvo de aquellas acciones que pongan en riesgo la seguridad de la Red y el correcto funcionamiento de los sistemas y recursos que en ella se encuentran.

Los usuarios podrán acceder a todas las prestaciones de la red incluyendo los servicios de Internet.

Responsabilidades:

- El usuario es responsable sobre el buen uso de su password de acceso y los procesos que desarrolle en la red.

- El usuario debe de someterse las disposiciones dictadas en las políticas de seguridad y uso de la red.
- Cualquier cambio en el hardware de la estación de trabajo o extensión deberá ser notificado a la Unidad de Sistemas del GAMC.

III. De las restricciones de uso

Dadas las limitantes existentes en los recursos informáticos disponibles en el Gobierno Autónomo Municipal de Cobija, se formulan las siguientes restricciones que ayudara al control de acceso y uso a los recursos de la red sin perjudicar las prestaciones existentes y asegurando su calidad.

Restricciones asociados al acceso a los recursos

- Se habilitara un identificador y clave de acceso a cada uno de los usuarios del predio central del GAMC, para optimizar el flujo de información, uso adecuado de los recursos, y acceso a internet.

- La autentificación, el acceso a la red y sus recursos no tendrá ningún costo para la comunicación interna y los usuarios registrado en el servidor de autentificación.

- La reubicación o cambio de extensión dentro de la red, cambio de parámetros en la configuraciones de equipos y el servidor de autenticación, la instalación y modificación de la redes, es de competencia y responsabilidad exclusiva del personal del de la ºUnidad de Sistemas del GAMC.

IV. De las sanciones.

El incumplimiento a cualquiera de las políticas establecidas en el presente documento acarreara las sanciones:

Primera llamada de atención verbal previo conocimiento del encargado de RR.HH del GAMC sobre la falta a la presente política.

Última llamada de atención formal y suspensión del servicio de acuerdo al marco legal de la institución.