UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

INGENIERÍA EN SISTEMAS

TEMA:

"DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACION EN EL AREA DE ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, UTILIZANDO HERRAMIENTAS OPEN SOURCE."

Tesis previa a la obtención del Título de Ingeniero en Sistema

AUTORES:

GILVER STALIN AGUILAR PUCHAICELA

JANNETH ELIZABETH MONCAYO ROMERO

DIRECTOR:

ING. HERNAN LEONARDO TORRES CARRION

LOJA – ECUADOR

2010

1. RESUMEN

La seguridad informática requiere no solo de recursos tecnológicos, sino también de procesos y recursos humanos capacitados y especializados, esta meta es difícil de alcanzar pues existe un constante cambio, ya que día a día se descubren nuevas vulnerabilidades, nuevos tipos de ataques y nuevos parches que aplicar a los sistemas institucionales, convirtiendo la operación de la seguridad en una tarea sumamente compleja y demandante.

El presente documento es sobre el desarrollo del esquema de seguridad informática en la Intranet Universitaria, considerando las amenazas de seguridad desde perspectivas diferentes para permitir de esta forma conocer algunos riesgos que pueden afectar a la institución, así como determinar el nivel de madurez de la seguridad informática con relación a los estándares, además se presentan una serie de lineamientos que la Universidad Nacional de Loja tiene que seguir para la adecuada implementación del plan táctico que se propone en la presente investigación.

2. SUMARY

The computer security not requires alone of technological resources, but also of processes and qualified human resources and specialized, this goal is difficult to reach a constant change then it exists, since day by day they are discovered new vulnerabilities, new types of attacks and new patches that to apply to the institutional systems, transforming the operation of the security into an extremely complex task and plaintiff.

The present document is on the development of the outline of computer security in the University Intranet, considering the threats of security from different perspectives to allow this way to know some risks that can affect to the institution, as well as to determine the level of maturity of the computer security with relationship to the standards, they are also presented a series of limits that the National University of Loja has to continue for the appropriate implementation of the tactical plan that intends in the present investigation.

3. INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

4. INTRODUCCION

Desde la creación de la Universidad Nacional de Loja, juega un papel importante en la sociedad y ha tenido una participación activa en los campos científico, técnico, y cultural de la Región Sur del país. A pesar de sus limitaciones presupuestarias tiene muchos logros a su haber. Ha dado certeros pasos en el cumplimiento de su misión.

El modelo pedagógico implementado en la Universidad Nacional de Loja, denominado Sistema Académico Modular por Objetos de Transformación (SAMOT), se ha convertido en un eje importante de generación de conocimientos para el estudiantado universitario, puesto que impulsa la investigación en los alumnos desde los primeros módulos de enseñanza, involucrándolos en la problemática social con el objetivo de generar medios de solución.

Las instituciones de educación superior (IES) han incorporado a su infraestructura de trabajo nuevas tecnologías que representan un incremento en la importancia de la seguridad en su Intranet. El surgimiento de las aplicaciones bajo una plataforma Web y la automatización de los sistemas administrativos, son algunos indicios que indican la importancia de mantener la integridad de la información y de los servicios que ofrece.

La seguridad informática, protege la información de una gran gama de amenazas con la finalidad de asegurar la continuidad del servicio, minimizar los daños y maximizar el retorno de inversión. La información, los cambios tecnológicos y la utilización de un estándar de seguridad, son puntos clave para el establecimiento de un plan táctico de seguridad que involucre proyectos a corto, mediano y largo plazo, que tomen en cuenta estos factores críticos de la Intranet universitaria.

A medida de la evolución de la tecnología se han propuesto varias recomendaciones para dotar de un nivel de seguridad adecuado, actualmente se están desarrollando propuestas más concretas de mecanismos que permiten mejorar este nivel. Entre las soluciones de seguridad más eficientes para el control de acceso a los recursos y la protección de la información en la Intranet, se describe una de las más eficientes, la cual

se basa en el uso de autenticación, autorización para el acceso a la red y en el uso de encriptación en las comunicaciones sobre este tipo de redes.

El Área de Energía, Industrias y Recursos Naturales No Renovable con el fin de suplir estas necesidades ha implementado backbone en su Intranet, permitiendo de esta forma que la mayoría del personal tenga acceso a los diversos servicios y facilidades que soporta la red de datos.

La presente investigación denominada *"*DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACION EN EL AREA DE ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, UTILIZANDO HERRAMIENTAS OPEN SOURCE*",* Tiene como objetivo Diseñar el esquema de seguridad para la intranet de la Universidad Nacional de Loja e implementarlo en el Área de Energía, las Industrias y los Recursos Naturales no Renovables, que contemple Sistemas AAA (Autenticación, Autorización y Administración).

El desarrollo de la investigación se ha estructurado de la siguiente manera:

En una primera parte realizamos la descripción de la metodología utilizada en el desarrollo de las tareas planificadas en el proyecto inicial, así como anotamos los métodos e instrumentos que fueron de gran importancia para el desarrollo de la investigación.

Para llegar a una comprensión mayor del problema a solucionar con la presente investigación, se ha construido un sustento teórico, que aborda los siguientes puntos: Inicialmente se explica los conceptos y características principales de Redes tanto alámbricas como inalámbricas, se analizan las diferentes topologías de las redes LAN alámbricas e inalámbricas. Además se realiza una explicación de la seguridad en las redes en especial sobre la Identificación, Autorización, Autenticación. También, se detallan los principales aspectos de lo que se refiere a políticas de seguridad, para poder brindar una mayor información. Igualmente para su funcionamiento se requiere la

utilización de algunos protocolos de redes para lo cual se realiza una explicación de características, ventajas y desventajas de los principales protocolos que se utilizan en la seguridad de redes Alambricas e Inalámbricas. Así mismo se realiza comparativa entre ellos, que permiten tener una idea clara de su funcionamiento. También, se detalla la instalación y configuración del servidor freeradius, ldap. Se describe los requerimientos de software y hardware que se utiliza en el proceso de implementación del servidor, así como las políticas de seguridad a ser implementadas.

5. METODOLOGIA

En la presente sección se describe la aplicación de las metodologías planteadas en el anteproyecto. La metodología nos da una visión de cómo se ha desarrollado el proceso investigativo.

Nuestra investigación estuvo planificada mediante tareas que nos han permitido encontrar los mecanismos correctos para llegar a cumplir los objetivos.

Las tareas, métodos, instrumentos que se utilizó para el desarrollo del proyecto investigativo son:

Tabla 5.1 Métodos e instrumentos utilizados

TAREA REALIZADA	METODOLOGÍA
Investigación bibliográfica en libros sobre seguridad en redes de datos. Investigación sobre software que contenga sistemas AAA Investigación sobre FREERADIUS Investigación acerca de la arquitectura de FREERADIUS Entrevistas con personas relacionadas al campo de Redes. Investigar sobre configuración de archivos 3Com Analizar la información recogida.	El método sintético (Consiste en la reunión racional de varios elementos dispersos en una nueva totalidad donde El investigador sintetiza las superaciones en la imaginación para establecer una explicación tentativa que se someterá a prueba). Este método nos permitió en primera instancia buscar en bibliografía especializada (libros, Internet), y en entrevistas con personas relacionadas y así acumular gran cantidad de información. Pero no toda la información recolectada puede ser utilizada debido a que no es verídica o porque está fuera del ámbito de la investigación planteada. Es así que se realizó un análisis de la documentación para poder tener como resultado datos verídicos que nos permitieron conocer como es el funcionamiento real de mecanismos de

	seguridad en redes. Métodos e instrumentos utilizados en estas tareas: *Observación Directa.*- Es aquella en la cual el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar *Observación Indirecta.*- Cuando el investigador entra en el conocimiento del hecho o fenómeno observado a través de las observaciones realizadas anteriormente por otra persona. *Entrevista.*- Consiste en el diálogo entre dos personas: el entrevistador (el investigador) y el entrevistado; se realiza con el fin de obtener información por parte de una persona entendida en la materia de la investigación. *Mapa Conceptual.*- Esquema gráfico que refleja un conjunto de conceptos sobre una temática específica y las relaciones que existen entre ellos. *Lectura comprensiva.*- Tiene por objeto el conocimiento ordenado y sistemático de un aspecto de la realidad o de los acontecimientos, hechos o ideas relacionadas con un tema específico.
Investigar cómo se encuentra distribuida la red de datos de la Universidad Nacional de Loja. Análisis de la tecnología existente (hardware, software). Análisis de los esquemas de red	Para tener una idea clara de cómo se encuentra distribuida la red de la Universidad y su situación actual, utilizamos método descriptivo que consiste en la recolección de datos directamente por los investigadores con el adicional de interpretar los mismos de una

(alámbrica, e inalámbrica) actuales. Análisis de los esquemas de seguridad existentes. Definir las falencias del sistema actual y sus proyecciones de uso y crecimiento.	manera racional. Este método nos permitió describir la red de datos de las Área Académicas - Administrativas y Departamentos de la Universidad y realizar un análisis de la situación actual, además detallamos los equipos principales con los que cuenta la Universidad para brindar los diferentes servicios que brinda a los usuarios de la red. Métodos e instrumentos utilizados en estas tareas: Observación Directa Observación Indirecta Entrevistas Encuestas
Obtener requerimientos funcionales y requerimientos de seguridad. Análisis de los requerimientos obtenidos. Establecer políticas de seguridad necesarias para acceder a cada recurso.	Mapa conceptual o Mapa de conceptos, tipo de esquema gráfico que refleja un conjunto de conceptos sobre una temática específica y las relaciones que existen entre ellos. Su finalidad es sintetizar o resumir de forma gráfica lo más significativo de un tema determinado que se refleja en un texto. Los mapas de conceptos son muy empleados en las disciplinas sociales. Es una técnica muy útil para hacer evidentes los conceptos clave, para separar la información significativa de la trivial y para establecer conexiones entre conocimientos.
Obtener el software requerido para instalar FREERADIUS. Investigación sobre configuración de archivos para FREERADIUS Instalación del software requerido	El método científico experimental (la aplicación más completa de la investigación científica porque permite establecer con toda claridad el principio de relación causa – efecto. Consiste en provocar voluntariamente una

para FREERADIUS Pruebas del servicio	situación que se quiere estudiar) nos ha permitido desarrollar algunas tareas planificadas. Este método nos permitirá a través de software y hardware vinculado a seguridad en redes realizar pruebas que nos llevan a definir con exactitud los mecanismos con los cuales lograremos la configuración final de: Servidor RADIUS. Seguridad en redes inalámbricas. Seguridad en redes alámbricas. Métodos e instrumentos utilizados en estas tareas: Observación Directa Observación Indirecta

6. FUNDAMENTACION TEORICA

CAPÍTULO I

1. DESCRIPCIÓN GENERAL SOBRE LAS REDES ALÁMBRICAS E INALÁMBRICAS

1.1. INTRODUCCIÓN A LAS REDES

Las redes en general, consisten en "compartir recursos" y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Las computadoras pequeños tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos computadoras personales, uno por usuario, con los datos guardados una o más máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo

extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo más procesadores. Con máquinas grandes, cuando el sistema está lleno, deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí. Con el ejemplo de una red es relativamente fácil para dos o más personas que viven en lugares separados, escribir informes juntos. Cuando un autor hace un cambio inmediato, en lugar de esperar varios días para recibirlos por carta.

Trabajando en el mismo programa. Después vienen los multiprocesadores, que son sistemas que se comunican a través de memoria compartida. En seguida de los multiprocesadores se muestran verdaderas redes, que son computadoras que se comunican por medio del intercambio de mensajes.

1.2. HISTORIA DE LAS REDES

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras (computadores), así como a la puesta en órbita de los satélites de comunicación.[1]

[1] http://usuarios.multimania.es/aledomiisa/historia.php

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de computadoras ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de computadoras separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computadoras. Estas nos dan a entender una colección interconectada de computadoras autónomas. Se dice que las computadoras están interconectadas, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que las computadoras son autónomas, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

1.3. USOS DE LAS REDES

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN (ya establecida) si genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad. Para dar una idea sobre algunos de los usos importantes de redes de computadoras, veremos ahora brevemente tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido.[2]

[2] http://pantuflo.gsyc.es/~jvergara/memoria/node14.html

Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver cómo pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente ó necesita de una máquina muy grande para correrlo.

Todas estas aplicaciones operan sobre redes por razones económicas: el llamar a un ordenador remoto mediante una red resulta más económico que hacerlo directamente. La posibilidad de tener un precio más bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuando se están transmitiendo los datos.

Una tercera forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (INTERNET). Como por ejemplo, el tan conocido por todos, correo electrónico (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.

1.4. LAS REDES Y LOS SISTEMAS DISTRIBUIDOS[3]

Las primeras redes de computadoras fueron diseñadas para satisfacer los requisitos de aplicación del tipo transferencia de archivos, conexión a sistemas remotos, correo electrónico y servicios de noticias, como se menciono anteriormente.

Con el crecimiento y comercialización de Internet se han impuestos requisitos más exigentes en cuanto a:

- PRESTACIONES: Los parámetros indicadores de las prestaciones son aquellos que afectan a la velocidad con la que los mensajes individuales pueden ser transferidos entre dos computadores interconectados. Estos son:

[3] http://www.monografias.com/trabajos16/sistemas-distribuidos/sistemas-distribuidos.shtml

- La Latencia: Es el intervalo de tiempo que ocurre entre la ejecución de la operación de envío y en instante en que los datos comienzan a estar disponibles en el destino.
- La Taza de Transferencia de Datos: Es la velocidad a la cual se pueden transferir datos entre dos computadoras conectadas a la red. La transmisión, una vez ya inicializada es medida en bits por segundos.

El tiempo requerido por una red para la transmisión de un mensaje de 1 bits de longitud entre dos computadores es:

Tiempo de transmisión del mensaje = Latencia + Longitud/Tasa de transferencia

Esta ecuación es válida para mensajes cuya longitud no supere un máximo que viene determinado por la tecnología de la red subyacente. Para mensajes más largos se los segmenta y el tiempo de transmisión es igual a la suma del tiempo de transmisión de cada segmento.

La tasa de transferencia de una red está determinada por sus características físicas y la latencia estará determinada por las sobrecargas del software, los retrasos en el encaminamiento y una componente estadística derivada de los conflictos en el uso de los canales de transmisión.

El ancho de banda total del sistema de una red es una medida de la productividad (throughput), del volumen de tráfico que puede ser transferido a través de la red en un intervalo de tiempo dado. En muchas tecnologías de red local, se utiliza toda la capacidad de transmisión de la red en cada transmisión y el ancho de banda es igual a la tasa de transferencia. Sin embargo, en la mayoría de las redes de área extensa los mensajes pueden ser transferidos simultáneamente sobre varios canales diferentes de modo que el ancho de la banda no guarda relación directa con la tasa de transferencia.

- ESCABILIDAD: Al hablar de la infraestructura de la sociedad debemos pensar en las redes de computadores puesto que estas son una parte de ella. El tamaño futuro de Internet será comparable con la población del planeta. Resulta creíble

esperar que alcance varios de miles de millones de nodos y cientos de millones de hots activos. Las tecnologías de red no están diseñadas para soportar la escala de algunos cambios sustanciales para el direccionamiento y los mecanismos de encaminamiento, con el fin de dar soporte a la siguiente fase de crecimiento de Internet.

- FIABILIDAD: En la mayoría, los medios de transmisión son muy altos. Cuando ocurren errores son normalmente debidos a fallos de sincronización en el software en el emisor o en el receptor, o desbordamientos en el buffer más que fallos en la red.

- SEGURIDAD: La mayoría de las organizaciones protegen sus redes y computadoras a través de cortafuegos (firewall. Este creó un límite de protección entre la red interna de la organización o intranet, y el resto de Internet. Su propósito es proteger los recursos en todos los computadores dentro de la organización del acceso por parte de usuarios o procesos externos, y controlar el uso de recursos del otro lado del cortafuego por parte de los usuarios dentro de la organización.

Un cortafuegos se ejecuta sobre un Gateway o pasarela, un computador que se coloca en el punto de entrada de la red interna de una organización. El cortafuego recibe y filtra todos los mensajes que viajan desde y hacia la organización. Está configurado de acuerdo con políticas de seguridad de la organización para permitir que ciertos mensajes entrantes o salientes pasen a través de él, y para rechazar los demás.

- MOVILIDAD: Los dispositivos móviles se desplazan frecuentemente entre distintos lugares y se adhieren en puntos de conexión variados. Los modos de direccionamiento y encaminamiento de Internet y de otras redes, fueron desarrolladas antes de la llegada de los dispositivos móviles, y aunque los mecanismos actuales han sido adoptados y extendidos para soportar cierta movilidad, el esperado crecimiento del uso de los dispositivos móviles hará necesarias nuevas extensiones.

- MULTIDIFUCIÓN (Multicasting): La comunicación de uno a muchos puede ser simulada enviando mensajes a varios destinos, pero resulta más costoso de lo necesario y no posee las características de tolerancia a fallos requeridos por las aplicaciones.

1.5. TIPOS DE REDES[4]

Los principales tipos de redes para soportar los sistemas distribuidos son:

1.5.1. Redes de área local[5]

Las redes de área local (Local Area Networks) llevan mensajes a velocidades relativamente grande entre computadoras conectadas a un único medio de comunicación: Un cable de par trenzado, un cable coaxial o una fibra óptica, un segmento es una sección de cable que da servicio y que puede tener varios computadoras conectadas, el ancho de banda del mismo se reparte entre dichas computadoras. Las redes de área local mayores están compuestas por varios segmentos interconectados por conmutadores (switch) o concentradores (hubs). El ancho de banda total del sistema es grande y la latencia pequeña, salvo cuando el tráfico es muy alto.

En los años 70s se han desarrollado varias tecnologías de redes de área local, destacándose Ethernet como tecnología dominante para las redes de área amplia; estando esta carente de garantías necesarias sobre latencia y ancho de banda necesario para la aplicación multimedia. Como consecuencia de esta surge ATM para cubrir estas falencias impidiendo su costo su implementación en redes de área local. Entonces en su lugar se implementan las redes Ethernet de alta velocidad que resuelven estas limitaciones, no superando la eficiencia de ATM.

1.5.1.1. Características Importantes

- Tecnología broadcast (difusión) con el medio de transmisión compartido.

[4] http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml
[5] http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km (una FDDI puede llegar a 200 km).
- Uso de un medio de comunicación privado.
- La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
- La facilidad con que se pueden efectuar cambios en el hardware y el software.
- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.
- Limitante de 100 m.

1.5.1.2. Dispositivos de una red LAN

Los dispositivos que se conectan de forma directa a un segmento de red se denominan hosts, estos hosts incluyen computadores, tanto clientes y servidores, impresoras, escáneres y varios otros dispositivos de usuario.

Estos dispositivos suministran a los usuarios conexión a la red, por medio de la cual los usuarios comparten, crean y obtienen información, además pueden existir sin una red, pero sin la red las capacidades de los hosts se ven sumamente limitadas.

Tienen una conexión física con los medios de red ya que tienen una tarjeta de interfaz de red (NIC).

El PC mismo se puede considerar como una red muy pequeña que conecta el bus y las ranuras de expansión con la CPU, la RAM y la ROM.

No existen símbolos estandarizados dentro de la industria de networking para los hosts, pero por lo general son lo bastante obvios como para detectarlos.

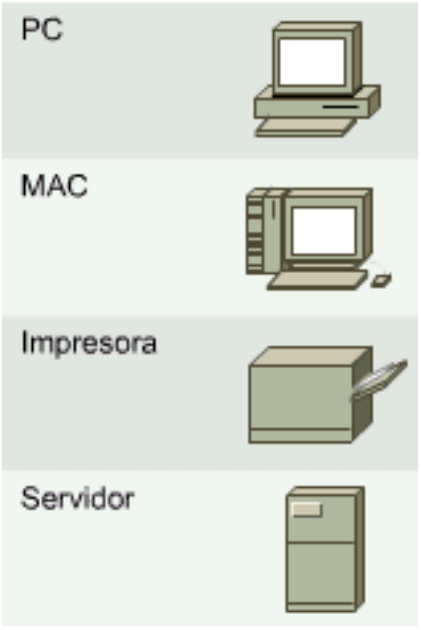


Figura 1.1. Dispositivos de una red LAN

1.5.2. Redes de Área Extensa

Estas pueden llevar mensajes entre nodos que están a menudo en diferentes organizaciones y quizás separadas por grandes distancias, pero a una velocidad menor que las redes LAN. El medio de comunicación está compuesto por un conjunto de círculos de enlazadas mediante computadoras dedicadas, llamados routers o encaminadores. Esto gestiona la red de comunicaciones y encaminan mensajes o paquetes hacia su destino. En la mayoría de las redes se produce un retardo en cada punto de la ruta a causa de las operaciones de encaminamiento, por lo que la latencia total de la transmisión de un mensaje depende de la ruta seguida y de la carga de tráfico en los distintos segmentos que atraviese. La velocidad de las señales electrónicas en la mayoría de los medios es cercana a la velocidad de la luz, y esto impone un límite inferior a la latencia de las transmisiones para las transmisiones de larga distancia.

1.5.3. Redes de Área Metropolitana

Las redes de área metropolitana (metropolitan area networks) se basan en el gran ancho de banda de las cableadas de cobre y fibra óptica recientemente instalados para la transmisión de videos, voz, y otro tipo de datos. Varias han sido las tecnologías

utilizadas para implementar el encaminamiento en las redes LAN, desde Ethernet hasta ATM. Las conexiones de línea de suscripción digital, DLS (digital subscribe line) y los MODEM de cable son un ejemplo de esto. DSL utiliza generalmente conmutadores digitales sobre par trenzado a velocidades entre 0.25 y 6.0 Mbps; la utilización de este par trenzado para las conexiones limita la distancia al conmutador a 1.5 kilómetros. Una conexión de MODEM por cable utiliza una señalización análoga sobre el cable coaxial de televisión para conseguir velocidades de 1.5 Mbps con un alcance superior que DSL.

1.5.4. Redes Inalámbricas[6]

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable. Con estas redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar portacables o conectores.

Por el otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los

[6] http://es.kioskea.net/contents/wireless/wlintro.php3

rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un hacker puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

1.5.4.1. Categorías de redes inalámbricas

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (denominada *área de cobertura*):

Figura 1.2. Categorías de redes inalámbricas

1.5.4.1.1. Redes de área local inalámbricas

WLAN (en inglés; *Wireless Local Area Network*) es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son

muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

Trabajan utilizando ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto.

En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN 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. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado 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. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

Pueden ser de muy diversos tipos y tan simples o complejas como sea necesario. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual (peer to peer). Cada cliente tendría únicamente acceso a los recursos del otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o pre configuración.

1.5.4.1.2. Wireless Personal Area Network

En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth (protocolo que sigue la especificación IEEE 802.15.1); ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo);RFID (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

1.5.4.1.3. Wireless Metropolitan Area Network

Para redes de área metropolitana se encuentran tecnologías basadas en WiMAX (*Worldwide Interoperability for Microwave Access*, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (*Local Multipoint Distribution Service*).

1.5.4.1.4. Wireless Wide Area Network

En estas redes encontramos tecnologías como UMTS (*Universal Mobile Telecommunications System*), utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G), o también la tecnología digital para móviles GPRS (*General Packet Radio Service*).

Así mismo se pueden conectar diferentes localidades utilizando conexiones satelitales o por antenas de radio microondas. Estas redes son mucho más flexibles, económicas y fáciles de instalar.

En sí la forma más común de implantación de una red WAN es por medio de Satélites, los cuales enlazan una o más estaciones bases, para la emisión y recepción, conocidas como estaciones terrestres. Los satélites utilizan una banda de frecuencias para recibir la información, luego amplifican y repiten la señal para enviarla en otra frecuencia.

Para que la comunicación satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35,784 Km.

1.5.4.2.Características de una red Inalámbrica

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos, por ejemplo. Dependiendo del medio, la red inalámbrica tendrá unas características u otras:

Ondas de radio: las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30Hz, hasta la banda UHF que va de los 300 a los 3000 MHz, es decir, comprende el espectro radioeléctrico de 30 - 3000000 Hz.

Microondas terrestres: se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

Microondas por satélite: se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en

una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia se mezclan bastante, así que pueden haber interferencias con las comunicaciones en determinadas frecuencias.

Infrarrojos: se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384THz.

1.5.5. Interredes

Una Interred es un sistema de comunicación compuesto por varias redes que se han enlazado juntas para proporcionar unas posibilidades de comunicación ocultando las tecnologías y los protocolos y métodos de interconexión de las redes individuales que la componen.

Estas son necesarias para el desarrollo de sistemas distribuidos abiertos extensibles. En ellas se puede integrar una gran variedad de tecnología de redes de área local y amplia, para proporcionar la capacidad de trabajo en la red necesaria para cada grupo de usuario. Así, las interredes aportan gran parte de los beneficios de los sistemas abiertos a las comunicaciones de los sistemas distribuidos.

Las interredes se construyen a partir de varias redes. Estas están interconectadas por computadoras dedicadas llamadas routers y computadores de propósito general llamadas gateways, y por un subsistema integrado de comunicaciones producidos por una capa de software que soporta el direccionamiento y la transmisión de datos a las computadoras a través de la interred. Los resultados pueden contemplarse como una red virtual construida a partir de solapar una capa de interred sobre un medio de comunicación que consiste en varias redes, routers y gateways.

1.6. COMPARACIÓN DE REDES[7]

En las redes inalámbricas los paquetes se pierden con frecuencia debido a las interferencias externas, en cambio, en el resto de los tipos de redes la fiabilidad de los mecanismos de transmisión es muy alta. En todos los tipos de redes las pérdidas de paquetes son como consecuencia de los retardos de procesamiento o por los desbordamientos en los destinos.

Los paquetes pueden entregarse en diferente orden al que fueron transmitidos. También se pueden entregar copias duplicadas de paquetes, tanto la retransmisión del paquete como el original llegan a su destino. Todos los fallos descritos son ocultados por TCP y por otros protocolos llamados protocolos fiables, que hacen posible que las aplicaciones supongan que todo lo que es transmitido será recibido por destinatario. Existen, sin embargo, buenas razones para utilizar protocolos menos fiables como UDP en algunos casos de sistemas distribuidos, y en aquellas circunstancias en las que los programas de aplicación puedan tolerar los fallos.

Tabla1.1. Comparación de Redes

Tipo de red	Rango	Ancho de Banda	Latencia (ms)
LAN	1-2 km.	10-1.000	1-10
WAN	Mundial	0.010-600	100-500
MAN	2-50 km	1-150	10
LAN inalámbrica	0,15-1,5 km	2-11	5-20
WAN inalámbrica	mundial	0.010-2	100-500
Internet	mundial	0.010-2	100-500

1.7. INTERCONEXIÓN DE REDES

Para construir una red integrada (una interred) se deben integrar muchas subredes, cada una de las cuales se basa en una tecnología de red. Par hacerlo se necesita:

[7]http://docs.google.com/viewer?a=v&q=cache:E96HRx0OLnAJ:www.redsinfronteras.org/pdf/redes_wireless.pdf+redes+inalambricas&hl=es&gl=ec&pid=bl&srcid=ADGEESiJ9pM757SoSFiGRJtPvVuWL6IOVg421pbx5T5GeVdaTuHJlRFhlrJCZrRJPd-R1BWd9wbHtIrbCsBbJ939AEOA5etqKF60Om5bwNUGARD9jYKSj-DBW5fD_onx_Yz4V26gwkN&sig=AHIEtbRRBNBAzCiyBQXONGzjfTz6vKd0-w

- Un esquema de direccionamiento unificado que posibilite que los paquetes sean dirigidos a cualquier hosts conectado en cualquier subred.
- Un protocolo que defina el formato de paquetes interred y las reglas según las cuales serán gestionados.
- Componentes de interconexión que encaminen paquetes hacia su destino en términos de dirección, transmitiendo los paquetes utilizando subredes con tecnología de red variada.

1.8. COMPONENTES DE UNA RED[8]

- ROUTERS: En una interred los routers pueden enlazarse mediante conexiones directas o pueden estar interconectados a través de subredes. Ellos son los responsables de reenviar paquetes que llegan hacia las conexiones salientes correctas para lo cual se mantienen las tablas de encaminamiento.

- PUENTES (bridges): Enlazan redes de distintos tipos. Algunos puentes comunican varias redes y se llama puente/ruters ya que efectúan funciones de encaminamiento.

- CONCENTRADORES (hubs): Modo para conectar hosts y extender los segmentos de redes locales de difusión. Tienen (entre 4 y 64) conectores a los que conecta hosts. También son utilizados para hacer limitaciones de distancia en un único segmento y proporcionar un modo de añadir hosts adicionales.

- CONMUTADORES (switch): Función similar a un routers, pero restringida a redes locales. La ventaja de estos sobre los concentradores es que pueden separar el tráfico entrante y transmitirlo solo hacia la red de salida relevante, reduciendo la congestión (colisiones: paquetes que chocan) con otras redes a las que estas conectados.

[8] http://www.slideshare.net/whyp/componentes-de-una-red-presentation

- TUNELES: los puentes y routers transmiten paquetes sobre una variedad de redes subyacentes, pero se da una situación en la cual el protocolo de red puede quedar oculto para los protocolos superiores sin tener que utilizar un protocolo especial de interred. Cuando un par de nodos conectados a dos redes separadas necesitan comunicarse a través de algún otro tipo de red o sobre un protocolo extraño, pueden hacerlo construyendo un protocolo enterrado o de túnel (tunnelling). Un protocolo túnel es una capa de software que transmite paquetes a través de un entorno de red extraño.

1.9. TOPOLOGÍAS DE REDES[9]

Las redes de computadoras surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos. Pero los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red. La disposición de los diferentes componentes de una red se conoce con el nombre de topología de la red. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

1.9.1. Aspectos para considerar una topología

- La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.

- La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

[9]http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml

- La topología matemática, mapas de nodos y enlaces, a menudo formando patrones.

- La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

1.9.2. Modelos de topología

1.9.2.1. Topología de bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.

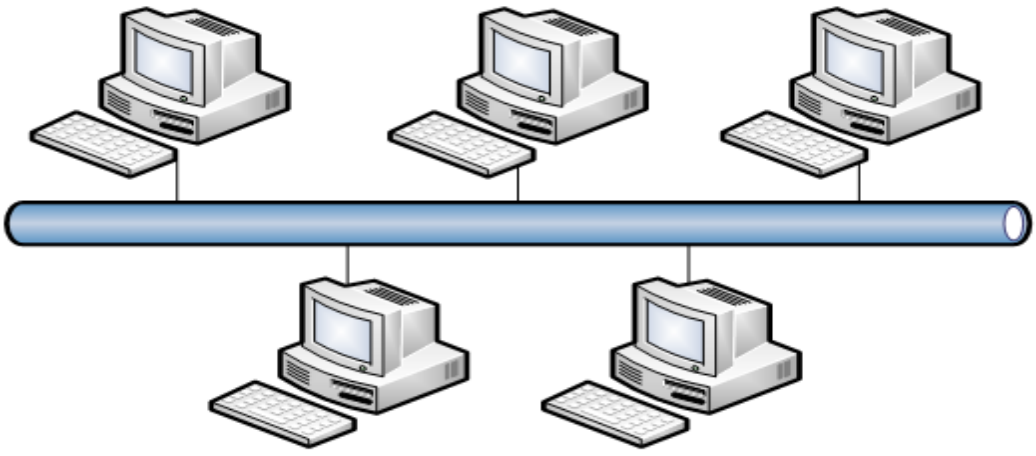


Figura 1.3. Topología de Bus

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

1.9.2.2. Topología de anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

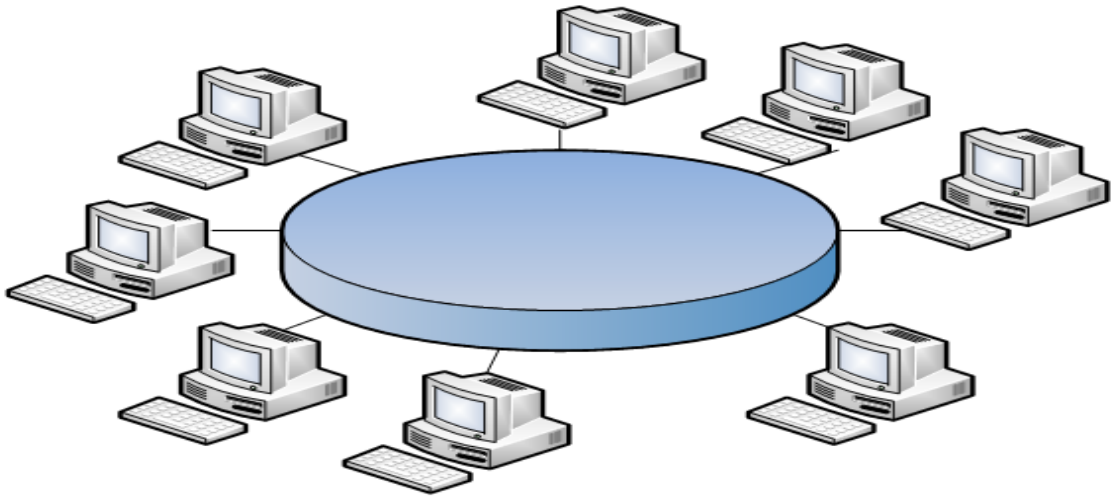


Figura 1.4. Topología de Anillo

Los dispositivos se conectan directamente entre sí. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

1.9.2.3. Topología de anillo doble.

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante

que conecta los mismos dispositivos. La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

1.9.2.4. Topología en estrella.

La topología en estrella tiene un nodo central desde el que se conectan todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red.

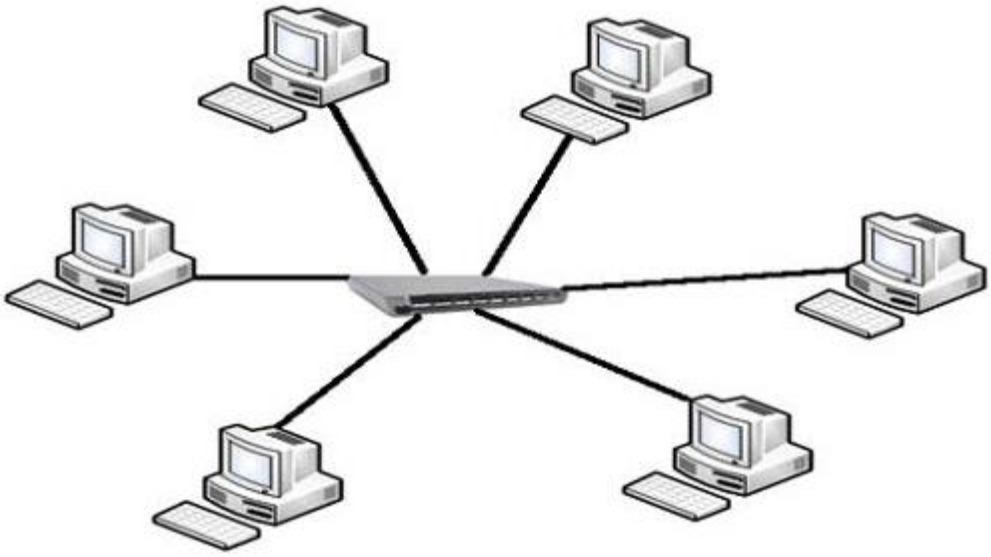


Figura 1.5. Topología en Estrella

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

1.9.2.5. Topología en estrella extendida.

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La

topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

1.9.2.6. Topología en árbol.

La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

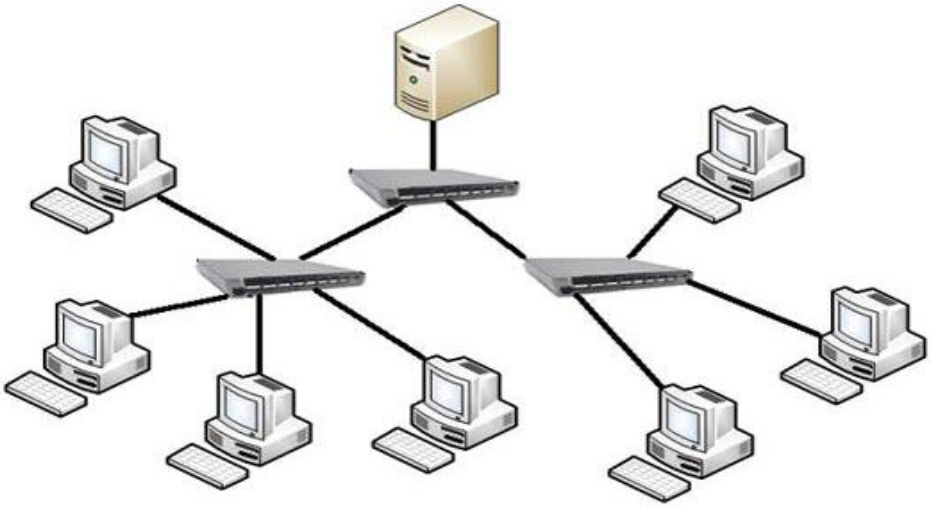


Figura 1.6. Topología en Árbol

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

1.9.2.7. Topología en malla completa.

En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como todos se conectan físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

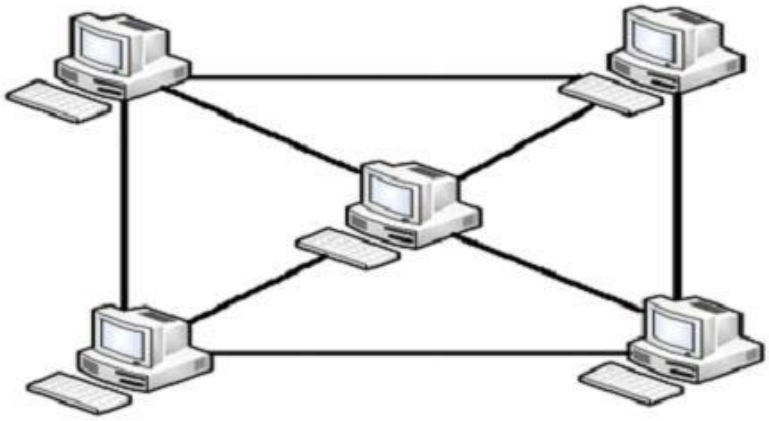


Figura 1.7. Topología en Malla completa

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

1.9.2.8. Topología de red celular.

La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

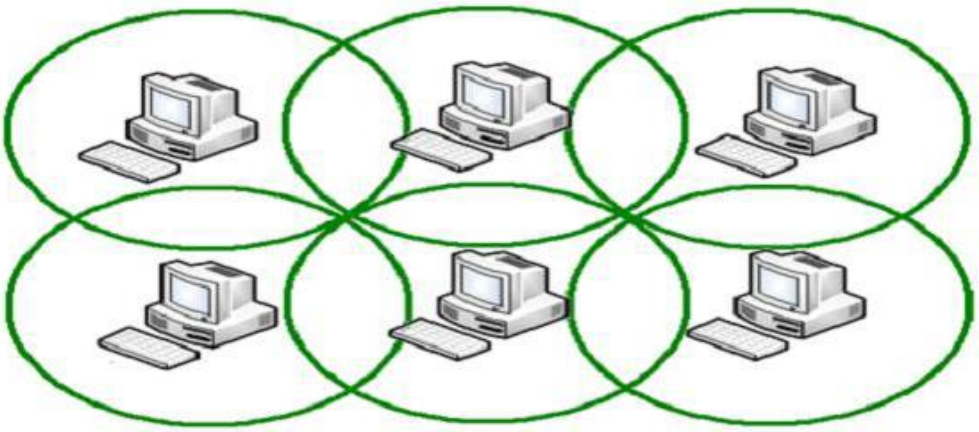


Figura 1.8. Topología de Red Celular

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas. La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en

cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad. Como norma, las topologías basadas en celdas se integran con otras topologías.

1.9.2.9. Topología irregular.

En este tipo de topología no existe un patrón obvio de enlaces y nodos. El cableado no sigue un modelo determinado; de los nodos salen cantidades variables de cables. Las redes que se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas, a menudo se conectan de esta manera. Las topologías LAN más comunes son:

- Ethernet: Topología de bus lógica y en estrella física o en estrella extendida.
- Token Ring: Topología de anillo lógica y una topología física en estrella.
- FDDI: Topología de anillo lógica y topología física de anillo doble.

1.10. REDES INALÁMBRICAS[10]

Espectro electromagnético.- Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar en el espacio libre, aun en el vació.

La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia, f, y se mide en Hz. La distancia entre dos máximos o mínimos consecutivos se llama longitud de onda y se designa con la letra griega λ. Al conectarse una antena apropiada a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio.

En el vació todas las ondas electromagnéticas viajan a la misma velocidad, sin importar su frecuencia. Esta velocidad, usualmente llamada velocidad de la luz, c, es aproximadamente 3x108 m/seg.

[10] http://www.redsinfronteras.org/pdf/redes_wireless.pdf

La figura 1.9 nos muestra el espectro electromagnético. Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas.

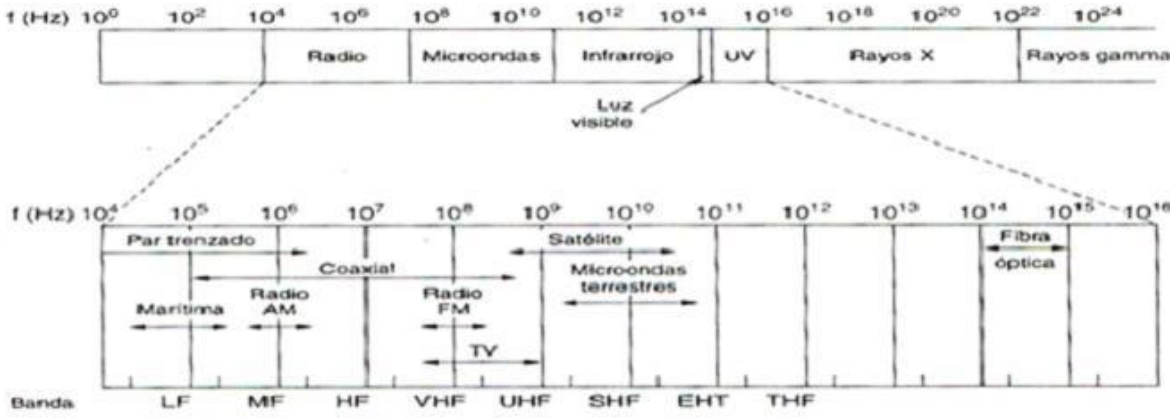


Figura 1.9. Espectro Electromagnético

- Radio Transmisión.- Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto de interiores como de exteriores. Las ondas de radio también son omnidireccionales, ó sea viajan en todas las direcciones desde la fuente, por lo cual el transmisor y el receptor no tienen que alinearse. Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia. Todas las ondas de radio están sujetas a interferencia por los motores y equipos eléctricos.

  Debido a la capacidad de viajar distancias largas y la interferencia entre usuarios, los gobiernos legislan el uso de radiotransmisores. Transmisión por microondas.- Por encima de los 100MHZ las ondas viajan en línea recta y, por tanto se pueden enfocar en un haz estrecho. Concentrar toda la energía en haz pequeño con una antena parabólica produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora se deben alinear entre sí.

- Ondas Infrarrojas.- Las ondas infrarrojas se usan mucho para la comunicación de corto alcance. Por ejemplo los controles remotos de los equipos utilizan comunicación infrarroja. Estos controles son direccionales, tienen el inconveniente de no atravesar los objetos sólidos.

  El hecho de que las ondas infrarrojas no atraviesen los sólidos es una ventaja. Por lo que un sistema infrarrojo no interferirá un sistema similar en un lado adyacente. Además la seguridad de estos sistemas contra espionaje es mejor que la de los sistemas de radio. Este sistema no necesita de licencia del gobierno para operar en contraste con los sistemas de radio. Esta propiedad ha hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores.

- Transmisión Por Ondas De Luz.- Este tipo de transmisión se ha usado durante siglos. Una aplicación es conectar las LAN de dos edificios por medio de láseres montados en la parte más alta de los edificios, esta señalización óptica es unidireccional por lo que cada edificio necesita su propio láser y su propio foto detector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. Fácil de instalar y no requiere de licencia.

  Por ser un haz muy estrecho tiene ventajas pero también es una debilidad. La desventaja es que los rayos láser no pueden penetrar la lluvia ni la niebla densa, funcionan bien en días soleados.

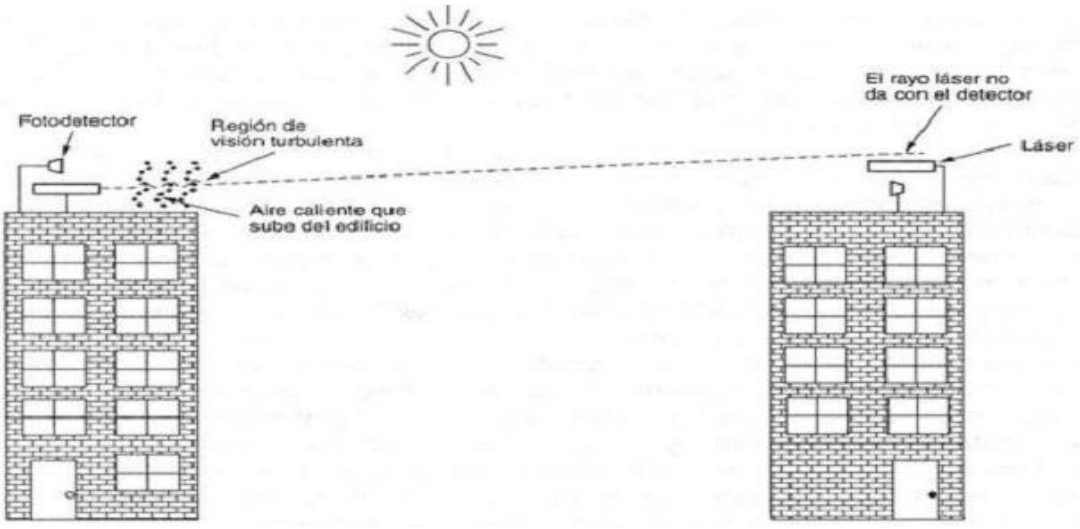


Figura 1.10. Transmisión por Ondas de Luz

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

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

- De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps
- De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuitería especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular son:

- La carga de los teléfonos se termina fácilmente.

- La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).
- Las velocidades de transmisión son bajas.
- Todas estas desventajas hacen que la comunicación celular se utilice poco, o únicamente para archivos muy pequeños como cartas, planos, etc. Pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable en algunas situaciones.

La otra opción que existe en redes de larga distancia son las denominadas: Red Pública De Conmutación De Paquetes Por Radio. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringida por la propia organización de sus sistemas de cómputo.

Redes públicas de radio. Las ondas de radio pueden viajar a grandes distancias y penetrar los edificios sin problemas, razón por la cual se usan tanto en interiores como en exteriores. Las ondas de radio son omnidireccionales ó sea viajan en todas las direcciones por lo que el transmisor y receptor no tienen que alinearse. Las propiedades de la onda dependen de la frecuencia. A bajas frecuencias las ondas de radio cruzan bien los obstáculos, pero la potencia disminuye drásticamente con la distancia de la fuente. A frecuencias altas, las ondas tienden a viajar en línea recta y a rebotar por los obstáculos también son absorbidas por la lluvia.

En todas las frecuencias, las ondas de radio están sujetas a interferencia por motores y otros equipos eléctricos. Esta es una de las razones por la cual, los gobiernos legislan el uso de los radiotransmisores. Las redes públicas tienen dos protagonistas principales: "ARDIS" (una asociación de Motorola e IBM) y "RAM Mobile Data" (desarrollado por Ericsson AB, denominado MOBITEX). Este último es el más utilizado en Europa. Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia.

La compañía proporciona la infraestructura de la red, se incluye controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas, estos sistemas soportan el estándar de conmutación de paquetes X.25, así como su propia estructura de paquetes. Estas redes se encuentran de acuerdo al modelo de referencia OSI.

ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software (por ej. una compañía llamada RF Data, desarrollo una rutina de compresión de datos para utilizarla en estas redes públicas).Los fabricantes de equipos de computo venden periféricos para estas redes (IBM desarrollo su "PC Radio" para utilizarla con ARDIS y otras redes, públicas y privadas). La PC Radio es un dispositivo manual con un microprocesador 80C186 que corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de memoria y 640 Kb de RAM. Estas redes operan en un rango de 800 a 900 MHz ARDIS ofrece una velocidad de transmisión de 4.8 Kbps Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta). Las redes públicas de radio como ARDIS y MOBITEX jugaran un papel significativo en el mercado de redes de área local (LAN´s) especialmente para corporaciones de gran tamaño.

1.11. BENEFICIOS DE LAS REDES INALÁMBRICAS[11]

Utilizando una WLAN se puede acceder a información compartida sin necesidad de buscar un lugar para conectar el computador, y los administradores de la red pueden poner a punto o aumentar la red sin instalar o mover cables. Veamos más ampliamente sus beneficios.

Visión general de los beneficios de una WLAN Frente a las redes tradicionales se tienen las siguientes ventajas en cuanto a productividad, comodidad y costos:

- Movilidad: Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.

[11] http://www.monografias.com/trabajos43/redes-inalambricas/redes-inalambricas2.shtml

- Facilidad de instalación: Evita obras para tirar cable por muros y techos.
- Flexibilidad: Permite llegar donde el cable no puede.
- Reducción de costos: Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.

CAPITULO II

2. ESPECIFICACIONES DE LAS REDES ALÁMBRICAS E INALÁMBRICAS

2.1.ESPECIFICACIONES DE LAS REDES INALÁMBRICAS

2.1.1. ESTÁNDARES DE LAS REDES INALÁMBRICAS (IEEE 802.11)[12]

2.1.1.1. IEEE 802.11

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps. Este fue el primero de los estándares definidos por la IEEE para aplicaciones WLAN, y fue publicado en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales de radiofrecuencia (RF) e infrarrojas (IR). Funciona sobre la banda ISM ("*Industrial, Scientific and Medical*") Industria Científica y Médica de 2.4 GHz (de 2.400 MHz a 2.483,5 MHz) y utiliza dos tipos de modulación: DSSS ("*Direct Sequence Spread Spectrum*") y FHSS ("*Frequency Hopped Spread Spectrum*"). La velocidad de transmisión que es capaz de alcanzar está entre 1 ó 2 Mbps, dependiendo del fabricante.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Este estándar está prácticamente en desuso, debido a la aparición de una serie de variantes que mejoran no sólo la velocidad de transferencia, sino que además dan cobertura a funciones especiales de seguridad.

[12] http://es.wikipedia.org/wiki/IEEE_802.11

2.1.1.2. IEEE 802.11a

En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b, este nuevo estándar que fue ratificado en 1999, también conocido como "Wi-Fi5", presenta, como diferencia fundamental, su funcionamiento sobre la banda de frecuencia de 5 GHz (de 5.150 MHz a 5.350 MHz y de 5.470 MHz a 5.725 MHz), utilizando la técnica de modulación de radio OFDM ("*Ortogonal Frequency Division Multiplexing*"). Esta técnica permite dividir una portadora de datos de alta velocidad en 52 subportadoras ortogonal frequency-division multiplexing (OFDM) de baja velocidad que se transmiten en paralelo con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. Estas subportadoras se pueden agrupar de un modo mucho más integrado que con la técnica de espectro que utiliza el estándar 802.11b. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto, con el consiguiente aumento en la capacidad para las comunicaciones simultáneas.

Aunque este aumento en la velocidad presenta una excelente ventaja, lo cierto es que esta norma cuenta también con algunas desventajas con respecto a su antecesora, como es el mayor nivel de consumo (que la hace menos idónea para su instalación en portátiles o PDAs), o la falta de compatibilidad con el 802.11b debido al cambio de frecuencia, aunque esto último ya se ha resuelto a través de puntos de acceso que ofrecen soporte para ambos estándares.

Otro dato que se puede resaltar sobre este estándar es que las distancias de cobertura se ven reducidas significativamente, alcanzando entre 30 m (54 Mbps) y 300 m (6 Mbps) en exteriores, y entre 12 m (54 Mbps) y 90 m (6 Mbps) cuando se utiliza en interiores.

2.1.1.3.IEEE 802.11b

Es la evolución natural del IEEE 802.11 fue ratificada en 1999. Tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA

definido en el estándar original, también trabaja en la banda de 2.4 GHz debido al espacio ocupado por la codificación del protocolo CSMA/CA.

Básicamente se diferencian en el uso exclusivo de la modulación DSSS con el sistema de codificación CCK ("*Complementary Code Keying*") que sólo funciona con esta modulación. Esto le permite ofrecer hasta 11 Mbps. Las velocidades de transmisión que es capaz de variar desde 1, 2,5.5, y 11 Mbps, dependiendo de diferentes factores.

Esta característica, denominada DRS ("*Dynamic Rate Shifting*") permite a los adaptadores de red inalámbricos reducir las velocidades para compensar los posibles problemas de recepción que se pueden generar por las distancias o los materiales que es necesario atravesar como paredes, tabique, madera etc.

Otros datos a tener en cuenta sobre este estándar es el soporte para tres canales sin traslape y su reducido nivel de consumo, que lo hace perfecto para su uso en PCs portátiles o PDAs.

En cuanto a las distancias a cubrir, dependerá de las velocidades aplicadas, del número de usuarios conectados y del tipo de antenas y amplificadores que se puedan utilizar. Aún así, se podrían dar unas cifras de alrededor de entre 120m (a 11 Mbps) y 460m (a 1 Mbps) en espacios abiertos, y entre 30m (a 11 Mbps) y 90m (a 1 Mbps) en interiores, dependiendo lógicamente del tipo de materiales que sea necesario atravesar.

En la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

2.1.1.4. IEEE 802.11c

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo 'c' es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el

otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo ‘c’ es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación.

"El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI)".

2.1.1.5.IEEE 802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

2.1.1.6.IEEE 802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access y
- (HCCA) Controlled Access.

2.1.1.7.IEEE 802.11f

Básicamente, es una especificación que funciona bajo el estándar 802.11g y que se aplica a la intercomunicación entre puntos de acceso de distintos fabricantes, permitiendo el *roaming* de clientes.

2.1.1.8.IEEE 802.11g

A mediados del año 2003 se aprobó un nuevo estándar, el 802.11g, que se basa en la norma 802.11b. Más avanzada que su predecesora, trabaja sobre la misma frecuencia de los 2.4 GHz y es capaz de utilizar dos métodos de modulación (DSSS y OFDM), lo que la hace compatible con el estándar de facto en esta industria.

Al soportar ambas codificaciones, este nuevo estándar será capaz de incrementar notablemente la velocidad de transmisión, pudiendo llegar hasta los 54 Mbps o cerca de 24.7 Mbit/s de velocidad real de transferencia que oferta la norma 802.11a, aunque manteniendo las características propias del 802.11b en cuanto a distancia, niveles de consumo y frecuencia utilizada.

De este modo, la mayor bondad de esta nueva norma es el incremento de velocidad manteniendo una total compatibilidad con el estándar Wi-Fi, permitiendo la coexistencia entre ambos estándares en una misma instalación, algo realmente significativo si tenemos en cuenta la importancia de la base instalada.

Sin embargo, en redes bajo el estándar g y la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión, esto puede ser una desventaja al combinar los dos estándares.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

2.1.1.9.IEEE 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélites en la banda de los 5 GHz (802.11a).

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ERC/DEC/ (99)23).

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

Selección Dinámica de Frecuencias y Control de Potencia del Transmisor DFS (Dynamic Frequency Selection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

2.1.1.10. IEEE 802.11i

Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Encriptación Avanzado).

2.1.1.11. IEEE 802.11k

Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

2.1.1.12. IEEE 802.11n

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabo el segundo boceto.

2.1.1.13. IEEE 802.11p

Este estándar opera en el espectro de frecuencias de 5.9 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

2.1.1.14. IEEE 802.11r

También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

2.1.1.15. IEEE 802.11s

Define la interoperabilidad de fabricantes en cuanto a protocolos Mesh (son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura.). Bien es sabido que no existe un estándar, y que por eso cada fabricante tiene sus propios mecanismos de generación de mallas.

2.1.1.16. IEEE 802.11u

IEEE 802.11u está una enmienda propuesta a IEEE 802.11-2007 estándar para agregar las características que mejoran intertrabajar con las redes externas.

802.11 es IEEE estándar eso permite que los dispositivos tales como computadoras de computadora portátil o teléfonos portátiles ensamblen una radio LAN ampliamente utilizado en el hogar, la oficina y algunos establecimientos comerciales.

2.1.1.17. IEEE 802.11v

IEEE 802.11v servirá (previsto para el 2010) para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías: mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

2.1.1.18. IEEE 802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envía la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

2.1.1.19. IEEE 802.11y

Este estandar Publicado en noviembre de 2008, y permite operar en la banda de 3650 a 3700 MHz (excepto cuando pueda interferir con una estación terrestre de comunicaciones por satélite) en EEUU, aunque otras bandas en diferentes dominios reguladores también se están estudiando. Las normas FCC para la banda de 3650 MHz permiten que las estaciones registradas operen a una potencia mucho mayor que en las tradicionales bandas ISM (hasta 20 W PIRE). Otros tres conceptos se añaden: Contention Base Protocol (CBP), Extended Channel Switch Announcement (ECSA), y Dependent Station Enablement (DSE). CBP incluye mejoras en los mecanismos de detección de portadora. ECSA proporciona un mecanismo para que los puntos de acceso (APs) notifiquen a las estaciones conectadas a él de su intención de cambiar de canal o ancho de banda. Por último, la DSE se utiliza para la gestión de licencias.

2.2. ESPECIFICACIONES DE LAS REDES ALÁMBRICAS

2.2.1. ESTÁNDARES DE LAS REDES ALÁMBRICAS (IEEE 802.11)[13]

2.2.1.1. IEEE 802.1 Definición Internacional de Redes

Define la relación entre los estándares 802 del IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI) de la ISO (Organización Internacional de Estándares). Por ejemplo, este Comité definió direcciones para estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única. Los vendedores de tarjetas de interface de red están registrados y los tres primeros bytes de la dirección son asignados por el IEEE. Cada vendedor es entonces responsable de crear una dirección única para cada uno de sus productos.

[13] http://www.scribd.com/doc/21146436/Estandares-IEEE-802

2.2.1.2.IEEE 802.2

Control de Enlaces Lógicos. Define el protocolo de control de enlaces lógicos (LLC) del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación. La capa de Datos-Enlace en el protocolo OSI esta subdividida en las subcapas de Control de Acceso a Medios (MAC) y de Control de Enlaces Lógicos (LLC). En Puentes, estas dos capas sirven como un mecanismo de switcheo modular, como se muestra en la figura I-5. El protocolo LLC es derivado del protocolo de Alto nivel para Control de Datos-Enlaces (HDLC) y es similar en su operación. Nótese que el LLC provee las direcciones de Puntos de Acceso a Servicios (SAP's), mientras que la subcapa MAC provee la dirección física de red de un dispositivo. Las SAP's son específicamente las direcciones de una o más procesos de aplicaciones ejecutándose en una computadora o dispositivo de red.

El LLC provee los siguientes servicios:

- Servicio orientado a la conexión, en el que una sesión es empezada con un Destino, y terminada cuando la transferencia de datos se completa. Cada nodo participa activamente en la transmisión, pero sesiones similares requieren un tiempo de configuración y monitoreo en ambas estaciones.

- Servicios de reconocimiento orientado a conexiones. Similares al anterior, del que son reconocidos los paquetes de transmisión.

- Servicio de conexión sin reconocimiento. En el cual no se define una sesión. Los paquetes son puramente enviados a su destino. Los protocolos de alto nivel son responsables de solicitar el reenvío de paquetes que se hayan perdido. Este es el servicio normal en redes de área local (LAN's), por su alta confiabilidad.

2.2.1.3.IEEE 802.3

Redes CSMA/CD. El estándar 802.3 del IEEE (ISO 8802-3), que define cómo opera el método de Acceso Múltiple con Detección de Colisiones (CSMA/CD) sobre varios

medios. El estándar define la conexión de redes sobre cable coaxial, cable de par trenzado, y medios de fibra óptica. La tasa de transmisión original es de 10 Mbits/seg, pero nuevas implementaciones transmiten arriba de los 100 Mbits/seg calidad de datos en cables de par trenzado.

2.2.1.4.IEEE 802.4

Redes Token Bus. El estándar token bus define esquemas de red de anchos de banda grandes, usados en la industria de manufactura. Se deriva del Protocolo de Automatización de Manufactura (MAP). La red implementa el método token-passing para una transmisión bus. Un token es pasado de una estación a la siguiente en la red y la estación puede transmitir manteniendo el token. Los tokens son pasados en orden lógico basado en la dirección del nodo, pero este orden puede no relacionar la posición física del nodo como se hace en una red token ring. El estándar no es ampliamente implementado en ambientes LAN.

2.2.1.5. IEEE 802.5

Redes Token Ring. También llamado ANSI 802.1-1985, define los protocolos de acceso, cableado e interface para la LAN token ring. IBM hizo popular este estándar. Usa un método de acceso de paso de tokens y es físicamente conectada en topología estrella, pero lógicamente forma un anillo. Los nodos son conectados a una unidad de acceso central (concentrador) que repite las señales de una estación a la siguiente. Las unidades de acceso son conectadas para expandir la red, que amplía el anillo lógico. La Interface de Datos en Fibra Distribuida (FDDI) fue basada en el protocolo token ring 802.5, pero fue desarrollado por el Comité de Acreditación de Estándares (ASC) X3T9.

Es compatible con la capa 802.2 de Control de Enlaces Lógicos y por consiguiente otros estándares de red 802.

2.2.1.6.IEEE 802.6

Redes de Área Metropolitana (MAN). Define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado Bus Dual de Cola Distribuida (DQDB). El bus dual provee tolerancia de fallos para mantener las conexiones si el bus se rompe. El estándar MAN está diseñado para proveer servicios de datos, voz y vídeo en un área metropolitana de aproximadamente 50 kilómetros a tasas de 1.5, 45, y 155 Mbits/seg. DQDB es el protocolo de acceso subyacente para el SMDS (Servicio de Datos de Multimegabits Switcheados), en el que muchos de los portadores públicos son ofrecidos como una manera de construir redes privadas en áreas metropolitanas. El DQDB es una red repetidora que switchea celdas de longitud fija de 53 bytes; por consiguiente, es compatible con el Ancho de Banda ISDN y el Modo de Transferencia Asíncrona (ATM). Las celdas son switcheables en la capa de Control de Enlaces Lógicos.

Los servicios de las MAN son Sin Conexión, Orientados a Conexión, y/o isócronas (vídeo en tiempo real). El bus tiene una cantidad de slots de longitud fija en el que son situados los datos para transmitir sobre el bus. Cualquier estación que necesite transmitir simplemente sitúa los datos en uno o más slots. Sin embargo, para servir datos isócronos, los slots en intervalos regulares son reservados para garantizar que los datos llegan a tiempo y en orden.

2.2.1.7.IEEE 802.7

Grupo Asesor Técnico de Anchos de Banda. Este comité provee consejos técnicos a otros subcomités en técnicas sobre anchos de banda de redes.

2.2.1.8.IEEE 802.8

Grupo Asesor Técnico de Fibra Óptica. Provee consejo a otros subcomités en redes por fibra óptica como una alternativa a las redes basadas en cable de cobre. Los estándares propuestos están todavía bajo desarrollo.

2.2.1.9.IEEE 802.9

Redes Integradas de Datos y Voz. El grupo de trabajo del IEEE 802.9 trabaja en la integración de tráfico de voz, datos y vídeo para las LAN 802 y Redes Digitales de Servicios Integrados (ISDN's). Los nodos definidos en la especificación incluyen teléfonos, computadoras y codificadores/decodificadores de vídeo (codecs). La especificación ha sido llamada Datos y Voz Integrados (IVD). El servicio provee un flujo multiplexado que puede llevar canales de información de datos y voz conectando dos estaciones sobre un cable de cobre en par trenzado. Varios tipos de diferentes de canales son definidos, incluyendo full duplex de 64 Kbits/seg sin switcheo, circuito switcheado, o canales de paquete switcheado.

2.2.1.10. IEEE 802.10

Grupo Asesor Técnico de Seguridad en Redes. Este grupo está trabajando en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y encriptamiento. Los estándares propuestos están todavía bajo desarrollo en este momento.

2.2.1.11. IEEE 802.11

El estándar **IEEE 802.11** define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

2.2.1.12. IEEE 802.12

Prioridad de Demanda (100VG-ANYLAN). Este comité está definiendo el estándar Ethernet de 100 Mbits/seg. Con el método de acceso por Prioridad de Demanda propuesto por Hewlett Packard y otros vendedores. El cable especificado es un par trenzado de 4 alambres de cobre y el método de acceso por Prioridad de Demanda usa

un hub central para controlar el acceso al cable. Hay prioridades disponibles para soportar envío en tiempo real de información multimedia.

2.2.1.13. IEEE 802.15

IEEE 802.15 es un grupo de trabajo dentro de IEEE 802 especializado en redes inalámbricas de área personal (*wireless personal area networks*, WPAN). Se divide en cinco subgrupos, del 1 al 5.

Los estándares que desarrolla definen redes tipo PAN o HAN, centradas en las cortas distancias. Al igual que Bluetooth o ZigBee, el grupo de estándares 802.15 permite que dispositivos portátiles como PC, PDAs, teléfonos, pagers, sensores y actuadores utilizados en domótica, entre otros, puedan comunicarse e interoperar. Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11.x, se definió este estándar para permitir la interoperatibilidad de las redes inalámbricas LAN con las redes tipo PAN o HAN.

2.2.1.14. IEEE 802.16

IEEE 802.16 es el nombre de un grupo de trabajo del comite IEEE 802 y el nombre se aplica igualmente a los trabajos publicados.

Se trata de una especificación para las redes de acceso metropolitanas inalámbricas de banda ancha fijas (no móvil) publicada inicialmente el 8 de abril de 2002. En esencia recoge el estándar *de facto* **WiMAX**.

El estandar 802.16 ocupa el espectro de frecuencias ampliamente, usando las frecuencias desde 2 hasta 11 Ghz para la comunicación de la última milla (de la estación

base a los usuarios finales) y ocupando frecuencias entre 11 y 60 Ghz para las comunicaciones con línea vista entre las estaciones bases.

2.2.1.15. IEEE 802.17

El grupo de funcionamiento resistente del anillo del paquete de IEEE 802,17 (RPRWG) está definiendo un protocolo resistente del acceso del anillo del paquete para el uso en las redes de área local, metropolitana y amplia para la transferencia de los paquetes de los datos en las tarifas scalable a muchos gigabites por segundo. El nuevo estándar utilizará especificaciones existentes de la capa física y desarrollará PHYs nuevo cuando sea apropiado.

En redes de área metropolitana y amplia, los anillos ópticos de la fibra se despliegan extensamente. Estos anillos están utilizando actualmente los protocolos que son ni optimizados ni scalable a las demandas de las redes del paquete, incluyendo la velocidad del despliegue, de la asignación y del rendimiento de procesamiento de la anchura de banda, de la viveza a las averías, y de los costes reducidos del equipo y operacionales.

2.2.1.16. IEEE 802.18

IEEE 802, el comité de estándares de LAN/MAN, o LMSC, tiene actualmente 4 grupos de funcionamiento con proyectos sobre los estándares para los sistemas radio-basados... 802,11 (WLAN), 802,15 (WPAN), 802,16 (WMAN), y 802,20 (movilidad sin hilos). Por lo tanto, la supervisión, y la participación activa de adentro, las actividades reguladoras de radio en curso, en los niveles nacionales e internacionales, son una parte importante del trabajo de LMSC. Ése es el trabajo de los 802,18 grupos consultivos técnicos reguladores de radio ("Rr-etiqueta"). Cualquier sugerencia para las mejoras a estas páginas para hacerles que una voluntad más útil siempre es recepción y se puede enviar a Carl R. Stevenson.

2.2.1.17. IEEE 802.19

El grupo consultivo técnico de la coexistencia de IEEE 802,19 (ETIQUETA) desarrollará y mantendrá las políticas que definen las responsabilidades de 802 reveladores de los estándares de tratar aplicaciones la coexistencia con estándares existentes y otros estándares bajo desarrollo. También, cuando está requerido, los gravámenes de la oferta al comité ejecutivo del patrocinador (SEC) con respecto al grado con el cual los reveladores de los estándares se han conformado con esas convenciones. La ETIQUETA puede también desarrollar la documentación de la coexistencia del interés a la comunidad técnica fuera de 802.

2.2.1.18. IEEE 802.20

La misión de IEEE 802,20 es desarrollar la especificación para un interfaz basado paquete eficiente del aire que se optimice para el transporte de servicios basados IP. La meta es permitir el despliegue mundial de comprables, de ubicuos, siempre-en y las redes de acceso sin hilos de banda ancha móviles multi-vendor interoperable que resuelvan las necesidades del negocio y de los mercados residenciales del usuario del extremo.

2.2.1.19. IEEE 802.21

IEEE 802.21 está desarrollando estándares para permitir la entrega y la interoperabilidad entre los tipos de red heterogéneos, incluyendo dos 802 y no 802 redes

2.2.1.20. IEEE 802.22

Red inalámbrica de área regional. *802.22 WG on WRANs (Wireless Regional Area Networks).*

2.3.CARACTERÍSTICAS TÉCNICAS DE LAS REDES ALAMBRICAS E IMALAMBRICAS[14]

2.3.1. DIRECCIÓN IP

Una dirección IP es una serie de números que identifica a nuestro equipo dentro de una red.
Distinguimos entre IP pública (ej. 80.20.140.56), cuando es la dirección que nos identifica en Internet (por ejemplo la IP del router ADSL en Internet) e IP privada (ej. 192.168.0.2), que es la dirección que identifica a un equipo dentro de una red local (LAN).

Si, por ejemplo, pensamos en una red local con un router ADSL, los PCs o equipos conectados a la red tendrán sólo IP privada, mientras que el router tendrá una IP pública (su identificación en Internet) y una IP privada (su identificación en la red local).

2.3.2. MÁSCARA DE SUBRED

Es una cifra de 32 bits que especifica los bits de una dirección IP que corresponde a una red y a una subred. Normalmente será del tipo 255.255.255.0.

2.3.3. PUERTA DE ENLACE

Es la dirección IP privada de nuestro router.

2.3.4. SERVIDORES DNS

Las páginas web también tienen su dirección IP pública y es a través de ésta dirección como en realidad nos conectamos a ellas. Pero claro, es más sencillo memorizar o escribir el nombre del dominio (www.google.es) que su dirección IP (216.239.59.104).

[14] http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/438/1/LUCERNA.pdf

Para no memorizar la retahíla de números tenemos los servidores DNS. Un servidor DNS es un servidor en donde están almacenadas las correlaciones entre nombres de dominio y direcciones IP.

Cada vez que cargamos una página web, nuestro equipo (PDA, portátil u ordenador de sobremesa) envía una petición al servidor DNS para saber la dirección IP de la página que queremos cargar, y es entonces cuando hace la conexión.

2.3.5. SSID (SERVICE SET IDENTIFICATION)

Nombre con el que se identifica a una red Wi-Fi. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del Punto de Acceso.

2.3.6. DHCP

Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente.

Por defecto la mayoría de los routers ADSL y los Puntos de Acceso tienen DHCP activado.

2.3.7. DIRECCIÓN MAC

Es el código único de identificación que tienen todas las tarjetas de red. Nuestro accesorio Wi-Fi o nuestro PDA con Wi-Fi integrado, al ser un dispositivo de red, también tendrán una dirección MAC única.

Las direcciones MAC son únicas (ningún dispositivo de red tiene dos direcciones MAC iguales) y permanentes (ya que vienen preestablecidas de fábrica y no pueden modificarse).

CAPITULO III

3. SEGURIDAD EN REDES ALAMBRICAS E INALAMBRICAS

Los principales conceptos relacionados con la implementación de mecanismos de seguridad para el control de acceso en redes de datos cableadas e inalámbricas, se presentan a continuación:

3.1. CONTROL DE ACCESO

El control de acceso, en sistemas de información, es la capacidad de controlar la interacción de un elemento activo (usuario, dispositivo, servicio) con un recurso informático (red de datos, sistema, servicio). Adicionalmente, el control de acceso implica procedimientos de identificación, autenticación y autorización para permitir o denegar el uso de los recursos.

3.2. IDENTIFICACIÓN, AUTENTICACIÓN, AUTORIZACIÓN[15]

3.2.1. Identificación

La identificación es el procedimiento mediante el cual un elemento presenta su identidad a otro componente. Generalmente la identificación puede estar dada por un nombre de usuario, número de identificación o número de cuenta. Este parámetro no solo permite realizar la identificación, si no que habilita al sistema a relacionar la identidad con el uso de los recursos

3.2.2. Autenticación

Es el proceso de validar la identidad de quien accede o provee un servicio, mediante la verificación de ciertas credenciales o parámetros que debe proveer la entidad que se autentica. Entre los métodos más comunes de autenticación se encuentra el uso de una contraseña o clave personal, sin embargo cada vez es más requerido el uso de otros

[15] http://www.segu-info.com.ar/

factores de autenticación como tokens[16] o Biometría[17]. A nivel de enlace de datos, y de acuerdo al método y características de seguridad, existen diversos tipos de autenticación entre los cuales podemos citar:

- PAP (Password Authentication Protocol): Este protocolo realiza la validación cuando se establece la conexión entre el cliente y el servidor. Utiliza el nombre de usuario y contraseña como credenciales, las cuales son enviadas en texto plano sobre el enlace, por lo que se considera un método poco seguro.

- CHAP (Challenge Handshake Protocol): Provee un mejor nivel de seguridad, ya que realiza una validación de tres vías entre cliente y servidor, donde este último envía un parámetro de control a quien se autentica, este lo encripta con su contraseña y lo reenvía al servidor, donde se realiza el mismo procedimiento con la contraseña almacenada y se verifica si se obtiene el mismo resultado.

- EAP (Extensible Authentication Protocol): Es un protocolo que permite elevar aún más el nivel de seguridad de la autenticación, permitiendo diversos métodos autenticación y tipos de credenciales a utilizar (incluyendo la capacidad de manejar certificados digitales). De acuerdo a esto, diversos tipos de EAP se pueden implementar conforme a las características y condiciones propias de cada infraestructura donde se la requiera.

TABLA 3.1. Métodos del EAP

MÉTODO	CARACTERÍSTICAS
EAP-TLS	• Transport Layer Security • Autenticación muy segura. • Reemplaza simples claves por certificados para el cliente y el servidor.
EAP-TTLS	• Tunneled Transport Layer Security. • Extensión de TLS.

[16] T**oken de seguridad**, es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.
[17] **Biometría**, tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas.

	• Desarrollada para sobreponerse a la desventaja en cuanto a la necesidad de poseer un certificado por cliente.
EAP-PEAP	• Protected Extensible Authentication Protocol. • Soporta métodos EAP a través del túnel, pero a diferencia de TTLS, no soporta otros métodos para la negociación de la autenticación del cliente.
EAP-LEAP	• Light Extensible Authentication Protocol. • Autenticación mutua, distribución de clave de sesión segura y dinámica para cada usuario. • Vulnerable ante ataques de diccionario.

3.2.3. Autorización

Establece lo que un usuario puede o no hacer una vez identificado y autenticado.

3.3. SEGURIDAD EN REDES INALÁMBRICAS.[18]

Los usuarios de servicios de telecomunicaciones demandan, cada día más beneficios y flexibilidad. Por tal motivo, en los últimos cinco años ha existido un desarrollo acelerado de la tecnología inalámbrica, en el campo de las redes de área local. Así, nace la tecnología WiFi que define las normas de comunicación para la tecnología en cuestión. Pero, uno de los aspectos de mayor importancia que no fue atacado con el debido cuidado fue la seguridad en esta tecnología, que inicialmente incorporó protocolos existentes de seguridad de redes alambradas denominadas WEP (Wired Equivalent Privacy), y que al sufrir anomalías en su implementación, por tratarse de un tipo de encriptación del tipo estático, se llegó a determinar que para cierta cantidad de información encriptada era posible derivar la llave de encriptación. En consecuencia por ésta falta de seguridad, se crearon comités encargados en desarrollar un nuevo estándar orientado a la seguridad de las redes WiFi (802.11i). De ésta manera, se definieron nuevos conceptos de seguridad para redes WiFi que prometen asegurar la confidencialidad de los datos. Además existen varias empresas líderes en el desarrollo

[18] http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/438/1/LUCERNA.pdf

tecnológico que dan empuje para la utilización de nuevas técnicas de privacidad y autentificación de los usuarios.

En las últimas fechas aparecen noticias sobre lo fácil que es conseguir el acceso a redes wireless mal configuradas, aunque conviene recordar que una red inalámbrica correctamente administrada no es más que uno de los muchos puntos de seguridad que se deben mantener adecuadamente en cualquier institución.

3.3.1. Tecnologías de seguridad[19]

Hoy en día existen varias tecnologías de seguridad con las que contamos la cuales son:

- SSID (uso por default)
- MAC filtering
- VPN
- Captive Portal
- WEP (Wired equivalent privacy)
- WPA

3.3.1.1.SSID (Service Set IDentifier)

El SSID es el mecanismo para identificar redes inalámbricas, es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. A menudo al SSID se le conoce como nombre de la red. Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debería ser el único método de defensa para proteger una red inalámbrica.

[19] http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/438/1/LUCERNA.pdf

3.3.1.2. Filtrado de MAC

El filtrado por direcciones MAC permite hacer una lista de equipos que tienen acceso al AP, o bien denegar ciertas direcciones MAC, la dirección MAC es única en cada tarjeta de red ya sea Ethernet, modem, WiFi sin embargo la principal desventaja radica en que la dirección MAC de la tarjeta puede ser intercambiable (clonada), lo que permite una obtención de una entrada válida en el AP.

3.3.1.3. VPN (Red Privada Virtual)

Algunos AP permiten la configuración de VPN en el equipo, permitiendo que el usuario que se conecte tenga que autentificarse para poder salir del AP, además de ofrece una encriptación de los datos en el tránsito de datos, haciendo más difícil el husmeo de tráfico por un tercero.

La desventaja que presenta es que no todos los APs tienen este servicio La autenticación en la mayoría de los casos no es centralizada y cuando la es, se tiene acceso a una parte de la red que puede ser utilizada para otro tipo de ataques. Se requiere un software adicional, no todos los equipos lo soportan. Existe una gran diversidad de VPN, como: IPSec, L2TP, PPTP, entre otras, y pueden ser atacados por DOS o ataques de diccionario.

3.3.1.4. Captive Portal

Estos permiten dar acceso a un portal donde se autentifica el cliente, dando le acceso a este equipo por un tiempo determinado o bajo ciertas condiciones. Este esquema de seguridad no es muy utilizado debido a que debe de estar en el AP para un mejor funcionamiento.

No todos los AP tienen soporte, los OpenAP o soluciones fuentes abiertas (opensource) ofrecen estas cualidades. Puede ser atacado por DOS o ataques de diccionario. El problema aun sigue ya que el control de acceso al AP no existe.

3.3.1.5. WEP (Wired Equivalent Privacy)

La característica principal de las redes wireless es que utilizan el aire para transmitir la información. Esta particularidad le otorga enormes beneficios sobre las redes tradicionales por cables, pero también es el principal riegos de seguridad que presenta: si la información se transmite por el aire, cualquier persona, con el receptor adecuado, puede acceder a la información.

Desde las primeras fases del desarrollo del protocolo 802.11 por parte del IEEE, se tuvo en cuenta este problema, y en el estándar se incluyo un protocolo de seguridad de uso opcional, el WEP (Wired Equivalent Privacy). Como su nombre indica, se pretendía que otorgase a las redes inalámbricas una seguridad equiparable a las redes por cable, pero esto no fue así.

Este protocolo se basa en el algoritmo de encriptación simétrico RC4 de RSA Security, con claves secretas compartidas de 40 y 104 bits y un vector de inicialización de 24 bits, que deben ser introducidos en todos los dispositivos que participan en una misma red wireless. Diversos estudios declararon que el protocolo WEP presenta graves problemas de seguridad, siendo el más importante de ellos el ataque que consiste en el análisis de paquetes de información encriptados con el mismo vector de inicialización y la misma clave. Esta coincidencia ocurrirá tarde o temprano si no se renueva la clave de encriptación debido a lo reducido de la longitud del vector de inicialización (24 bits). Esto se puede evitar cambiando manualmente la clave WEP de la red wireless. Sin embargo, esta tarea consistiría en modificar la configuración de todos los equipos de una red, lo que puede convertirse en un trabajo bastante pesado.

Se encuentran disponibles diversos programas de libre distribución que realizan este ataque, con lo que basta con recoger cierta cantidad de tráfico de la red para obtener, gracias a estos programas, la clave WEP de una red wireless.

La solución a este problema se encuentra en el estándar 802.11i, en fase borrador; para no esperar a la publicación oficial del mismo, la WECA lanzó el protocolo WPA como sustituto de las deficiencias del protocolo WEP.

3.3.1.6. WPA (Wi-Fi Protected Access)

Hoy en día, los nuevos mecanismos para la encriptación de redes WiFi apuntan a la utilización de una variante del protocolo WEP denominado WEP Enhancement, que incorpora la utilización de un protocolo de integridad de llave temporal (Temporal Key Integrity Protocol, TKIP) el cual evita la derivación de la llave de encriptación del protocolo WEP. El protocolo TKIP es parte del nuevo estándar 802.11i.

La WECA (*Wireless Ethernet Compatibility Alliance)* desarrolló el protocolo Wi-Fi Protected Access con los objetivos de encontrar un sustituto del protocolo WEP ante la revelación de su debilidad ante ataques pasivos y por la conveniencia de autentificar a los usuarios en lugar de a los dispositivos, tal como hace el protocolo WEP, hasta la aparición definitiva del protocolo 802.11i.

La WECA declara que los dispositivos que implementan WPA serán compatibles con el futuro 802.11i, con el fin de evitar el temor de los usuarios de tener que renovar su equipamiento para adaptar el nuevo estándar. WPA es una parte del borrador del 802.11i, tomando la autentificación mediante el protocolo 802.1x y la encriptación TKIP. Otros avances del 802.11i, como la asociación segura, no son posibles mediante el protocolo WPA.

El protocolo de encriptación TKIP, Temporal Key Integrity Protocol, es una modificación del WEP, del que se duplica la longitud del vector de inicialización (de 24 a 48 bits) para evitar la repetición de un mismo valor, y un método de renovación automática de la clave de encriptación entre los dispositivos wireless.

Además del protocolo TKIP, se desarrolló, en el estándar 802.11i un sistema de control de la integridad de los mensajes denominado MIC (Messges Integrity Control) que permite prevenir ataques que interceptan los datos y los retransmiten al receptor (Bit-Flip attack). El sistema MIC es posible de implementarse en ambos sentidos de la comunicación.

Hoy en día, uno de los mecanismos más robustos disponibles para la autentificación es el protocolo EAP (Extensible Authentication Protocol), que permite habilitar en forma individual por usuario, por llave para cada sesión (EAPTLS).

Finalmente, a diferencia del protocolo WEP que utiliza el algoritmo de encriptación RC4, el protocolo WEP Enhancement ha adoptado la utilización del algoritmo de encriptación AES (Advanced Encryption Standard).

El conjunto de estas nuevas formas de autentificar a los usuarios de las redes WiFi se denomina WPA (WiFi Protected Access).

3.3.1.7. WPA y servidores RADUIS

Para obtener las mayores prestaciones del protocolo WPA, se requiere el uso de un servidor de autentificación externo como el RADIUS. Estas dos herramientas juntas, proporcionan una administración y un control de acceso centralizado de toda la red inalámbrica. Con esto, la necesidad de soluciones adicionales como VPN puede ser eliminada, al menos, en lo referente al enlace inalámbrico.

Un cliente wireless debe ser autentificado antes de tener acceso a los recursos de la red.

Sin embargo, en redes pequeñas o domésticas no se dispone de un servicio como el RADIUS, por lo que el protocolo WPA permite operar en un modo más sencillo llamado PSK (PreShared Key), muy parecido al protocolo WEP, en el que se debe introducir una misma clave en todos los dispositivos de la red inalámbrica. Esta clave se emplea para autentificar al equipo en el momento del acceso a la red posteriormente, entra en funcionamiento el protocolo TKIP.

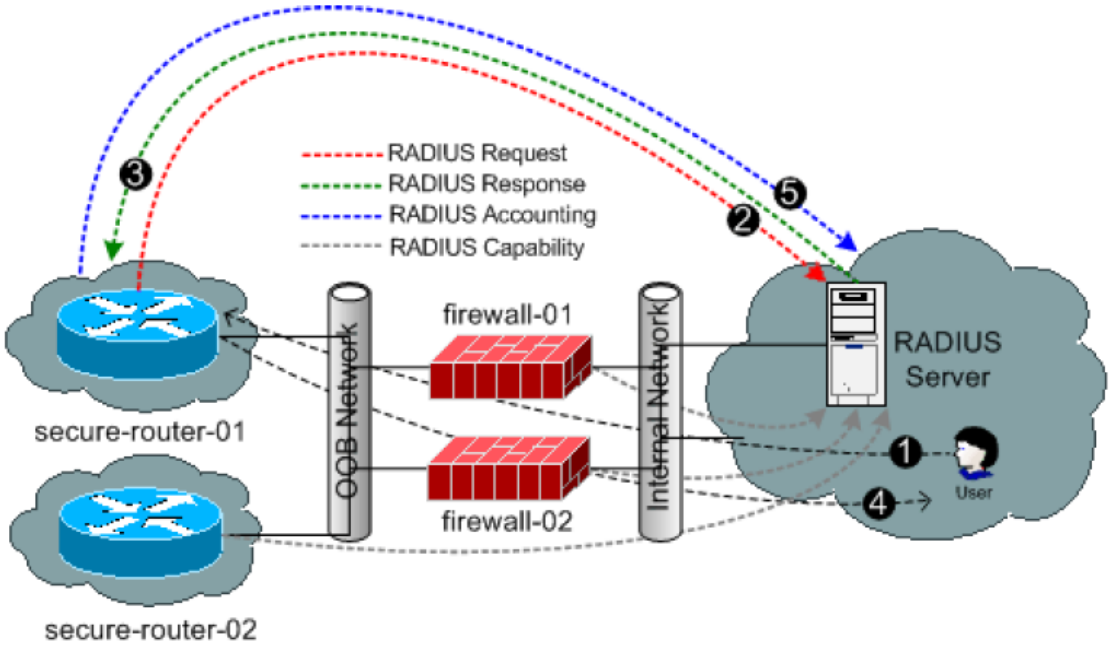


Figura 3.1. Esquema de servidor RADIUS[20]

Como ya se había mencionado en temas anteriores el estándar 802.11i ratificado en Junio del 2004, resuelve las debilidades del WPA. Este es dividido en 3 categorías principales:

1. *Temporary Key Integrity Protocol (TKIP)* es el termino de la solución que resuelve los problemas del WEP. TKIP puede ser usado por el equipo con soporte 802.11, este provee la integridad y la confidencialidad requerida.

2. *Counter Mode with CBC-MAC Protocol (CCMP) [RFC2610]* es un algoritmo criptográfico, utiliza AES [FIPS 197] como algoritmo principal, desde ahí podemos decir que es mayor el consumo de la CPU con respecto a RC4, este requiere un nuevo hardware así como driver con soporte a CCMP.

3. *802.1X Port-Based Network Access Control:* Este usa tanto TKIP como CCMP, 802.1X para la autentificación.

[20] http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/438/1/LUCERNA.pdf

3.4. SEGURIDAD EN REDES CABLEADAS

3.4.1. Tecnologías de seguridad

Hoy en día existen varias tecnologías de seguridad con las que contamos la cuales son:

- Encriptación
- Firewall
- DMZ

3.4.1.1. Encriptación[21]

La encriptación en sistemas de información, es el proceso mediante el cual, utilizando una llave o un valor de control, un mensaje (generalmente datos en texto plano) es codificado para evitar que su contenido sea accedido y/o entendido por personal no autorizado. Para poder acceder al mensaje cifrado es necesario desencriptar el mensaje, proceso mediante el cual, utilizando la llave indicada, se recupera la información del mensaje en su estado original.

3.4.1.1.1. Encriptación simétrica

Es el proceso de cifrado de datos, en el cual se realiza la encriptación y desencripción utilizando la misma llave. La encriptación simétrica es un procedimiento rápido, que provee mecanismos para asegurar la confidencialidad e integridad de la información que protege. Por otro lado el hecho de utilizar la misma clave en los procesos mencionados implica realizar una distribución segura de llaves por vías alternas a la que se quiere proteger. Por lo anterior también es recomendado utilizar la llave la menor cantidad de veces posible, idealmente una sola vez. Algunos de los estándares de encriptación simétrica más conocidos son: DES (Data Encription Standard) Triple DES y AES (Advanced Encription Standard).

[21] http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion

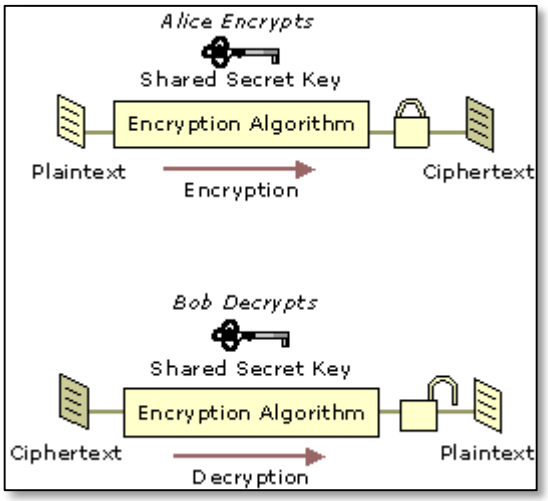


Figura. 3.2. Encriptación Simétrica

3.4.1.1.2. Encriptación asimétrica

Es el proceso de cifrado de datos, en el cual se utiliza llaves diferentes para la encriptación y desencriptación, una de estas de carácter privado o secreto y la otra es de acceso público (dentro de un sistema). También se le conoce como encriptación de clave pública y se dice que se implementa bajo una infraestructura de clave pública (PKI). Este tipo de encriptación fue desarrollado a finales de los años 70's y adicionó nuevas funcionalidades a los mecanismos de encriptación como la posibilidad de realizar autenticación fuerte, no repudio, y el hecho de mejorar y facilitar los esquemas de confidencialidad e integridad. Algunos de los estándares de encriptación asimétrica más conocidos son: RSA (Rivest, Shamir & Addleman), Diffie-Hellman y El Gamal.

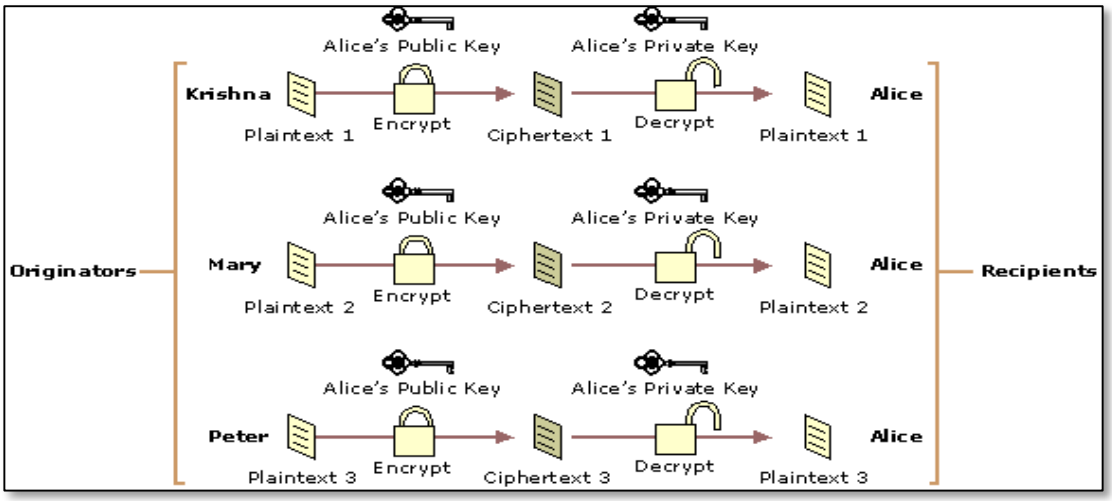


Figura 3.3. Encriptación Asimétrica

3.4.1.2. Firewall / Cortafuegos[22]

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

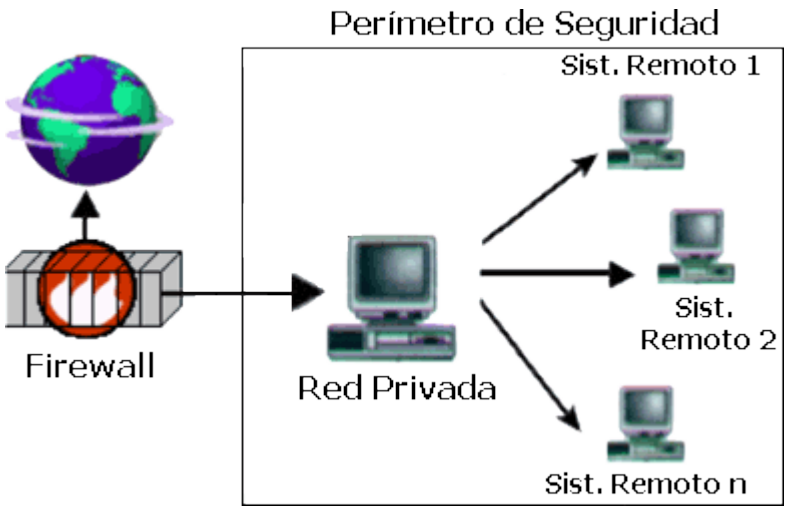


Figura 3.4. Firewall

[22] http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación.

3.4.1.2.1. Tipos de Firewall

- Filtrado de Paquetes
- Proxy-Gateways de Aplicaciones
- Dual-Homed Host
- Screened Host
- Screened Subnet
- Inspección de Paquetes: Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.
- Firewalls Personales: Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

3.4.1.2.2. Políticas de diseño de firewalls[23]

Las políticas de accesos en un Firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir. Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.
- ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

Paradigmas de seguridad

- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más

[23] http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.

Estrategias de seguridad

- Paranoica: se controla todo, no se permite nada.
- Prudente: se controla y se conoce todo lo que sucede.
- Permisiva: se controla pero se permite demasiado.
- Promiscua: no se controla (o se hace poco) y se permite todo.
- ¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuánto es conveniente invertir.

3.4.1.3. DMZ[24]

Los sistemas Firewall permiten definir las reglas de acceso entre dos redes. Sin embargo, en la práctica, las compañías cuentan generalmente con varias subredes con diferentes políticas de seguridad. Por esta razón, es necesario configurar arquitecturas de firewall que aíslen las diferentes redes de una compañía. Esto se denomina "**aislamiento de la red**".

Una **DMZ** (del inglés *Demilitarized zone*) o Zona DesMilitarizada. Una **zona desmilitarizada** (DMZ) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones **desde** la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

[24] file:///C:/Documents%20and%20Settings/JANNETH/Escritorio/tesis/consulta/que-es-una-dmz.html

3.4.1.3.1. Arquitectura DMZ

Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores web, servidores de correo electrónico, servidores FTP), a veces es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer la seguridad de la compañía. El término "**zona desmilitarizada**" o **DMZ** hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

Esto permite que los equipos (hosts) de la DMZ's puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Esto se ve muchísimo más claro en un esquema:

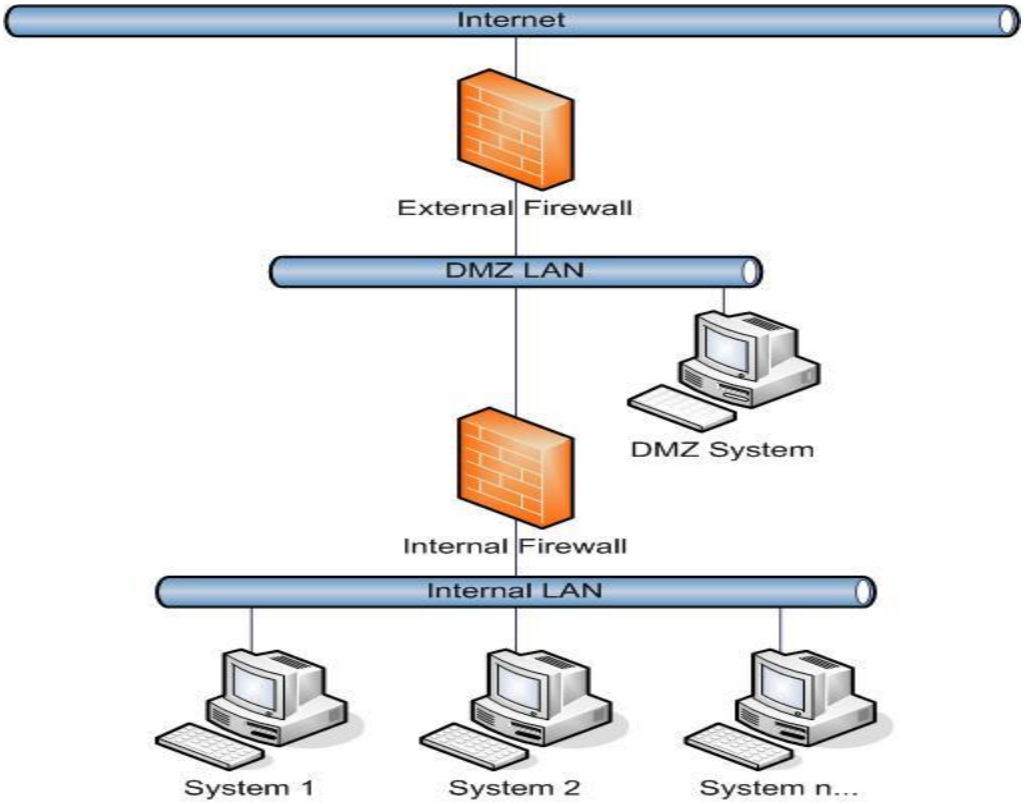


Figura 3.5. Arquitectura de un dmz

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Habitualmente una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

3.4.1.3.2. Políticas de seguridad de un dmz[25]

Por lo general, la política de seguridad para la DMZ es la siguiente:

[25] http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3

- El tráfico de la red externa a la DMZ está **autorizado**
- El tráfico de la red externa a la red interna está **prohibido**
- El tráfico de la red interna a la DMZ está **autorizado**
- El tráfico de la red interna a la red externa está **autorizado**
- El tráfico de la DMZ a la red interna está **prohibido**
- El tráfico de la DMZ a la red externa está **denegado**

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.

Debe observarse que es posible instalar las DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

CAPITULO IV

4. POLITICAS DE SEGURIDAD[26]

Una política de seguridad es un 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.

El uso de la política de seguridad de red debe proteger las redes y riesgos y pérdidas asociadas con recursos de red y seguridad. Las Políticas de Seguridad de Red son la responsabilidad de encontrar una reputación así como responsabilidad potencial. Las Políticas de Seguridad de Red y la seguridad constituyen un riesgo a la misión académica. La pérdida de datos o la revelación no autorizada de la información en investigación y ordenadores educacionales, archivos de estudiante, y sistemas financieros podrían afectar enormemente la facultad y estudiantes.

Los objetivos de la política de seguridad de red son establecer políticas proteger las redes y sistemas de ordenador del uso inadecuado. Los mecanismos de Políticas de Seguridad de Red ayudarán en la identificación y la prevención del abuso de sistemas de ordenador y redes. Las Políticas de Seguridad de Red proporcionan un mecanismo para responder a quejas y preguntas sobre verdaderas redes y sistemas de ordenador. Las Políticas de Seguridad de Red establecen mecanismos que protegerán y satisfarán responsabilidades legales a sus redes y conectividad de sistemas de ordenador al Internet mundial. Los mecanismos de Políticas de Seguridad de Red apoyarán los objetivos de existir políticas.

Una política de seguridad debe asegurar cuatro *aspectos fundamentales* en una solución de seguridad: *autenticación*, *control de acceso*, *integridad* y *confidencialidad*. A partir de estos, surgen los *principales componentes* de una política de seguridad:

- *Una política de privacidad*: define expectativas de privacidad con respecto a funciones como monitoreo, registro de actividades y acceso a recursos de la red.

[26] http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad

- *Una política de acceso*: que permite definir derechos de acceso y privilegios para proteger los objetivos clave de una pérdida o exposición mediante la especificación de guías de uso aceptables para los usuarios con respecto a conexiones externas, comunicación de datos, conexión de dispositivos a la red, incorporación de nuevo software a la red, etc.

- *Una política de autenticación*: que establece un servicio de confiabilidad mediante alguna política de contraseñas o mecanismos de firmas digitales, estableciendo guías para la autenticación remota y el uso de dispositivos de autenticación.

- *Un sistema de IT y una política de administración de la red*: describe como pueden manipular las tecnologías los encargados de la administración interna y externa. De aquí surge la consideración de si la administración externa será soportada y, en tal caso, como será controlada.

4.1. CARACTERÍSTICAS

- Duración: 5 años
- Documento breve: 4 ó 5 planes
- Exige el compromiso de los usuarios
- No debe tener referencias a tecnología

4.2.GESTIÓN DE RIESGOS

- Coste asociado a los riesgos, en función de su probabilidad
- Coste asociado a las medidas de seguridad
- Gestión de riesgos: equilibrio entre coste protección y exposición
- Decisiones
- Aceptar riesgos
- Asignarlos a terceros

4.3. IMPLEMENTACIÓN

- Medidas transparentes a usuarios
- Fomentar cultura de seguridad entre usuarios
- Todo bien determinado en la política de seguridad

4.4. ESTRATEGIAS DE SEGURIDAD[27]

4.4.1. Mínimos privilegios

- Consiste en asignar a cada usuario el mínimo de privilegios que necesite.
- El objetivo es minimizar los daños en caso de que la cuenta de un usuario sea invadida.
- En caso de que un usuario quiera realizar actividades diferentes tiene que solicitar que se le asignen los privilegios correspondientes.

4.4.2. Defensa en profundidad

- Consiste en usar tantos mecanismos de seguridad como sea posible, colocándolos uno tras otro.
- Puede hacer muy compleja la utilización del sistema.

4.4.3. Check Point

- Se hace pasar todo el tráfico de la red por un solo punto y se enfocan los esfuerzos de seguridad en ese punto.
- Puede disminuir el rendimiento.

4.4.4. Falla en posición segura

- Los sistemas deben estar diseñados para que en caso de falla queden en un estado seguro.

[27] http://www.desarrolloweb.com/articulos/1592.php

4.4.5. Seguridad por Obscuridad

- La estrategia es mantener un bajo perfil y tratar de pasar desapercibido, de modo que los atacantes no lo detecten.

4.4.6. Simplicidad

- Los sistemas muy complejos tienden a tener fallas y huecos de seguridad.
- La idea es mantener los sistemas tan simples como sea posible, eliminando funcionalidad innecesaria.
- Sistemas simples que tienen mucho tiempo, han sido tan depurados que prácticamente no tienen huecos de seguridad.

4.4.7. Seguridad basada en hosts

- Los mecanismos de seguridad están en los hosts.
- Puede ser diferente en cada host, lo cual hace difícil su instalación y mantenimiento.
- Si un host es atacado con éxito, peligra la seguridad de la red (muchos usuarios tienen el mismo *login* y *password* en todos los hosts a los que tienen acceso).

4.5. POLÍTICA DE SEGURIDAD PARA REDES CABLEADAS E INALÁMBRICAS[28]

El primer elemento para iniciar una infraestructura de seguridad en las redes cableadas e inalámbricas es el diseño apropiado de políticas de seguridad tales como:

- Aceptación de dispositivos, Registro, Actualización y Monitoreo
- Educación del usuario y Responsabilidad
- Seguridad Física
- Perímetro de Seguridad Física

[28] http://www.xbackup.net/spanish/Pol%C3%ADticas-de-Seguridad.html

- Desarrollo de la Red y posicionamiento
- Medidas de Seguridad
- Monitoreo de la Red y Respuesta a Incidentes

4.5.1. Recomendaciones de seguridad

Como en cualquier red de comunicaciones, las WLAN son un punto más de riesgo que debe ser correctamente protegido y administrado dentro del conjunto de la infraestructura de una organización. Sin embargo, la particularidad del medio de transmisión empleado las hace más susceptibles a los ataques externos por la facilidad de acceso a la información que se transmite.

Entre las posibles medidas que se pueden tomar en una red inalámbrica, se encuentran:

a. Utilizar WEP. Aunque su grado de seguridad es cuestionado, ofrece un mínimo de privacidad. Siempre será mejor que nada.

b. Emplear, si los dispositivos lo permiten, el protocolo WPA que permite la renovación automáticas de las claves de encriptación.

c. Inhabilitar el servicio de DHCP para las redes dinámicas si no es estrictamente necesario.

d. Mantener actualizados el fireware de los dispositivos para cubrir posibles agujeros en las diferentes soluciones wireless, con especial atención en los Puntos de Acceso.

e. Utilizar Listas de Control de Acceso (ACL) de direcciones MAC, que permiten restringir los dispositivos clientes que pueden acceder a la red inalámbrica. La práctica totalidad de los Puntos de Acceso comerciales poseen esta funcionalidad.

f. Proporcionar un entorno físico seguro a los Puntos de Acceso y desactivarlos cuando se presentar periodos prolongados de inactividad.

g. Cambiar el SSID por defecto que proporcionan los Puntos de Acceso, conocidos por todos: tsunami para Cisco, intel para Intel, etc.

h. Inhabilitar la emisión broadcast del SSID.

i. Reducir la propagación de ondas de radio fuera del área de cobertura. Por ejemplo, evitando que salga al exterior de los edificios.

j. Utilizar medidas de seguridad de red comunes como SSL, VPN, Firewalls.

7. EVALUACION DEL OBJETO DE INVESTIGACION

Una vez realizado el desarrollo de la presente investigación, es pertinente realizar la evaluación de cumplimiento de los diferentes objetivos planteados al inicio del desarrollo de la tesis.

- **Objetivo Específico 1**

Evaluar la situación actual de la red: aplicabilidad y uso, tecnología, equipamiento, topología.

Para dar cumplimiento al presente objetivo se realizó un análisis exhaustivo de la situación actual de intranet de la Universidad Nacional de Loja, tecnología, equipamiento: que trae consigo la instalación del servidor de seguridad para la intranet de la Universidad Nacional de Loja, para de esta manera determinar que es posible utilizar para implementar dicha tecnología de seguridad en la institución.

- **Objetivo Especifico 2**

Analizar los mecanismos de seguridad que incorporen sistemas de autenticación, autorización y Administración (AAA) para redes de datos que puedan ser implementados en la Universidad Nacional de Loja.

La recolección de información: archivos pdf, artículos científicos, diapositivas y más fuentes, como la observación y la práctica fueron herramientas fundamentales para el desarrollo de este objetivo; algunos de estos instrumentos se encontraron en internet de donde se obtuvo las direcciones necesarias para descargar algunos mecanismos de seguridad, así como todo el material bibliográfico de apoyo para el desarrollo de la investigación.

- **Objetivo Especifico 3**

Seleccionar la mejor alternativa en cuanto a mecanismos de seguridad, en base a los requerimientos y prestaciones del Área de Energía las Industrias y Recursos Naturales no Renovables.

Luego de aplicar diversas técnicas y metodologías de investigación para recabar información sobre los mecanismos de seguridad, se efectuó cuadros comparativos sobre los diferentes estándares aptos para el funcionamiento en redes de datos; estos cuadros comparativos permitieron determinar que el estándar IEEE 802.1x para redes de datos cableadas y el estándar IEEE 802.1x para redes wifi, es el más óptimo por su simplicidad y adaptación es el más adecuado para establecer conexiones.

- **Objetivo Especifico 4:**

Generar el manual de políticas de seguridad.

Para generar el manual de políticas de seguridad nos basamos en los mecanismos de seguridad implementados como el uso de contraseñas seguras, la Encriptación WPA, el establecimiento de permisos y las VPN, así como una serie de políticas de seguridad a tomarse en cuenta para el debido acceso a la red a través de usuarios definidos en tres grupos: administrativos, docentes y alumnos, para brindar una mejor seguridad en el acceso del Internet.

- **Objetivo Especifico 5:**

Implementar el esquema de seguridad planteado, en el Área de Energía las Industrias y Recursos Naturales no Renovables como plan piloto

Luego de haber investigado acerca de los requerimientos de hardware y de las configuraciones de los servidores a implementar, se procedió a verificar que se cuente con los recursos debidamente calificados para llevar a cabo esta implementación o si se

requería adquirir los servicios de un tercero, una vez que se contó con los recursos y se cumplieron con los requerimientos técnicos, se procedió a realizar la implementación considerando todos los componentes que intervienen en este proceso, y de esta manera establecer que procedimientos, cómo y cuando se desarrollaran y así informarlo, pedir autorización y evitar impactos negativos considerables.

- **Objetivo Especifico 6:**

Evaluar el esquema de seguridad a implementar.

Luego de haber configurado el servidor RADIUS, para la autenticación en la red inalámbrica del Área de Energía, Industrias y Recursos Naturales no Renovables de la Universidad Nacional de Loja, se planteó encuestas a los usuarios, para poder determinar el grado de satisfacción que tuvieron al utilizar dicho sistema.

8. DESARROLLO DE LA PROPUESTA ALTERNATIVA

8.1. INTRODUCCIÓN

Para dar cumplimiento a los objetivos planteados proponemos la siguiente solución que permitirá al usuario poder acceder a la red pública para Internet del Área de Energía, Industrias y Recursos Naturales no Renovables, en forma controlada cumpliendo así con la norma de validación por usuario y contraseña.

Aquí se describe la configuración de software y hardware necesario para la instalación del servidor Freradius y LDAP; y la conexión con el Acces Point Wireless Dlink-3200 del Área de Energía, Industrias y Recursos Naturales no Renovables.

Referente al software, se describe los paquetes para la instalación de Freeradius en el servidor, los ajustes necesarios en los archivos de configuración.

8.2. EVALUACION DE LA SITUACIÓN ACTUAL DE LA RED: APLICABILIDAD, USO Y TECNOLOGIA DE LA UNIVERSIDAD NACIONAL DE LOJA

8.2.1. Análisis de la Situación Actual

La Universidad Nacional de Loja, se encuentra ubicada al sur de la ciudad de Loja en el sector “La Argelia” ciudadela Universitaria. Esta Institución está formada por cinco Áreas Académico – Administrativas que se encuentran localizadas en un solo espacio físico.

La infraestructura de las Áreas, está destinada para el alojamiento de equipos, oficinas administrativas y aulas de clases, es decir, sus instalaciones están diseñadas para el desempeño de una institución educativa.

El Departamento de Jefatura de Informática es el ente autorizado de la administración y gestión de la red. Se encarga de la instalación de software, actualizaciones de antivirus, administración de las claves de configuración de equipos de red y de computación, tanto para el sector administrativo como estudiantil de toda la Universidad.

El Cuarto de equipos de la red de toda la Universidad, se encuentra Ubicado en la sección de Redes del Departamento de Jefatura de Informática, desde este departamento se administra y distribuye el internet hacia las demás Áreas; mientras que en el resto de áreas los equipos de red se localizan en los denominados *puntos de distribución (Centros de Computo),* que son sectores de trabajo no apropiados para el alojamiento de equipos, ya que no cuentan con la infraestructura adecuada (ambientes de acceso restringidos, control de temperatura, etc.) de un cuarto de equipos o de telecomunicaciones.

8.2.2. Análisis de los resultados obtenidos en las encuestas realizadas a los responsables de los centros de cómputo de la Universidad Nacional de Loja

Aquí se planteó una encuesta acerca de la seguridad informática aplicada al personal de los centros de cómputo de los siguientes departamentos: **(Para mayor detalle revisar anexo # 2 donde se encuentran las encuestas dirigidas a encargados de los centros de computos)**

- Jefatura de Informática
- Área de Energía, Industrias y Recursos Naturales no Renovables
- Área Jurídica, Social y Administrativa
- Área Agropecuaria y de Recursos Naturales Renovables
- Área de la Educación, el Arte y la Comunicación
- Área de la Salud Humana

Obteniendo los siguientes resultados:

1. **¿De quién depende la responsabilidad de la seguridad informática en la Institución?**

Tabla 8.1 Resultados Pregunta 1

ALTERNATIVAS	FRECUENCIA	%
Auditoría Interna	0	0
Jefatura Informática	9	90
Departamento de Finanzas	0	0
No se tiene específico formalmente	1	10
TOTAL	**10**	**100**

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

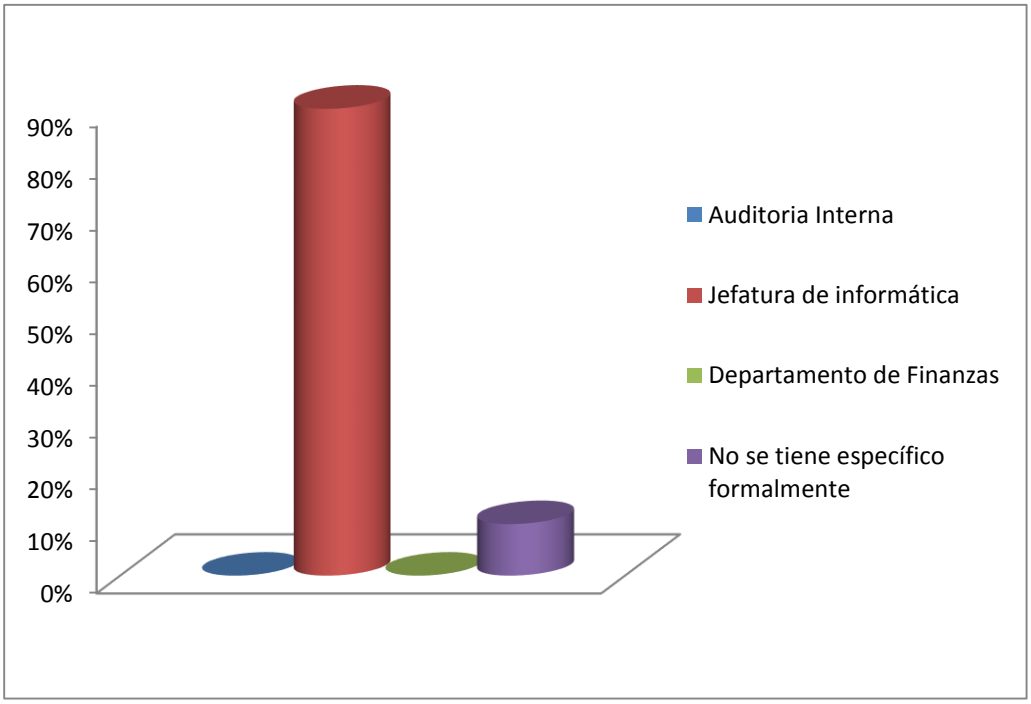


Figura 8.1 Resultado Pregunta 1
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior concluimos que el 90% de los encuestados dicen que la responsabilidad de la seguridad informática en la Institución recae en la jefatura Informática y que el 10% restante no tienen específico formalmente. Ninguno de los encuestados responde que el manejo de la seguridad informática en la Institución este dada por auditoría Interna y por el Departamento de finanzas

2. El presupuesto de la Institución incluye aspectos de seguridad informática.

Tabla 8.2 Resultados Pregunta 2

ALTERNATIVAS	FRECUENCIA	%
Si	1	10
No	9	90
TOTAL	**10**	**100**

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

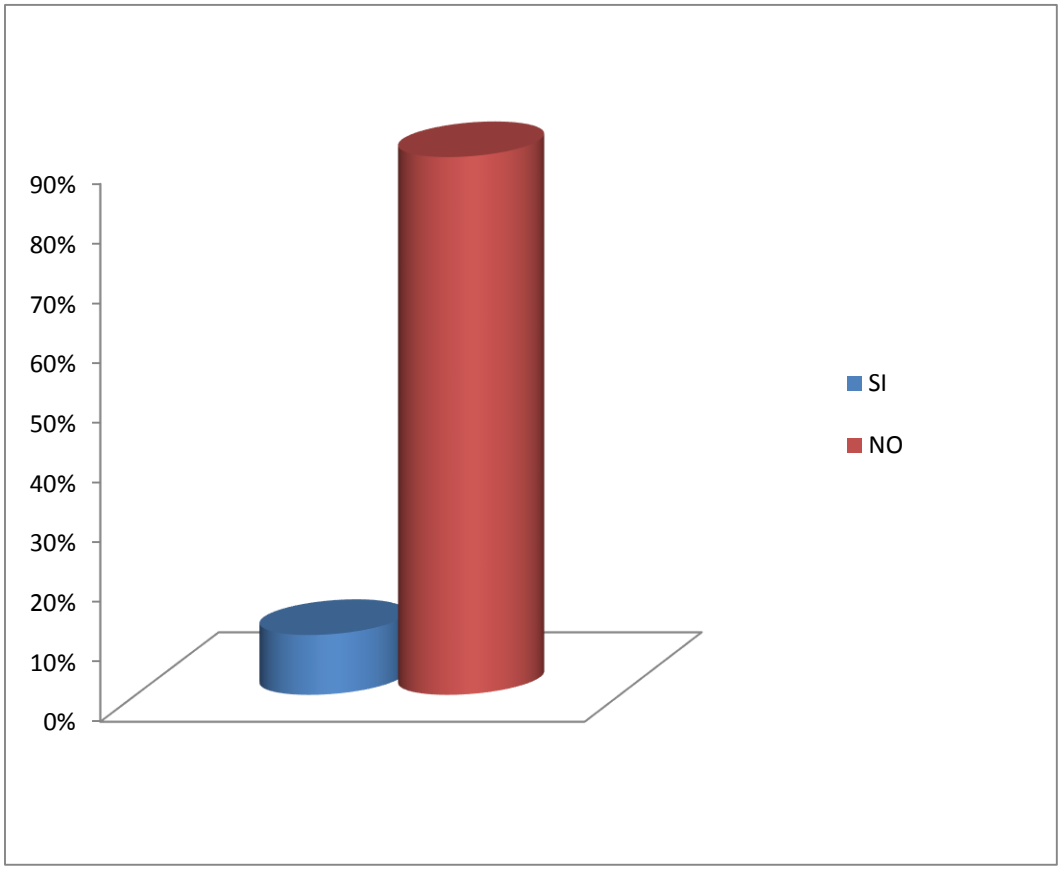


Figura 8.2 Resultado Pregunta 2
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior concluimos que el 90% de los encuestados dice q el presupuesto de la Institución no incluye aspectos de seguridad informática y que el 10% restante dice q el presupuesto de la Institución si incluye aspectos de seguridad informática.

3. **¿En qué se centra la seguridad informática en la Institución? (Elija todas las que se apliquen).**

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

Tabla 8.3 Resultados Pregunta 3

ALTERNATIVAS	FRECUENCIA	%
Protección de la red	7	26,92
Protección de los datos críticos de la Institución	8	30,77
Proteger el almacenamiento de los datos de los estudiantes	6	23,07
Desarrollo y afinamiento de seguridad de las aplicaciones	4	15,38
Otras	1	3,85
TOTAL	**26**	**100**

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

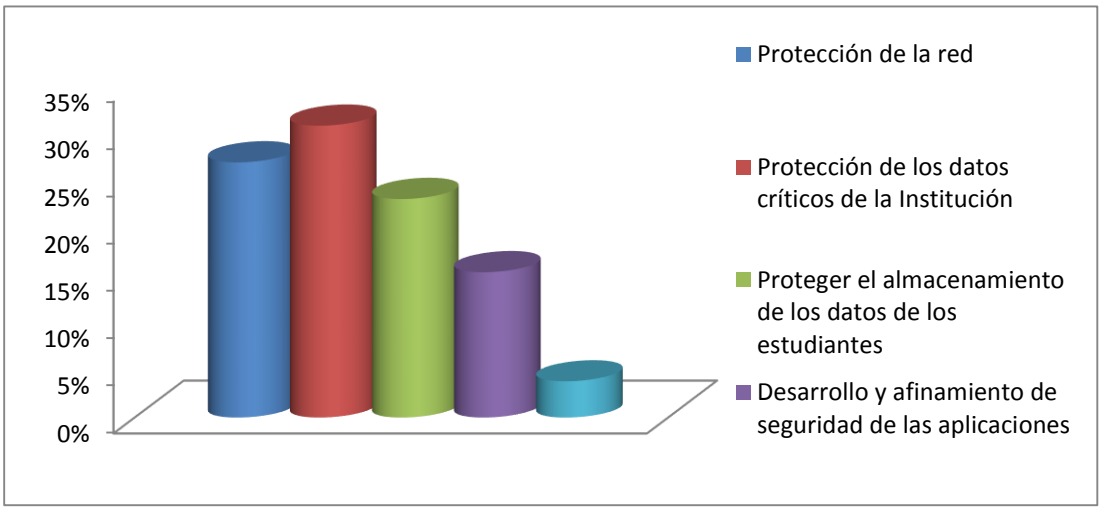


Figura 8.3 Resultado Pregunta 3
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior concluimos que el 30.77% de los encuestados opina que la seguridad informática se centra en la protección de los datos críticos de la institución, el 26.92% responde que la seguridad informática se centra en la protección de la red, el 23.07% restante contesta que la seguridad informática se centra en proteger el almacenamiento de los datos de los estudiantes, el 15.30% contesta que la seguridad informática se centra en el desarrollo y afinamiento de seguridad de las aplicaciones y el 3,85% opina que existen otros campos en los cuales se debe centrar la seguridad informática como:

- Protección de contenidos

4. **¿Qué casos de violación de seguridad tuvieron lugar en la Institución? (Elija todas las respuestas aplicables).**

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

Tabla 8.4 Resultados Pregunta 4

ALTERNATIVAS	FRECUENCIA	%
Manipulación de aplicaciones de Software	0	0
Accesos no Autorizados	5	20,8
Virus	9	37,5
Robo de datos	1	4,16
Monitoreo no autorizado de tráfico	3	12,5
Negación del Servicio	5	20,8
Pérdida de Integridad	1	4,16
Pérdida de Información	0	0
Ninguno	0	0
Otros	0	0
TOTAL	24	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

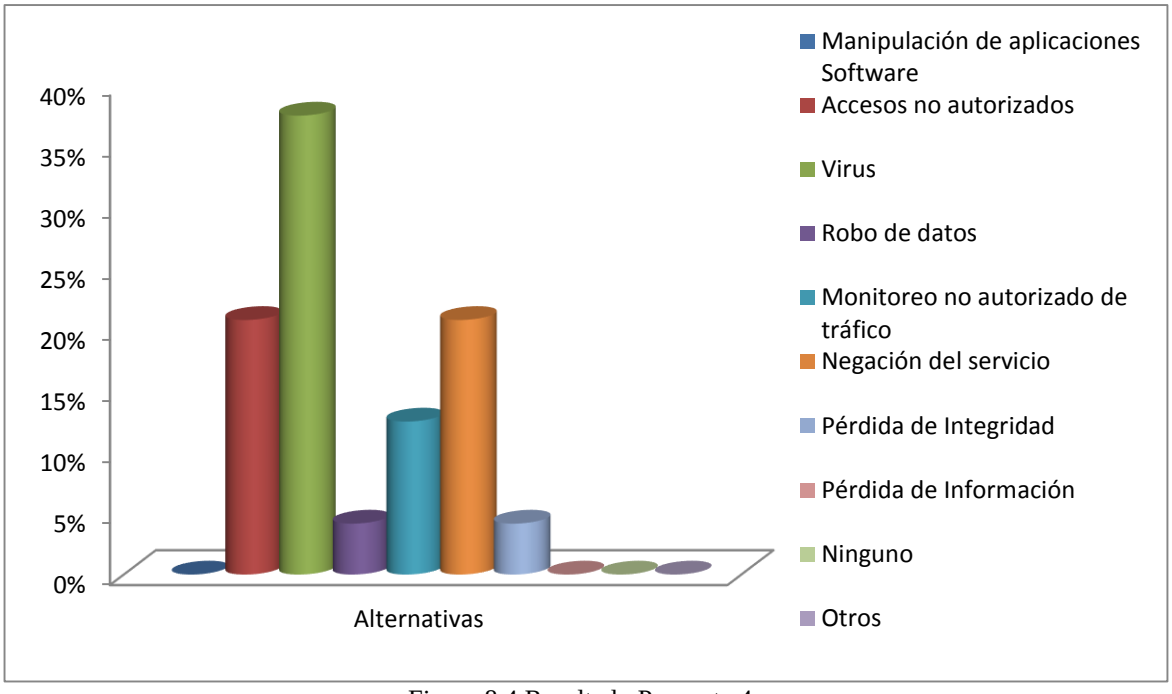


Figura 8.4 Resultado Pregunta 4
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 37.5% de los encuestados opina que las violaciones de seguridad se deben a los Virus, el 20.8% responde que las violaciones de seguridad se deben a accesos no autorizados, el 20.8% contesta que las violaciones de seguridad se deben a la negación del servicio, el 12.5% dice que las violaciones de seguridad se deben al monitoreo no autorizado del tráfico, el 4.16% considera que las violaciones de seguridad se deben al robo de datos, el 4.16% piensa que las violaciones de seguridad se deben a la pérdida de la Integridad. Ninguno de los encuestados responde que las violaciones de seguridad se deben a la manipulación de aplicación de software, a la pérdida de la información, ninguna y otra.

5. **¿Cuántas intrusiones o incidentes de seguridad identifico en promedio durante el periodo anterior?**

Tabla 8.5 Resultados Pregunta 5

ALTERNATIVAS	FRECUENCIA	%
Ninguna	5	50
Entre 1-3	2	20
Entre 4-7	2	20
Más de 7	1	10
No sabe	0	0
No responde	0	0
TOTAL	**10**	**100**

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

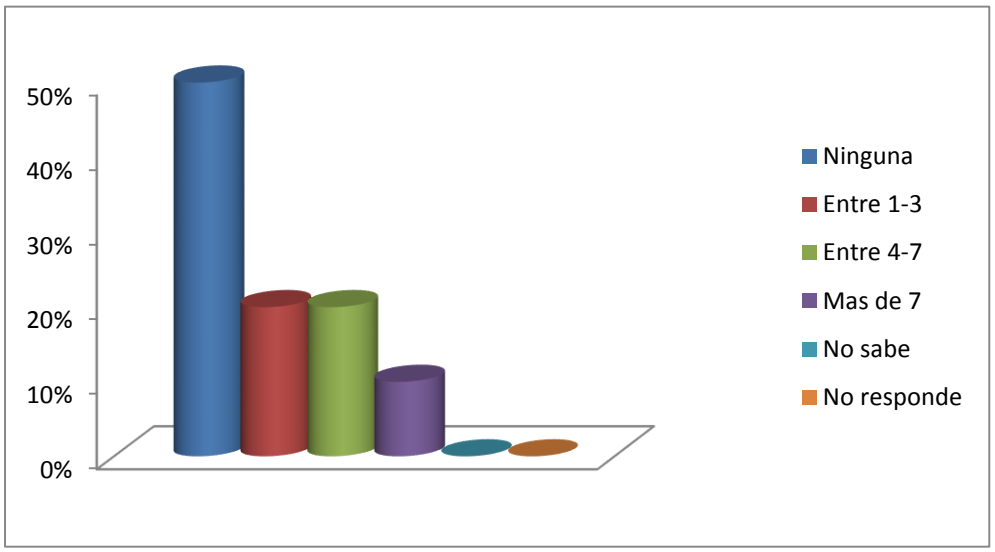


Figura8.5 Resultado Pregunta 5
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 50% de los encuestados opina que los no se dieron incidentes de seguridad en el período pasado, el 20% responde que en el período pasado se dieren entre 1-3 incidentes de seguridad, el 20% contesta que en el período pasado se dieren entre 4-7 incidentes de seguridad, el 10% dice que en el período pasado se dieren entre más de 7 incidentes de seguridad. Ninguno de los encuestados responde que no saben si se dieron incidentes de seguridad en el período pasado.

6. Una vez que ocurre la violación de seguridad esta se notifica a:

Tabla 8.6 Resultados Pregunta 6

ALTERNATIVAS	FRECUENCIA	%
Asesor Legal	0	0
Autoridades Locales	0	0
Departamento de Informática	7	70
Ninguna, no se denuncia	2	20
Otro	1	10
TOTAL	**10**	**100**

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

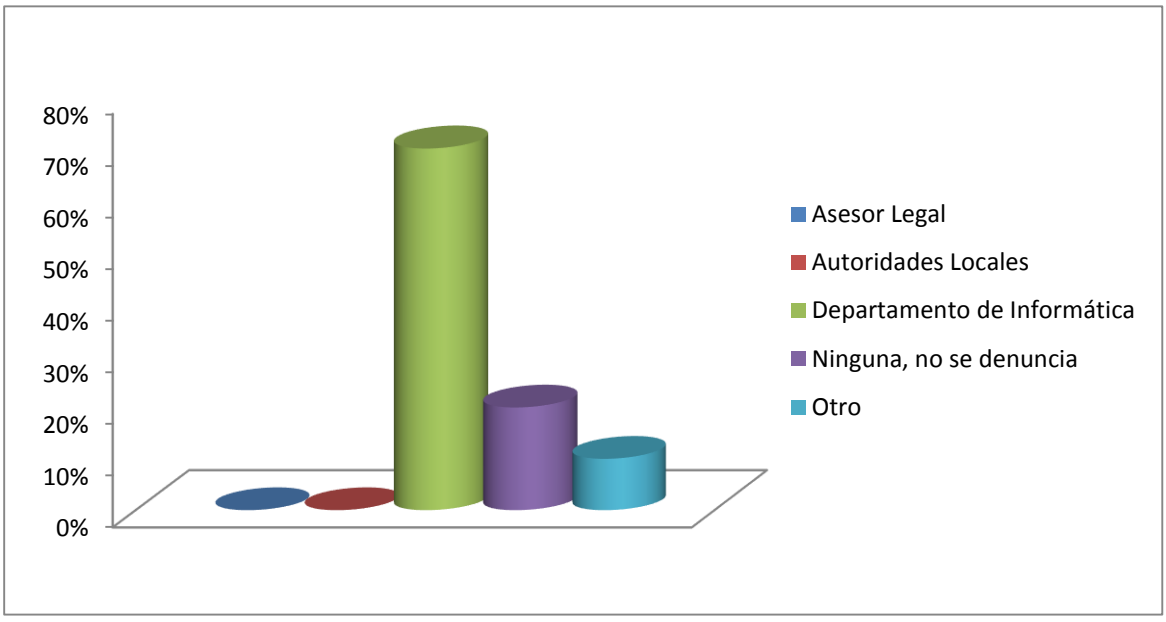


Figura 8.6 Resultado Pregunta 6
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 70% de los encuestados opina que las violaciones de seguridad que se notifican a el Departamento de Informática, el 20% responde que las violaciones de seguridad no se notifican, no se denuncian, Ninguno de

los encuestados responde que las violaciones de seguridad se notifican al Asesor legal o a las Autoridades locales. El 20% contesta opina que existen otros departamentos a los cuales denuncian las violaciones de seguridad como:

- El coordinador administrativo

7. ¿Cuántas pruebas de seguridad realiza la Institución para valorar el estado de seguridad informática?

Tabla 8.7 Resultados Pregunta 7

ALTERNATIVAS	FRECUENCIA	%
Una al año	4	40
Entre 2 y 4 al año	0	0
Más de 4 al año	1	10
Ninguna	5	50
TOTAL	10	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

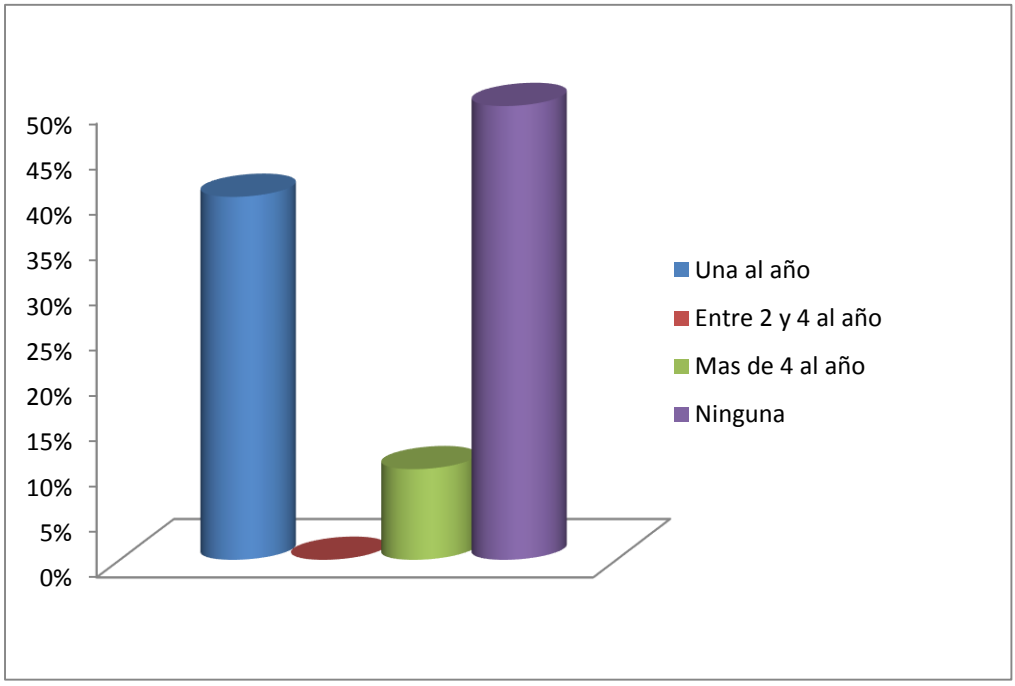


Figura 8.7 Resultado Pregunta 7
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 50% de los encuestados opina que no se realizan pruebas de seguridad en la Institución, el 40% responde que las pruebas de seguridad en

la Institución se dan una vez al año, el 10% contesta que las pruebas de seguridad en la Institución se dan más de cuatro al año. Ninguno de los encuestados responde que las pruebas de seguridad en la Institución se den entre dos y cuatro al año.

8. **¿Cuál de los siguientes mecanismos utiliza actualmente la Institución para proteger sus Sistemas de Información? (Elija todas las aplicables).**

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

Tabla 8.8 Resultados Pregunta 8

ALTERNATIVAS	FRECUENCIA	%
Smart Cards	0	0
Biometría	1	2,08
Antivirus	9	18,75
Autenticación, Autorización	3	6,25
Filtro de paquetes	3	6,25
Firewalls Hardware	5	10,42
Firewalls Software	5	10,42
Firmas digitales/certificados digitales	2	4,2
Redes privadas virtuales	4	8,33
Proxies	10	20,83
Sistema de detección de intrusos	1	2,08
Monitoreo	4	8,33
Ninguno	0	0
Otros	1	2,08
TOTAL	48	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

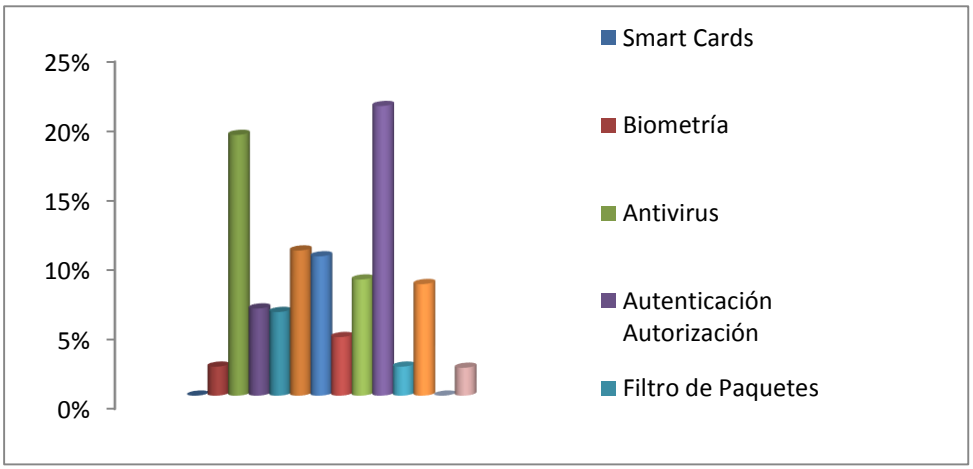


Figura 8.8 Resultado Pregunta 8
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 20.83% de los encuestados opina que la institución utiliza a los proxies como mecanismo para proteger sus sistemas de información, el 18.75% responde que la institución utiliza a los antivirus como mecanismo para proteger sus sistemas de información, el 10.42% contesta que la institución utiliza los firewalls Hardware como mecanismo para proteger sus sistemas de información, el 10.42% dice que la institución utiliza los firewalls software como mecanismo para proteger sus sistemas de información, el 8.33% piensa que la institución utiliza a las redes privadas virtuales como mecanismos para proteger sus sistemas de información, el 8.33% considera que la institución utiliza al monitoreo como mecanismo para proteger sus sistemas de información, el 6.25% cree que la institución utiliza a la Autenticación Autorización como mecanismos para proteger sus sistemas de información, el 6.25% opina que la institución utiliza al filtro de paquetes como mecanismos para proteger sus sistemas de información, el 4.2% responde que la institución utiliza las firmas digitales/certificados digitales como mecanismos para proteger sus sistemas de información, el 2.08% contesta que la institución utiliza la biometría como mecanismos para proteger sus sistemas de información, el 2.08% dice que la institución utiliza los sistemas de detección de intrusos como mecanismos para proteger sus sistemas de información. Ninguno de los encuestados responde que la Institución utiliza a los Smart Card como mecanismo para proteger sus sistemas de información. El 2.08% piensa que la institución debe utilizar otros mecanismos para proteger sus sistemas de información como:

- Iptables
- Hosts.allow
- Hosts.deny

9. ¿La Institución cuenta con políticas de seguridad de redes?

Tabla 8.9 Resultados Pregunta 9

ALTERNATIVAS	FRECUENCIA	%
No se tiene políticas de seguridad definidas	4	40
Actualmente se encuentra en desarrollo	3	30
Existe políticas formales, escritas documentadas e informadas a todos	3	30
TOTAL	10	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

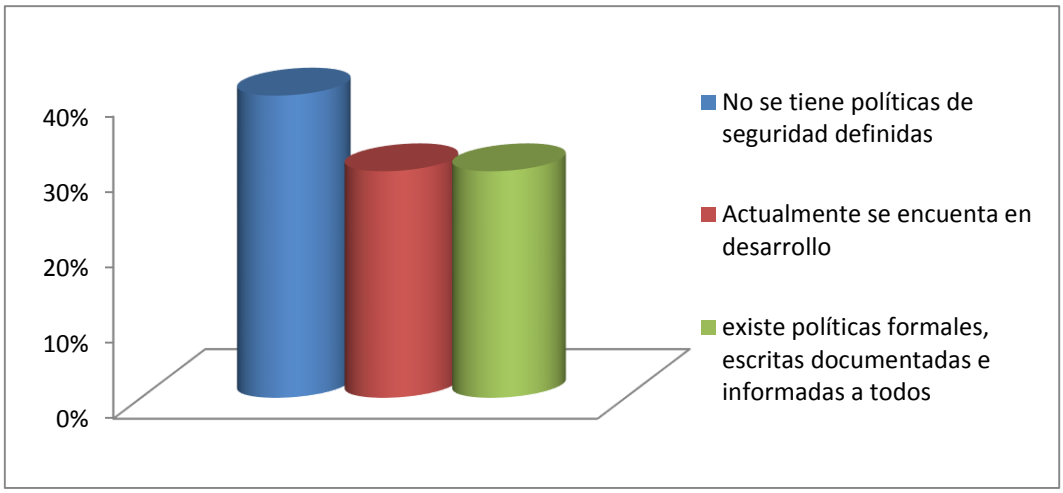


Figura 8.9 Resultado Pregunta 9
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 40% de los encuestados opina que la institución no tiene políticas de seguridad definidas, el 30% responde que las políticas de seguridad actualmente se encuentran en desarrollo y el 30% contesta que existen políticas formales, escritas documentadas e informadas a todos en la Institución.

10. ¿Cuáles de los siguientes es obstáculo principal para lograr una adecuada seguridad informática en la Institución?

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

Tabla 8.10 Resultados Pregunta 10

ALTERNATIVAS	FRECUENCIA	%
Inexistencias de políticas de seguridad	4	12,5
Falta de tiempo	3	9,37
Falta de formación técnica	4	12,5
Falta de apoyo de directivos	3	9,37
Falta de colaboración entre Áreas	3	9,37
Complejidad Tecnológica	1	3,12
Poco entendimiento de seguridad Informática	2	6,25
Falta de recursos	5	15,62
Falta de personal	7	21,87
Ninguno	0	0
TOTAL	32	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

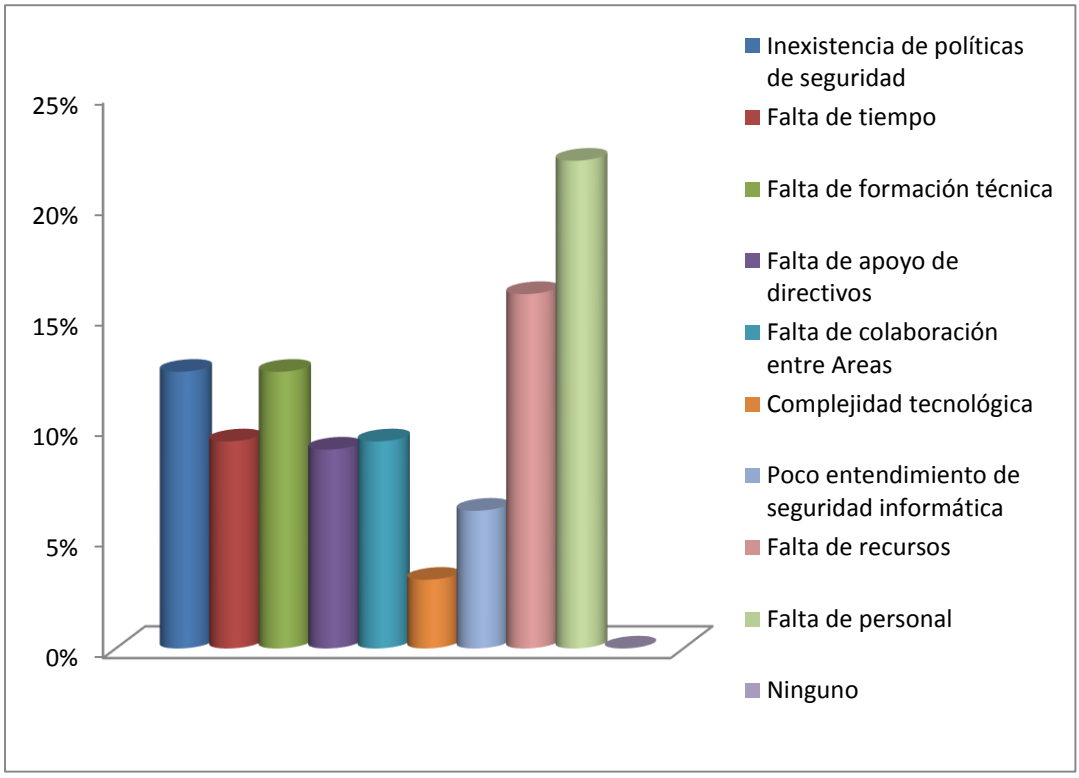


Figura 8.10 Resultado Pregunta 10
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 21.87% de los encuestados opina que la falta de personal es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 15.62% responde que la falta de recursos es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 12.5% contesta que la inexistencia de políticas es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 12.5% dice que la falta de formación técnica es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 9.37% piensa que la falta de tiempo es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 9.37% considera que la falta de apoyo de directivos es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 9.37% cree que la falta de colaboración entre Áreas es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 6.25% opina que el poco entendimiento de seguridad informática es obstáculo principal para lograr una adecuada seguridad informática en la Institución, el 3.12% responde que la complejidad tecnológica es obstáculo principal para lograr una adecuada seguridad informática en la

Institución. Ninguno de los encuestados responde que ninguno de los obstáculos anteriores sea principal para lograr una adecuada seguridad informática en la Institución.

11. ¿De las siguientes actividades de seguridad cuáles son realizadas en la Institución y cuáles son realizadas por personal externo?

Esta pregunta consta de dos partes, pero lo que se refiere con personal externo todas las respuestas son cero, solo se hace el cuadro de lo referente a la Institución, además es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

Tabla 8.11 Resultados Pregunta 11

ALTERNATIVAS	FRECUENCIA	%
Integración y pruebas de los planes de recuperación de información	1	5,26
Divulgación de aspectos relacionados con la seguridad	0	0
Manejo de incidentes y análisis de vulnerabilidades	1	5,26
Evaluación de seguridad	2	10,52
Seguimiento y monitoreo de actividades	3	15,79
Administración de seguridad	4	21,05
Configuraciones técnicas	8	42,11
TOTAL	19	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

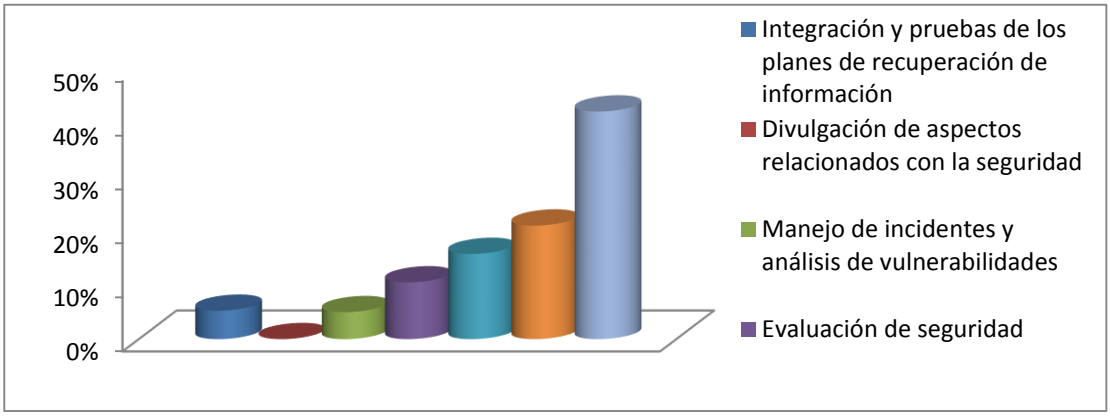


Figura 8.11 Resultado Pregunta 11
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 42.11% de los encuestados opina que las configuraciones técnicas son actividades realizadas por la institución, el 21.05%

contesta que la administración de seguridad es una actividad realizada por la institución, el 15.79% dice que el seguimiento y monitoreo de actividades es una actividad realizada por la institución, el 10.52% piensa que la evaluación de seguridad es una actividad realizada por la institución, el 5,26% considera que la integración y pruebas de los planes de recuperación de información es una actividad realizada por la institución, el 5.26% cree que el manejo de incidentes de seguridad y análisis de vulnerabilidades es una actividad realizada por la institución. Ninguno de los encuestados responde que la divulgación de aspectos relacionados con la seguridad sea una actividad realizada por la institución.

Ninguno de los encuestados describe que las actividades antes mencionadas sean realizadas por personal externo a la institución.

12. ¿Con que frecuencias se hacen las revisiones de seguridad de activos de información?

Tabla 8.12 Resultados Pregunta 12

ALTERNATIVAS	FRECUENCIA	%
Anual	0	0
Semestral	2	20
Eventual	4	40
Nunca	4	40
TOTAL	10	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

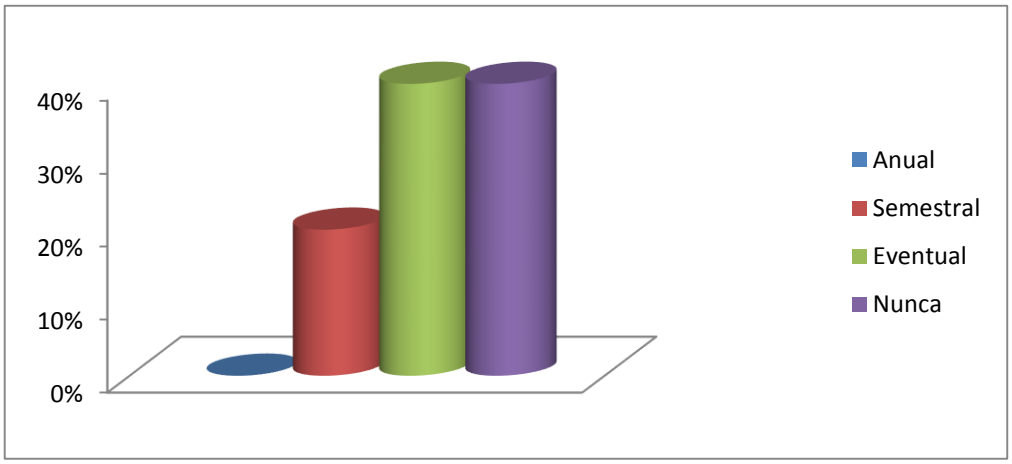


Figura 8.12 Resultado Pregunta 12
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 40% de los encuestados opina que las revisiones de seguridad de activos de información se hacen eventualmente, el 40% responde que las revisiones de seguridad de activos de información no se hacen nunca y el 20% contesta que las revisiones de seguridad de activos de información se hacen semestralmente. Ninguno de los encuestados opina que las revisiones de seguridad de activos de información se hagan anualmente.

13. Dentro de la Institución, ¿Cuáles de los siguientes aspectos son de mayor preocupación en el área de seguridad?

La pregunta es de opción múltiple, debido a esto el número total de encuestados no es igual al número de respuestas.

Tabla 8.13 Resultados Pregunta 13

ALTERNATIVAS	FRECUENCIA	%
Informática móvil	1	4
Memoria extraíble	6	24
Redes Inalámbricas	10	40
Telefonía voz sobre IP	1	4
Servidores	7	28
Ninguno	0	0
Otros	0	0
TOTAL	25	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

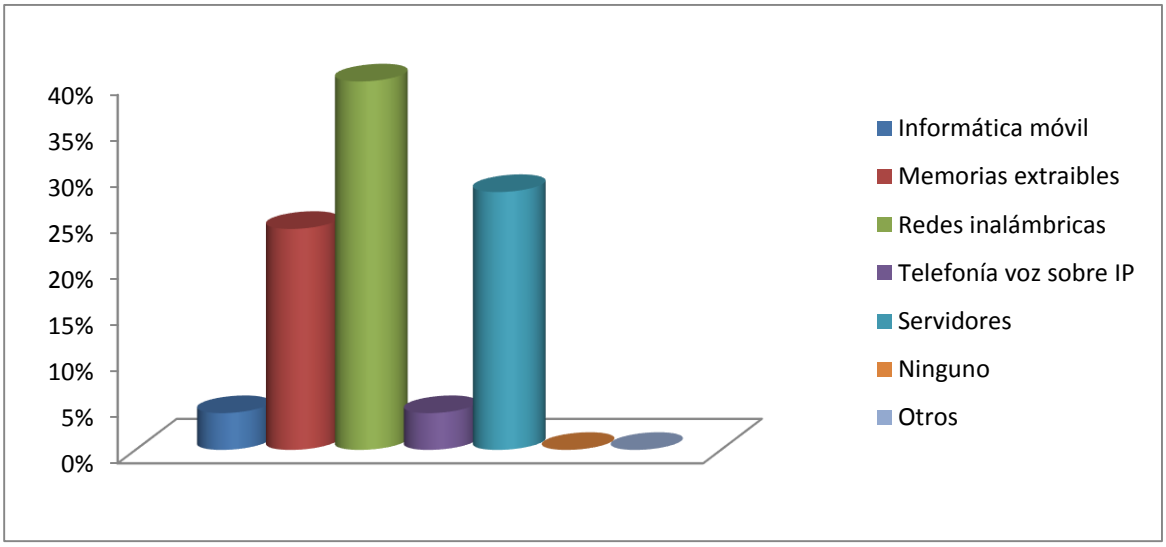


Figura 8.13 Resultado Pregunta 13
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 40% de los encuestados opina que las redes inalámbricas es el aspecto de mayor preocupación en el área de seguridad, el 28% contesta que los servidores es el aspecto de mayor preocupación en el área de seguridad, el 24% dice que las memorias extraíbles es el aspecto de mayor preocupación en el área de seguridad, el 4% piensa que la informática móvil es el aspecto de mayor preocupación en el área de seguridad, el 4% considera que la telefonía voz sobre IP es el aspecto de mayor preocupación en el área de seguridad. Ninguno de los encuestados considera que ninguno de los anteriores sea el aspecto de mayor preocupación en el área de seguridad o que existan otros aspectos.

14. ¿Cuáles de los siguientes mecanismos de protección a nivel de transporte utilizan?

Tabla 8.14 Resultados Pregunta 14

ALTERNATIVAS	FRECUENCIA	%
Protocolo de transporte secure sockets layer (SSL)	1	10
Transport layer security (TLS)	0	0
Wireless transport layer security (WTLS)	2	20
Ninguno	6	60
Otras	1	10
TOTAL	10	100

Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

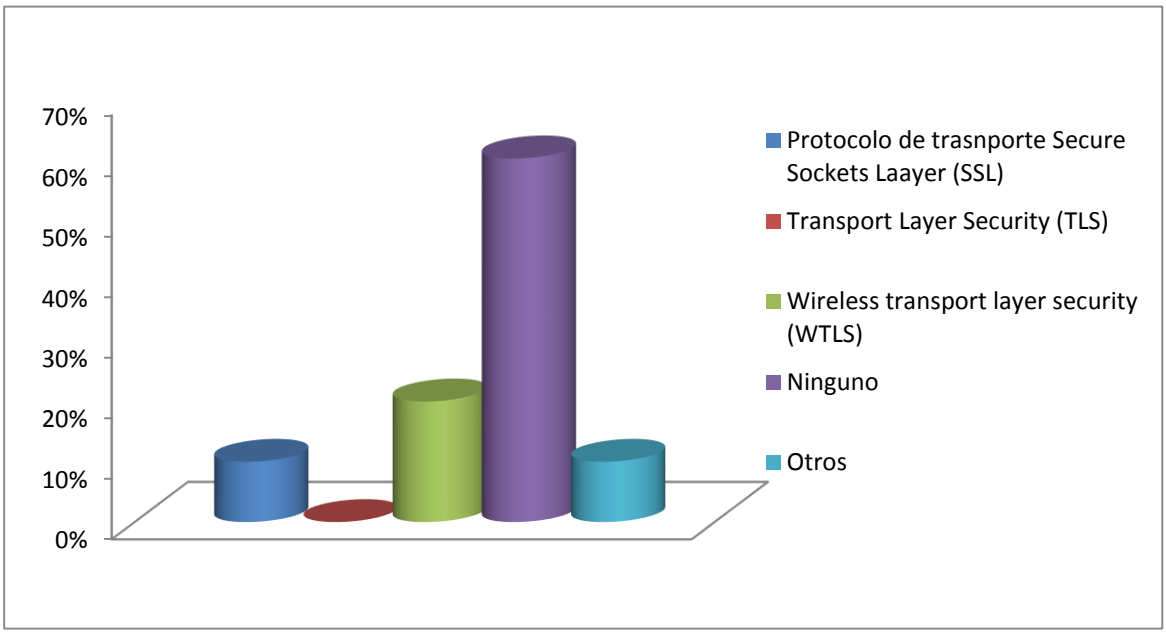


Figura 8.14 Resultado Pregunta 14
Fuente: Encuesta a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 50% de los encuestados opina que no se utilizan mecanismos de protección a nivel de transporte, el 20% responde que se utiliza el Wireless transport security (WTLS) como mecanismo de protección a nivel de red. Ninguno de los encuestados opina que se utilice Trasport layer secutiry (TLS) como mecanismo de protección a nivel de red. El 20% piensa que se deben utilizar otros mecanismos para la protección a nivel de red como:

- Seguridad wep[29]

8.2.3. Análisis de los resultados obtenidos en las entrevistas realizadas a los responsables de los centros de cómputo de la Universidad Nacional de Loja

Aquí se planteó una entrevista acerca de la seguridad informática aplicada al personal de los centros de cómputo de los siguientes departamentos: **(Para mayor detalle revisar anexo # 3 donde se encuentran las entrevistas dirigidas a encargados de los centros de computos)**

- Jefatura de Informática
- Área de Energía, Industrias y Recursos Naturales no Renovables
- Área de la Educación, el Arte y la Comunicación
- Área de la Salud Humana

Cabe mencionar que en el Área Jurídica, Social y Administrativa no se realizo dicha entrevista, debido a que no había una persona encargada de forma general de los centros de cómputo y los responsables de dichos centros eran personas que no conocían de la materia por eso se limitaron a no dar la entrevista.

Además en el Área Agropecuaria y de Recursos Naturales Renovables tampoco se realizo la entrevista, debido a que el encargado del centro de cómputo no se encontraba en la ciudad y no se realizo dicha entrevista.

De las entrevistas realizadas se obtuvieron los siguientes resultados:

[29] WEP: (Wired Equivalente Privacy: Privacidad equivalente al cable)

1. ¿Qué entiende usted sobre Seguridad Informática?

Tabla 8.15 Resultados Pregunta 1

ALTERNATIVAS	FRECUENCIA	%
Conoce bastante	3	60
Conoce poco	1	20
No conoce	1	20
TOTAL	5	100

Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

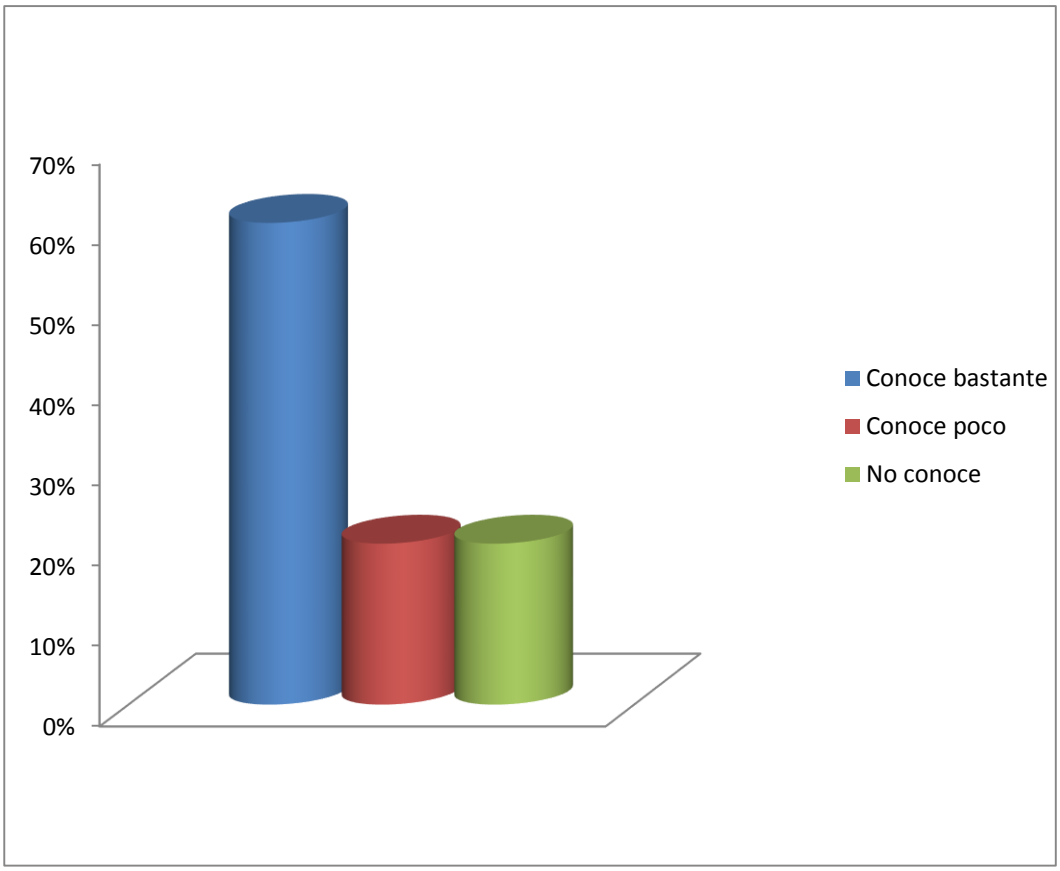


Figura 8.15 Resultado Pregunta 1
Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 60% de los entrevistados si conoce sobre lo que la seguridad informática, el 20% cono ce poco acerca de lo que refiere a la seguridad informática y el otro 20% de los entrevistados no conoce sobre dicho tema.

2. ¿Qué medidas implementaría usted para tener una mayor seguridad de los datos tanto inalámbrica como alámbricamente?

La pregunta es de varios criterios, debido a esto el número total de entrevistados no es igual al número de respuestas.

Tabla 8.16 Resultados Pregunta 2

ALTERNATIVAS	FRECUENCIA	%
VPN	2	22,2
Servidor radius	2	22,2
Cisco Pix	1	11,1
Monitoreo Correctivo y Preventivo de la red	1	11,1
Software con licencia	1	11,1
Servidores (web y proxi) de buena calidad	1	11,1
Crear esquemas de las redes existentes	1	11,1
TOTAL	9	100

Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

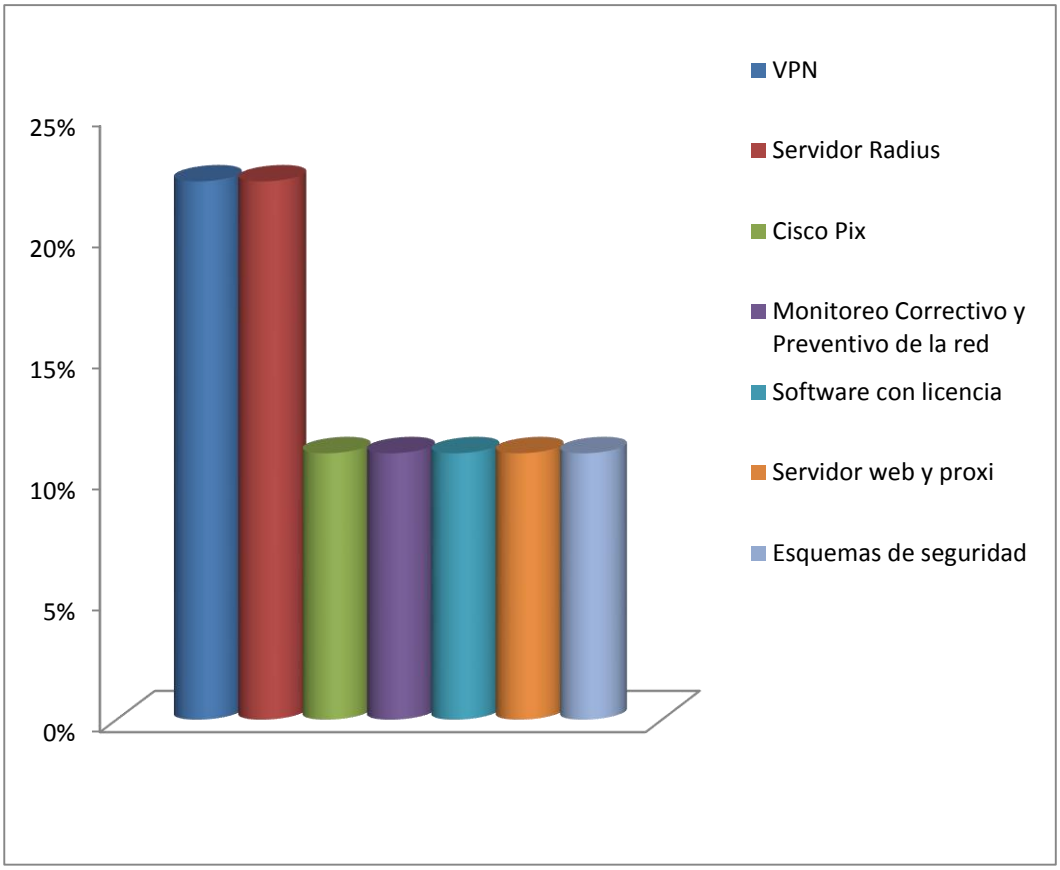


Figura 8.16 Resultado Pregunta 2
Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 22% de los entrevistados afirman que las medidas a implementar para tener una mayor seguridad de los datos en la intranet son las VPN, el 22% contesta que los servidores radius son de importancia a implementar para la seguridad de la intranet, el 11% dice que los Cisco Pix son de importancia a implementar para la seguridad de la intranet, el 11% piensa que el monitoreo correctivo y preventivo de la red son de importancia a implementar para la seguridad de la intranet, el 11% considera que el Software con licencia son de importancia a implementar para la seguridad de la intranet, el 11% aseveran que los servidores web y proxi son de importancia a implementar para la seguridad de la intranet y el 11% afirma que los esquemas de seguridad son de importancia a implementar para la seguridad de la intranet.

3. ¿Qué tipo de mecanismos de seguridad informática se ejecutan en la actualidad?

La pregunta es de varios criterios, debido a esto el número total de entrevistados no es igual al número de respuestas.

Tabla 8.17 Resultados Pregunta 3

ALTERNATIVAS	FRECUENCIA	%
Firewalls	1	12,5
Acceso web (Protocolos SSL[30] en el SGA[31])	1	12,5
Encriptación wep	1	12,5
Iptables	1	12,5
Host-deny	1	12,5
Monitoreo y gestión de redes	1	12,5
Mac Address	1	12,5
No existen	1	12,5
TOTAL	8	100

Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

[30] SSL: Secure Socket Layer

[31] SGA: Sistema de Gestión Académica de la Universidad Nacional de Loja

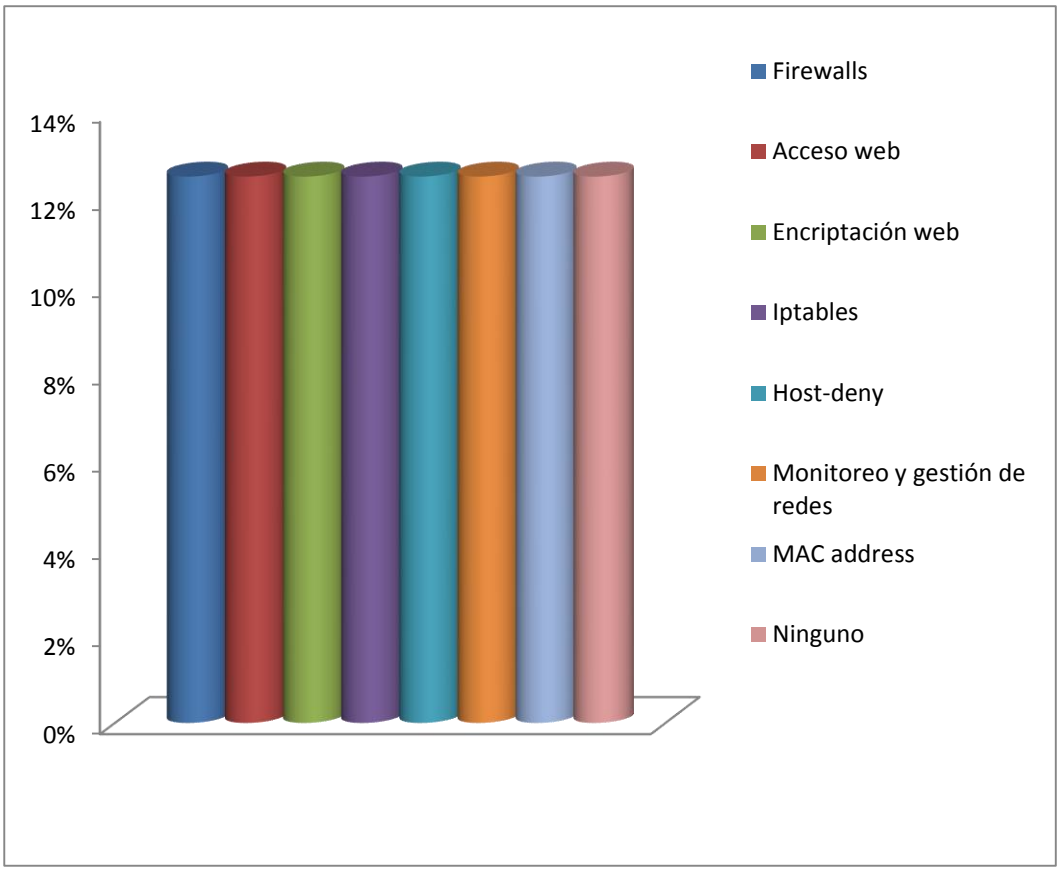


Figura 8.17 Resultado Pregunta 3
Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 12,5% de los entrevistados afirman que el firewall es un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% contesta que los Accesos web servidores son un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% dice que la encriptación web es un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% piensa que los Iptables son un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% considera que los host-denny son un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% aseveran que el monitoreo y gestión de redes es un mecanismo de seguridad que se ejecuta en la actualidad, el 12,5% afirma que las MAC Address son un mecanismo de seguridad que se ejecuta en la actualidad y por último un 12.5% niega la existencia de un mecanismo de seguridad que se ejecute en la actualidad

4. ¿Qué opina acerca del control de acceso (Autenticación, Autorización) en redes de datos?

Tabla 8.18 Resultados Pregunta 4

ALTERNATIVAS	FRECUENCIA	%
Conoce bastante	3	60
Conoce poco	1	20
No conoce	1	20
TOTAL	5	100

Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

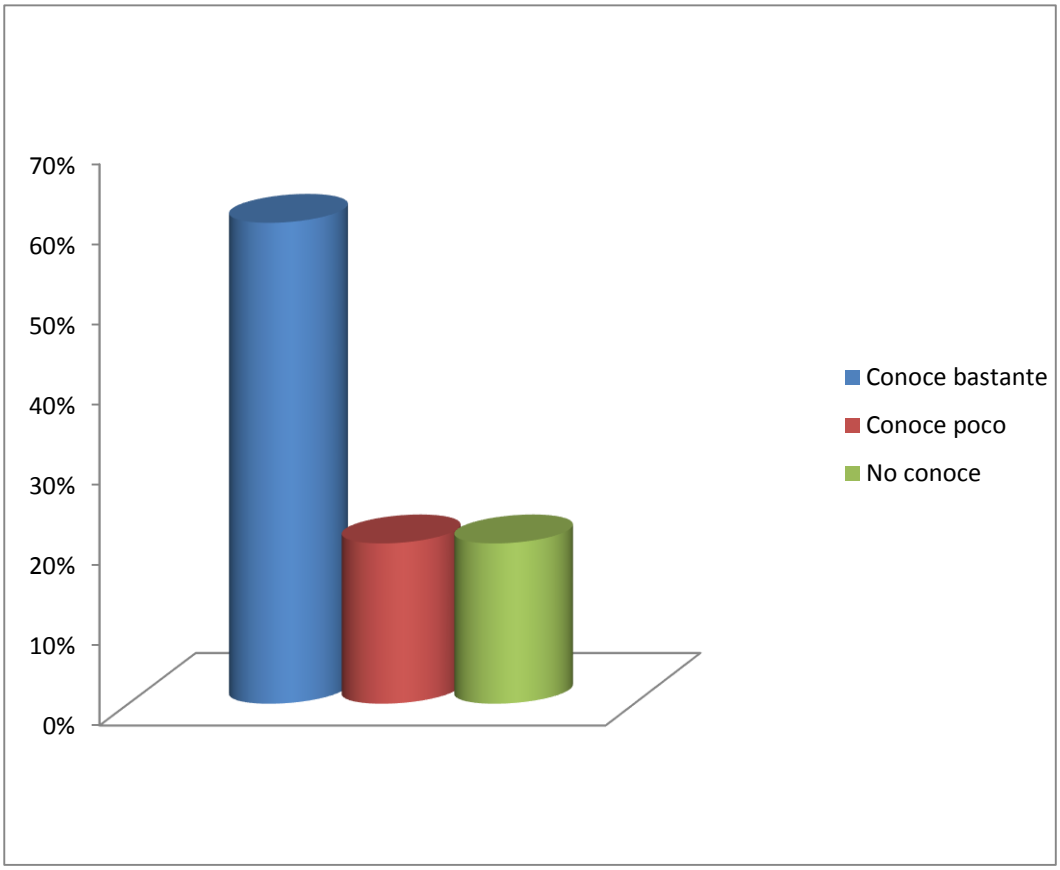


Figura 8.18 Resultado Pregunta 4
Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 60% de los entrevistados si conoce sobre lo que es el control de acceso en redes de datos, el 20% conoce poco acerca de lo que refiere al control de acceso en redes de datos y el otro 20% de los entrevistados no conoce sobre dicho tema.

5. **¿Considera usted que la seguridad en la red inalámbrica y alámbrica, implementada en la Universidad Nacional de Loja es segura?**

Tabla 8.19 Resultados Pregunta 5

ALTERNATIVAS	FRECUENCIA	%
SI	1	20
NO	4	80
TOTAL	5	100

Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

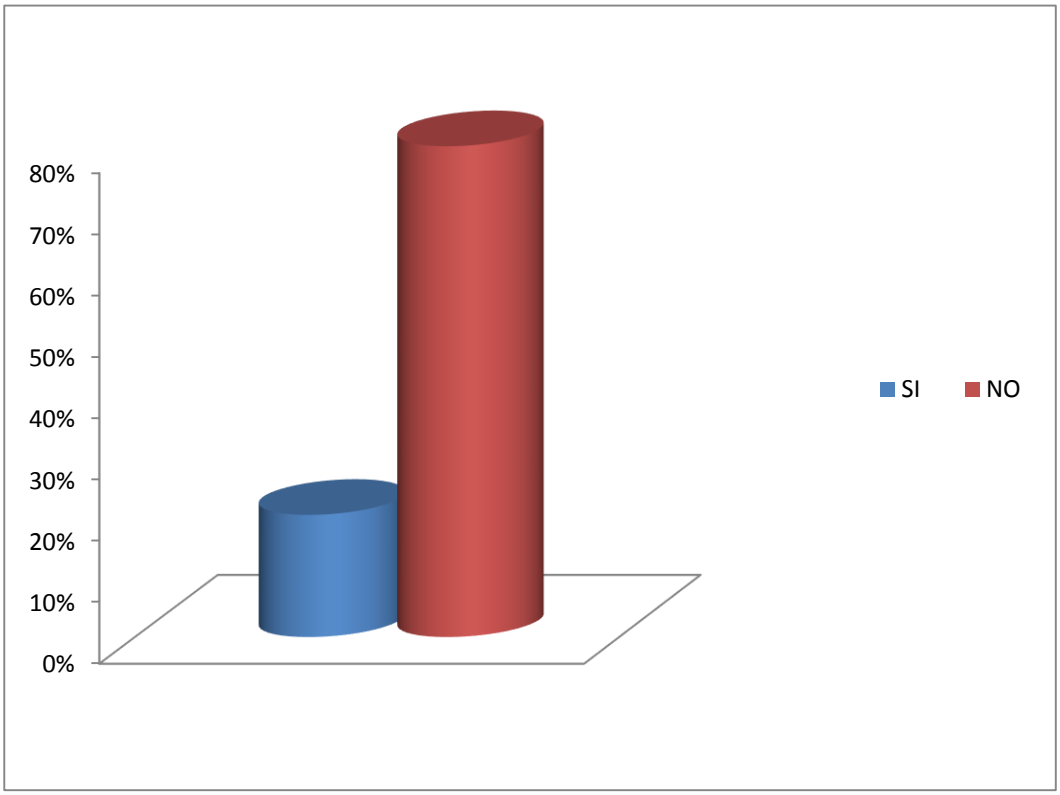


Figura 8.19 Resultado Pregunta 5
Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 20% de los entrevistados considera que la seguridad en la red inalámbrica y alámbrica, implementada en la Universidad Nacional de Loja si es segura y el otro 80% de los entrevistados afirman que la seguridad en la red inalámbrica y alámbrica, implementada en la Universidad Nacional de Loja no es segura

6. ¿Qué sugerencias ayudarían a mejorar la seguridad en la red de datos de la Universidad Nacional de Loja?

La pregunta es de varios criterios, debido a esto el número total de entrevistados no es igual al número de respuestas.

Tabla 8.20 Resultados Pregunta 6

ALTERNATIVAS	FRECUENCIA	%
Administración permanente de los historiales de los sistemas	1	7,6
Implementación de políticas de seguridad a nivel de usuario final	2	15,3
Inversión en equipos para la seguridad	2	15,3
Capacitación en seguridades LAN-WAN-WLAN	2	15,3
Que exista VPN en cada área	1	7,6
Que exista software libre para la administración de redes	2	15,3
Que exista en mecanismo de autenticación como servidor radius	1	7,6
Que exista manuales de distribución de la red en cada área.	1	7,6
Administración permanente de la red	1	7,6
TOTAL	13	100

Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

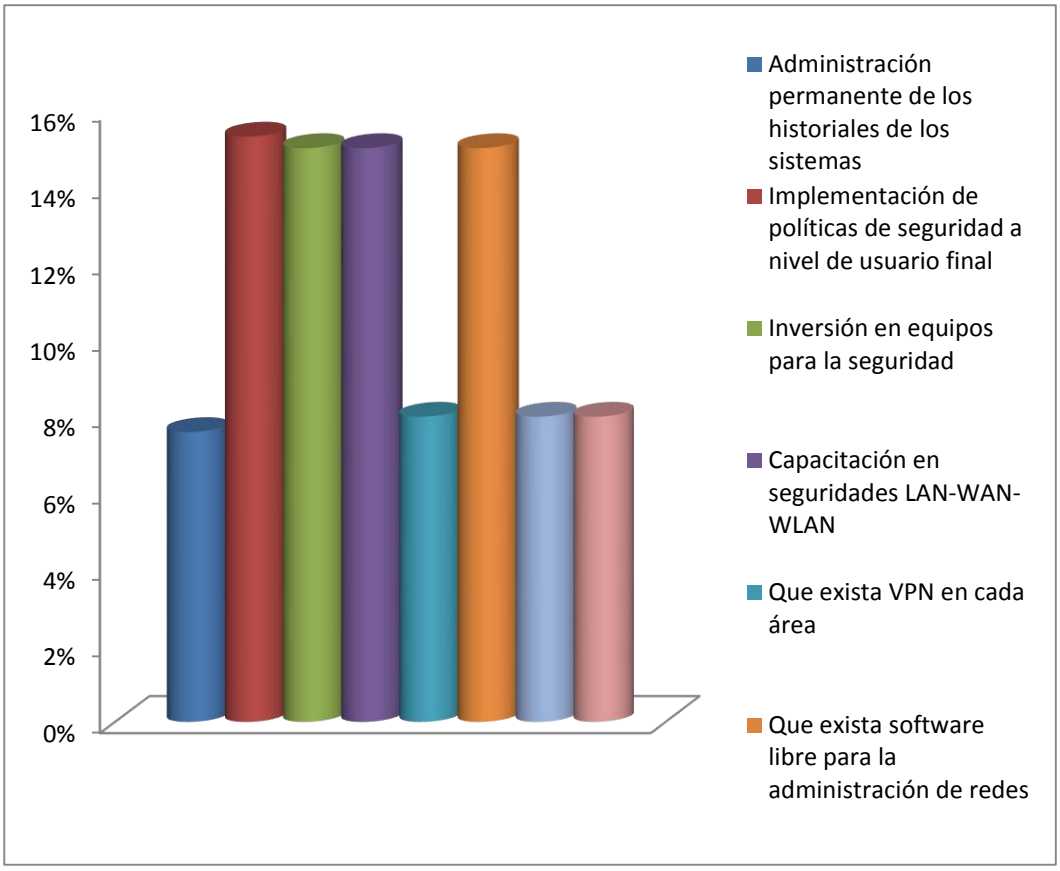


Figura 8.20 Resultado Pregunta 6
Fuente: Entrevista a los encargados de los centros de cómputo
Elaboración: Los Autores

De lo anterior podemos concluir que el 7,6% de los entrevistados afirman que se deberían implementar una Administración permanente de los historiales de los sistemas para mejorar la seguridad de la red, el 15,3% contesta que se deberían implementar políticas de seguridad a nivel de usuario final para mejorar la seguridad de la red, el 15,3% dice que se deberían implementar una Inversión en equipos para la seguridad para mejorar la seguridad de la red, el 15,3% piensa que se deberían implementar Capacitaciones en seguridades LAN-WAN-WLAN para mejorar la seguridad de la red, el 7,6% considera que se deberían implementar VPN en cada área para mejorar la seguridad de la red, el 15,3% aseveran que se deberían implementar software libre para la administración de redes para mejorar la seguridad de la red, el 7,6% afirma que se deberían implementar un mecanismo de autenticación como servidor radius para mejorar la seguridad de la red, un 7,6% menciona que se deberían implementar manuales de distribución de la red en cada área para mejorar la seguridad de la red y por

último un 7,6% sugiere que se deberían implementar una Administración permanente de la red para mejorar la seguridad de la red

8.2.4. Análisis de la tecnología existente (hardware y software) en la Universidad Nacional de Loja

El presente proyecto tiene como finalidad aprovechar la red de datos para a través de ella establecer seguridad de acceso a los usuarios que acceden a la misma.

La Universidad Nacional de Loja, posee una red de datos interna, que permite la comunicación entre usuarios de la red. La red tiene como punto central la Jefatura de Informática ubicada en el cuarto piso del segundo bloque de Administración Central, ésta se distribuye para las cinco Áreas Académicas Administrativas, Departamento de Bienestar Estudiantil, CINFA[32] y Federación de Estudiantes Universitarios de Loja.

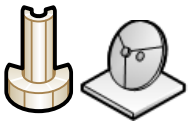
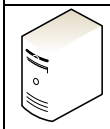
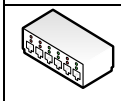
El backbone propiamente tal está constituido por una serie de puntos conectados a través de enlaces punto a punto, con antenas de elevadas ganancias y equipos confiables que permiten asegurar la disponibilidad de la red. La cobertura hacia los usuarios se proporciona mediante enlaces punto bajo estándar 802.11g.

El Internet llega a la Universidad a través de fibra óptica, la empresa encargada de brindar este servicio es TELCONET. El ancho de banda que posee la Universidad para los usuarios es de 31,14 mbp/s y 450 mbp/s para Internet comercial.

Para facilitar la comprensión de los esquemas y diagramas de redes mostrados a continuación es necesario emplear la siguiente simbología.

[32] CINFA: Centro de Informática Agropecuaria

Tabla 8.21 Simbología de Redes

SÍMBOLO	DESCRIPCIÓN
	**Antenas**
	**Cable UTP**
	**Caja Multimedia**
	**Convertidores Fibra a UTP "Transaiver"**
	**Fibra Óptica**
	Patch Fibra Óptica
	**PC Personales**
	**Radios**
	**Servidores**
	**Switch**
	**Torres**

8.2.4.1.Topología Física del Backbone y sus Puntos de Acceso

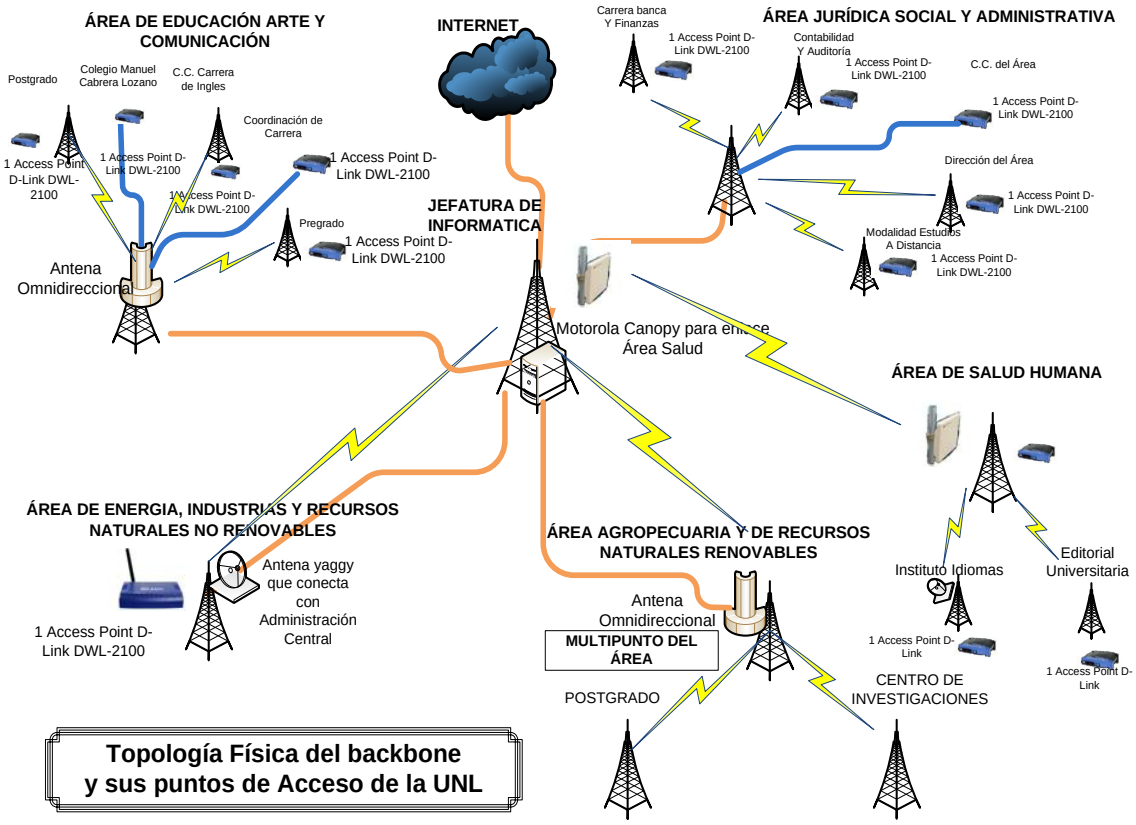


Figura 8.21 Topología Física del Backbone y sus Puntos de Acceso

8.2.4.2. Topología Lógica del Backbone y sus Puntos de Acceso

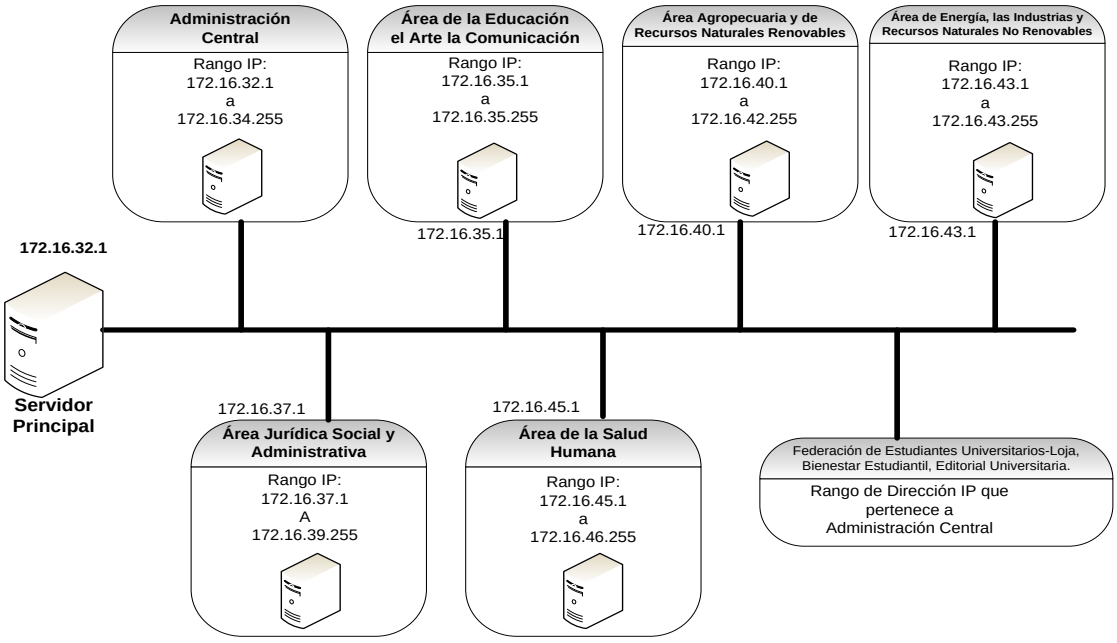


Figura 8.22 Topología Lógica del Backbone y sus Puntos de Acceso

Desde el punto de vista lógico el backbone de la red se encuentra operando bajo protocolo TCP/IP con una asignación formal de red clase B (172.16.32.1) con uso de máscara del tipo clase B (255.255.240.0). El Backbone de esta forma, es un segmento de red Ethernet trabajando en forma conmutada.

8.2.5. DISTRIBUCIÓN DE LA RED DE DATOS INTERNA DE LA UNIVERSIDAD NACIONAL DE LOJA

8.2.5.1. Administración Central

Los principales equipos y servidores que se encuentran en la Administración Central de la Universidad Nacional de Loja, los detallamos a continuación: **(Para mayor detalle revisar anexo # 5 donde se encuentra un video de la distribucion de la red de datos interna de la universidad nacional de loja)**

- **Equipos:**
    - Router Cisco, permite la interconexión con Internet comercial e Internet dos. El manejo de este equipo es de uso exclusivo del proveedor de Internet para la Universidad, TELCONET.
    - Un Switch Cisco 2960, que se encuentra conectado a la interfaz LAN del Router. Los servidores que se conectan a este Switch son:
        - Firewall,
        - Servidor WEB
        - Servidor Moodle (Educación Virtual a Distancia)
        - Servidor para la Radio Universitaria.

Switch Cisco 2960, conectado al Firewall. Los equipos conectados a este switch son:

- Servidor de Correos
- Servidor de Control de Contenido
- Servidor Financiero

- Servidor DHCP
- Switch 3com, desde este equipo inicia la interconexión con las Áreas Académicas Administrativas. Los equipos conectados a este dispositivo son:

    - Transaiver mc102xl Fast Ethernet media converter, realiza la conexión con el Área Agropecuaria y de Recursos Naturales Renovables por medio de fibra óptica
    - Transaiver D-link def-855, permite la conexión con el Área de la Educación el Arte y la Comunicación por medio de fibra óptica.
    - Transaiver D-link def-855, permite la conexión con el Área Jurídica, Social y Administrativa por medio de fibra óptica.
    - Radio Cannopy que permite tener comunicación inalámbrica con el Área de la Salud Humana.
    - Switch Catalyst 2950, permite la conexión con el Área de Energía las Industrias y los Recursos Naturales No Renovables por medio de un par de hilos de cobre.
    - Modem Cisco 673, permite la conexión con la FEUE.

- **Servidores**

  Firewall, servidor que permite tener la barrera entre la red pública y la red interna de datos, aquí constan las reglas que optimizan el uso del Internet en la Universidad Nacional de Loja. Las características del Firewall son:

    - Sistema Operativo Linux Fedora 3
    - Intel(R) Xeon (TM) cpu 3.2ghz
    - Memoria 1GB
    - Disco 160 GB

- Servidor WEB, aquí se encuentra instalada la página web de la Universidad. Las características las describimos a continuación:
    - Sistema Operativo Linux Fedora 3
    - Intel(R) Xeon (TM) cpu 3.2ghz
    - Memoria 1GB
    - Disco 160 GB

- Servidor Moodle. Utilizado para brindar educación a distancia vía internet. Las características las describimos a continuación:
    - Sistema Operativo Linux Fedora 3
    - Intel(R) Xeon (TM) cpu 3.2ghz
    - Memoria 1Gb
    - Disco 160 GB

- Servidor de Correo. Este servidor permite tener direcciones de correo electrónico bajo el dominio de la Universidad, por ejemplo informatica@unl.edu.ec. Las características las describimos a continuación:

    - Sistema Operativo Linux Fedora 3
    - Intel(R) Xeon (TM) 3.2ghz
    - Memoria 1GB
    - Disco 160 GB

- Servidor de DHCP, permite asignar dinámicamente direcciones de red a los computadores de la Universidad, por medio de la MAC de la interfaz de red. Las características las describimos a continuación:

    - Sistema Operativo Linux Fedora 6
    - Intel(R) Pentium (r) D 3.4ghz
    - Memoria 1GB
    - Disco 160GB

- Servidor para Control de Contenido, hace posible el control efectivo en el acceso a páginas pornográficas y de contenido malicioso principalmente, así como evita un consumo excesivo de ancho de banda. Para este propósito se utiliza Squid y Dansguardian, software que permite realizar el control en cada uno de los servidores de las Áreas. Las características las describimos a continuación:

    - Sistema Operativo Linux Fedora 3
    - Intel(R) Xeon (TM) cpu 3.2ghz
    - Memoria 1Gb
    - Disco 160 GB

- Servidor Financiero, posee el sistema contable Visual FOX. Las características las describimos a continuación:

    - Sistema Operativo Windows 2003 Server
    - Intel(R) Xeon (TM) 3.2ghz
    - Memoria 1GB
    - Disco 160 GB

- Servidor para la Radio Universitaria, replica la señal de "Radio Universitaria", a través de Internet. Las características las describimos a continuación:

    - Sistema Operativo Linux Fedora 6
    - Intel(R) Pentium (r) D 3.4ghz
    - Memoria 1GB
    - Disco 160GB.

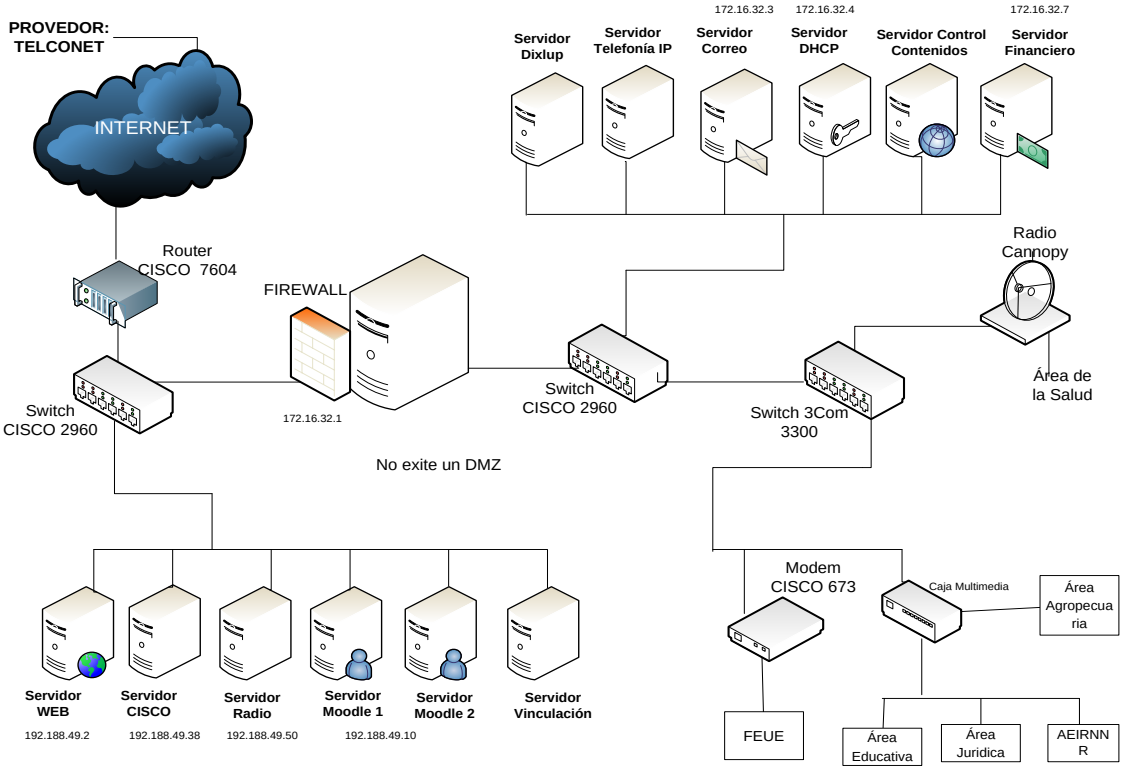


Figura 8.23 Equipos y Servidores Principales de la Red de Datos

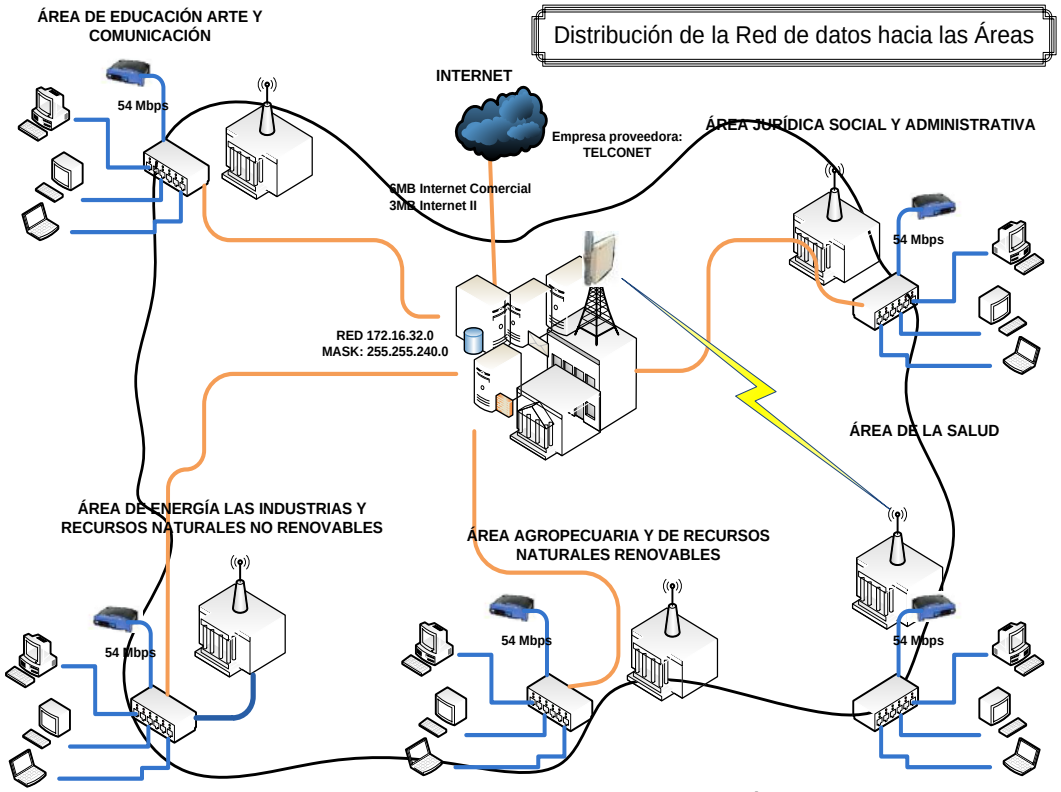


Figura 8.24 Distribución de la Red hacia las Áreas

8.2.5.2. Área Agropecuaria y de Recursos Naturales Renovables

La interconexión con el Área es por intermedio de fibra óptica. Los principales equipos que se encuentran en ésta son:

- Una caja multimedia donde llega la fibra óptica.
- Un transaiver D-link def-855 conectado a la caja multimedia y conectado al Switch 3COM
- Un Switch 3COM que conecta con el servidor del Área.
- Un Switch D-link (Switch Principal) conectado al Switch 3COM
- Un Servidor que tiene instalado: Squid y Danguardian para el control de contenido del internet a los usuarios del Área. Las características del servidor son:
  - Sistema Operativo Linux Fedora 6
  - Intel(R) Pentium (r) 4 3.0ghz
  - Memoria 512Mb
  - Disco 160 GB
- Un transaiver D-link def-855 enlazado al Switch Principal, el mismo permite conectar por medio de fibra óptica a otras dependencias del Área.
- Una antena omnidireccional D-Link que permite conectar inalámbricamente con el nivel de Postgrado del Área de esta dependencia y con el Centro de Investigación del Área.

El Centro de Cómputo de Ingles que funciona en el área cuenta con los siguientes dispositivos:

- 2 Switch 24 puertos D-Link DES-1024 D 10/100 Fast Etherneth
- 2 Organizadores
- 2 Patch Panel 24 puertos Category 5e System
- 2 Access Point D-Link DWL-2100

El Centro de Computo del Área Agropecuaria y de Recursos Naturales Renovables se encuentra a cargo de Ing. Ramiro Vásquez.

- **CINFA**

Al CINFA se llega por medio de una conexión de cable utp cat 5e, que parte desde el Switch 3COM al Switch del departamento; desde el cual existe la distribución para los host, posee los siguientes equipos:

- 2 Patch Panel de 24 puertos Quest Category 5e
- 2 Switch de 12 puertos/cu D-Link DES-1024 D 10/100 Fast Ethernet
- 2 Organizadores

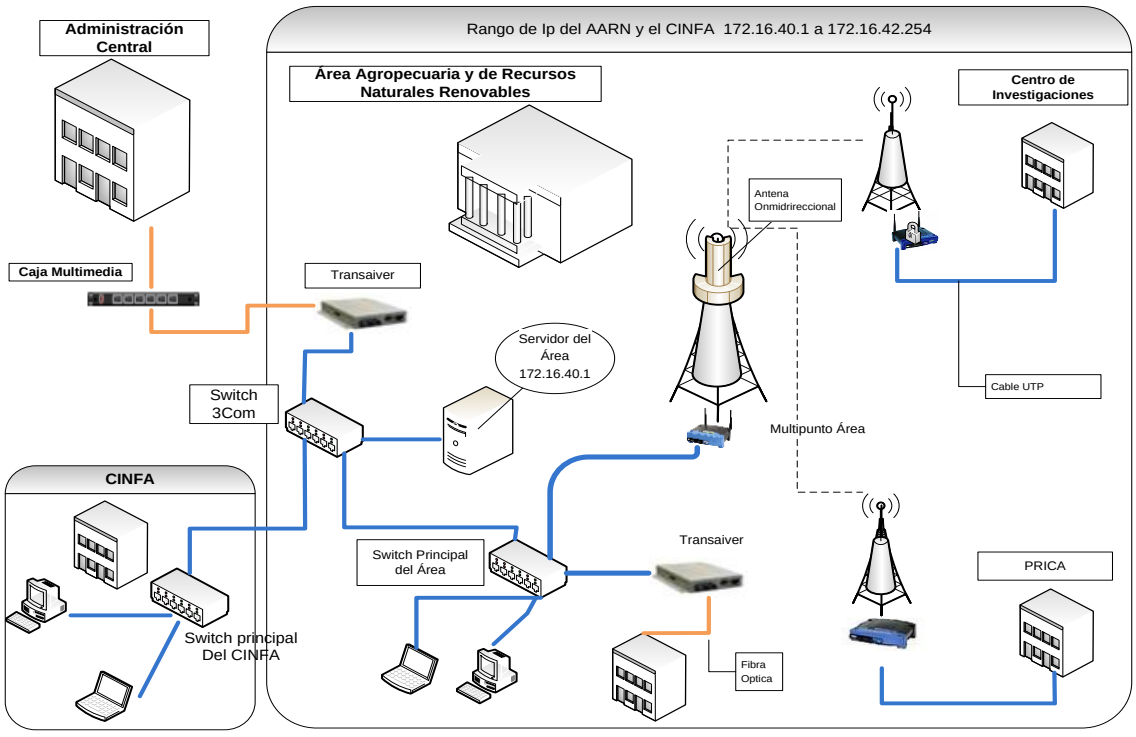


Figura 8.25 Red de Datos Área Agropecuaria y de Recursos Naturales Renovables

8.2.5.3. Área de Energía, Industrias y Recursos Naturales No Renovables y Federación De Estudiantes Universitarios de Loja (FEUE).

8.2.5.3.1. Área de Energía las Industrias y los Recursos Naturales No Renovables:

Se parte de la Caja multimedia, ubicada en la Jefatura de Informática, propia para el área de 8 Hilos de los cuales se utiliza 2 en multimodo, se encuentra conectado un Transaiver D-LINK DMC-300SC. A esta área se llega por medio de fibra óptica tendido por postes. La fibra se conecta a la Caja Multimedia del Área y a su vez a su convertidor Transaiver D-LINK DMC 700SC

Los equipos que posee el AEIRNNR son:

Para lo cual se hace referencia en el anexo # 3:

- 1 Switch 3Com 3C16476 Super Star Base Line 10/100/1000 Base T Capa 2 de
- 49,50 puertos, conectado al Transaiver y al servidor
- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Trasaiver D-Link DMC 700 SC onvertidor de fibra óptica a cable utp
- 1 Patch Panel RJ45 Leviton de 24 puertos
- 2 Bandejas de fibra óptica Hubbel 12 puertos cada uno
- 1 Switch D-Link DES 1016D de 16 puertos
- Un Servidor que tiene instalado: Squid y Danguardian para el control de contenido a los usuarios del área.

Existen varios equipos instalados en diferentes dependencias las que a continuación se describe:

Carrera de Geología

- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Bandejas de fibra óptica Hubbel 12 puertos cada uno

Coordinación Administrativa Financiera

- 1 Switch D-Link DES-1008D de 8 puertos

Secretaria General del Área

- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Bandejas de fibra óptica Hubbel 12 puertos cada uno

Edificio Nº 5

- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Bandejas de fibra óptica Hubbel 12 puertos cada uno

Centro De Computo 1.1

- 1 Switch Power Switch CNSH-1600 de 16 puertos

Centro De Computo 1.2

- 1 Switch 3Com 3C16476 Super Star Base Line 10/100/1000 Base T Capa 2 de 49,50 puertos
- 1 Switch 3Com Capa 3 3CR17561-91 Super Start Switch 4500 26 puertos
- 1 Trasaiver D-Link DMC 700 SC onvertidor de fibra óptica a cable utp
- 1 Patch Panel RJ45 Leviton de 24 puertos
- 2 Bandejas de fibra óptica Hubbel 12 puertos cada uno
- 1 Switch D-Link DES 1016D de 16 puertos

Centro De Computo 1.3

- 1 Switch 3Com Capa 2 3C16471 BaseLine de 24 puertos

El servidor que posee el Área de Energía, las Industrias y Recursos Naturales no Renovables son:

- Sistema Operativo Linux Fedora 10
- HP ML15063
    - Dual Core Intel Xeon 5120 (1.86 Ghz, 4 MB L2 cache)
    - 1066 Mhz FSB 1.5 Gb Memoria PC2-5300 /0/6 LFFHDD
- HP SATA RAID Controller / RAID 1011) /Red Gigabit
    - /56x CD-RW /Tower/2x HD 160 GB 1.56 SATA RAID (0/1)
    - /Red Gigabit /56x CD-RW /Tower / 2 x HP 160 GB 1.56 SATA
    - 7.2K 3.5" HDD Hot Plug (349238-B21)

Laboratorio Redes Y Sistemas Operativos

- 1 Switch D-Link DES 1016D 16 puertos

Departamento Administrativo

- 1 Switch 3COM 3C16794 de 8 puertos

Coordinación De Postgrado

- 1 Switch D-Link DES-1008D de 8 puertos

Unidad De Desarrollo Informático Y Planificación

- 1 Switch 3Com 3CFSUO8 de 8 puertos
- 1Switch D-Link DES-1008D de 8 puertos

Biblioteca del Área:

- Una caja multimedia donde llega la fibra óptica.
- 1 transaiver D-Link def-855 conectado a la caja multimedia y al Switch D-Link

- 1 Switch 3Com capa 3 Administrable 3CR 17561-R1 de 26 puertos
- 2 Switch 3Com capa 2 3C16471B de 24 puertos
- 1 Access Point AIR-PLUS DWL -2100
- 1 bandeja de fibra óptica de 12 puertos
- 2 patch panel de 24 puertos Quest NNP-1024
- 2 Access Point D-Link DWL 3200
- 2 antenas Omnidireccionales
- 4 Antenas Yaggy
- 1 Access Poitn D-Link DWL-2100 en Dirección General
- 1 Access Poitn D-Link DWL-2100 en la Torre de Recepción de Señal

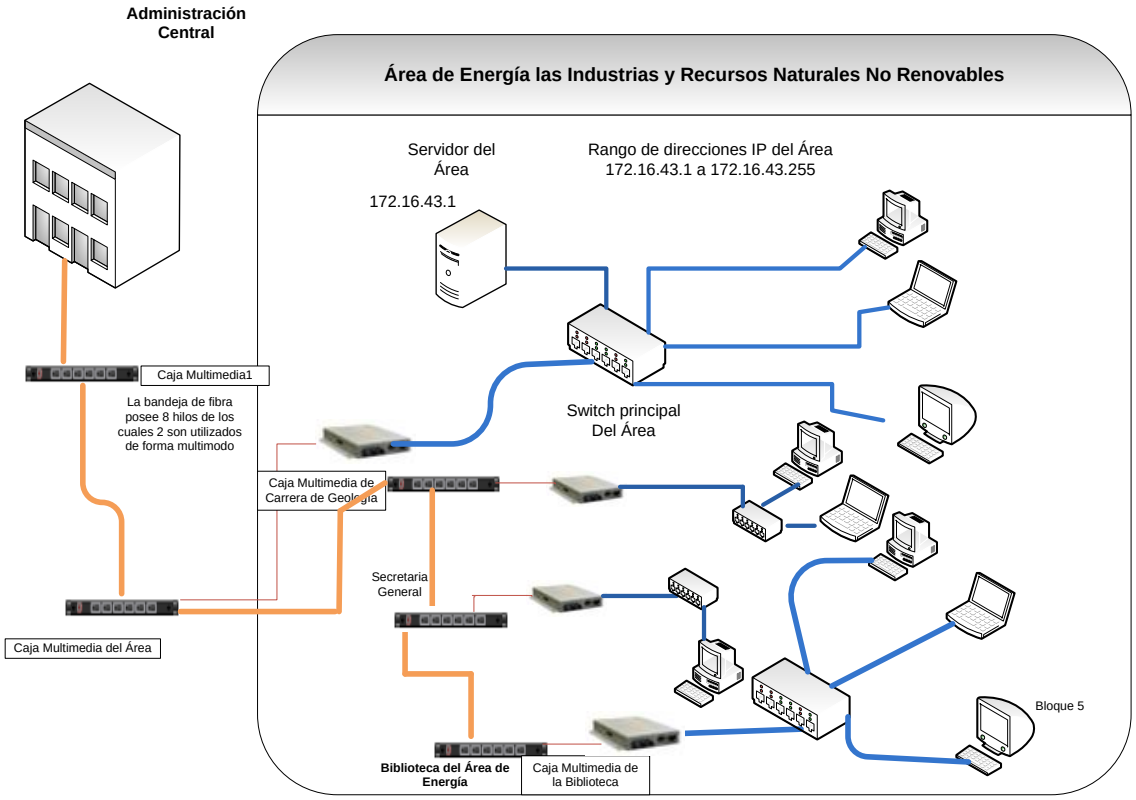


Figura 8.26 Red de Datos Área de Energía las Industrias y los Recursos Naturales No Renovables

8.2.5.3.2. Federación De Estudiantes Universitarios - Loja (FEUE)

- Parte desde el Modem Cisco – 673 de la Administración Central hasta un modem Cisco - 673 que está conectado al Switch principal.
- Swicth D-Link (Switch Principal)

- Swicth D-Link, para conectar las máquinas del Cyber de la FEUE
- Conexión desde Switch Principal hasta el Comisariato Universitario.

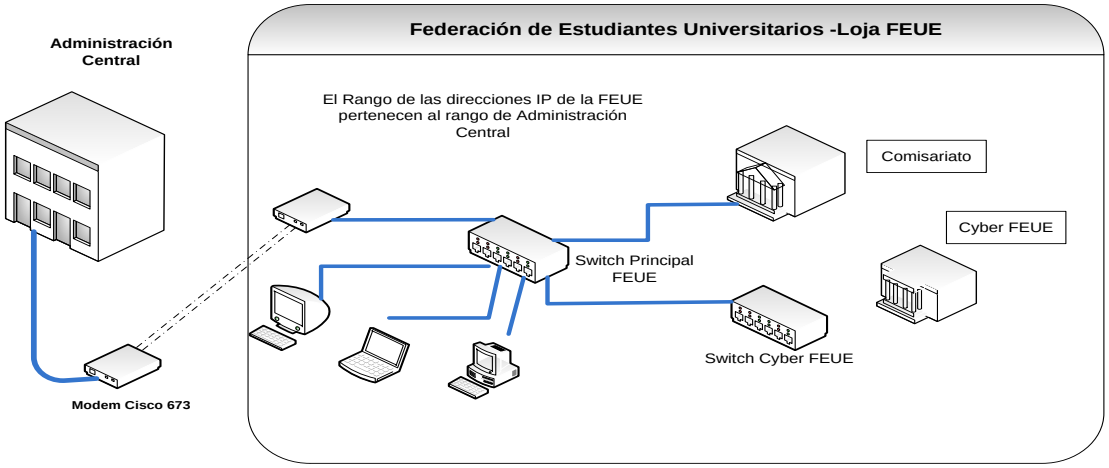


Figura 8.27 Red de Datos de la Federación De Estudiantes Universitarios de Loja (FEUE)

8.2.5.4. Área de la Educación el Arte y la Comunicación

La interconexión con el área es por intermedio de fibra óptica. Los principales equipos que se encuentran en esta área son:

Biblioteca del Área:

- Dos cajas multimedia.
- Un transaiver D-Link def-855 conectado a la caja multimedia (1) y al Switch D-Link
- Un Switch D-Link que está conectado al servidor.
- Switch 3COM enlazado con el Switch D-Link
- Un Servidor que tiene instalado: Squid y Danguardian para el control de contenido de internet a los usuarios del Área. Las características del servidor son:
    - Sistema Operativo Linux Fedora 6
    - Intel(R) Pentium (r) 4 cpu 3.0ghz
    - Memoria 512MB

- Disco 80GB

- Un transaiver D-link def-855 conectado con la caja multimedia (2), que permite enlazar la fibra óptica al Centro de Cómputo de Área**.**

Centro de Cómputo del Área

- Una caja multimedia donde llega la fibra óptica
- Un transaiver d-link def-855 que está conectado a la caja multimedia y al Switch D-Link
- Switch D-Link de 8 puertos, desde el cual se distribuye para los host del centro de cómputo.
- Una antena omnidireccional D-Link que permite conectar inalámbricamente con:
  - El nivel de Pregrado del Área
  - El nivel de Postgrado del Área.
  - Colegio Manuel Cabrera Lozano, anexo al Área.
  - Bloque de Coordinaciones de Carrera
  - Centro de Cómputo de la Carrera de Ingles

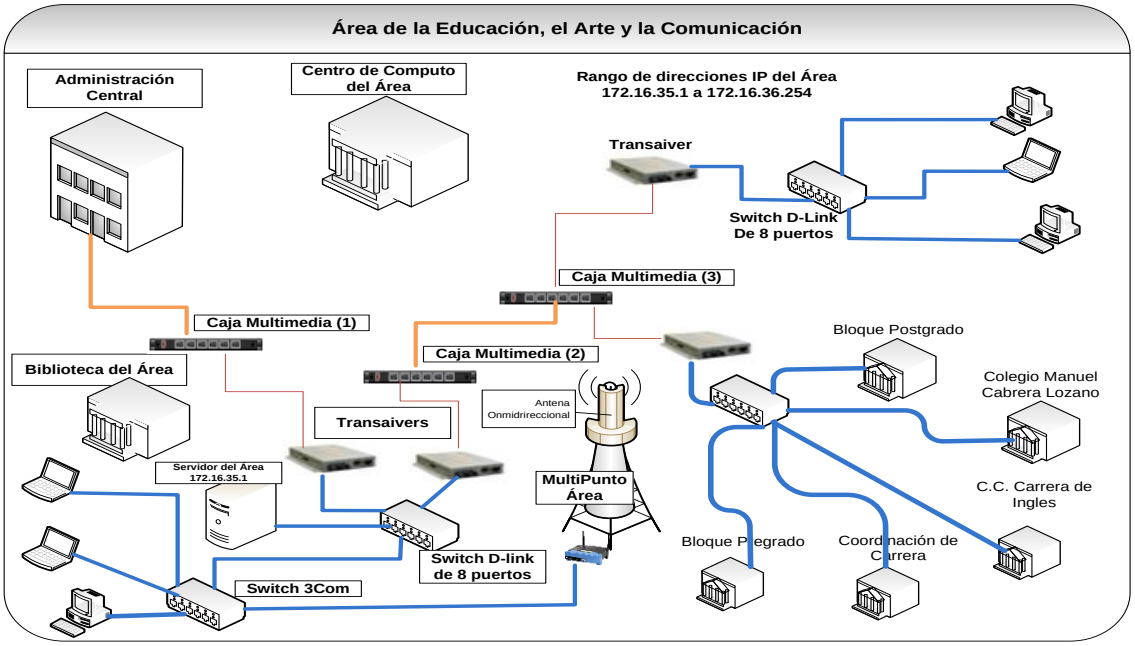


Figura 8.28 Red de Datos Área de la Educación el Arte y la Comunicación

8.2.5.5. Área Jurídica, Social y Administrativa

La interconexión con esta Área es por intermedio de fibra óptica. Los principales equipos que se encuentran en está son:

Biblioteca del Área:

- Una caja multimedia donde llega la fibra óptica.
- Un transaiver D-Link def-855 conectado a la caja multimedia y al Switch D-Link
- Un Switch D-Link que está conectado al servidor.
- Un Servidor que tiene instalado: Squid y Danguardian para el control de contenido a los usuarios del área. Las características del servidor son:
    - Sistema Operativo Linux Fedora 6
    - Intel(R) Pentium (r) 4 cpu 3.0ghz
    - Memoria 512Mb
    - Disco 80GB
- Un transaiver D-Link def-855 conectado con la caja multimedia, que lleva la fibra óptica al nivel de Postgrado del Área.

Nivel de Postgrado del Área

- Una caja multimedia donde llega la fibra óptica.
- Un transaiver D-Link def-855 conectado a la caja multimedia y al Switch
- Un Switch D-Link que distribuye a los host del bloque.
- Un transaiver D-Link def-855 conectado con la caja multimedia, que lleva la fibra óptica a Bienestar Estudiantil.

Además existe en esta Área dos antenas omnidireccionales que permite conectar inalámbricamente con:

Omnidireccional Uno

- Bloque principal del área.
- Centro de Cómputo principal del Área
- Bloque Modalidad de Estudios a Distancia.

Omnidireccional Dos

- Carrera de Contabilidad y Auditoria
- Carrera de Banca y Finanzas.

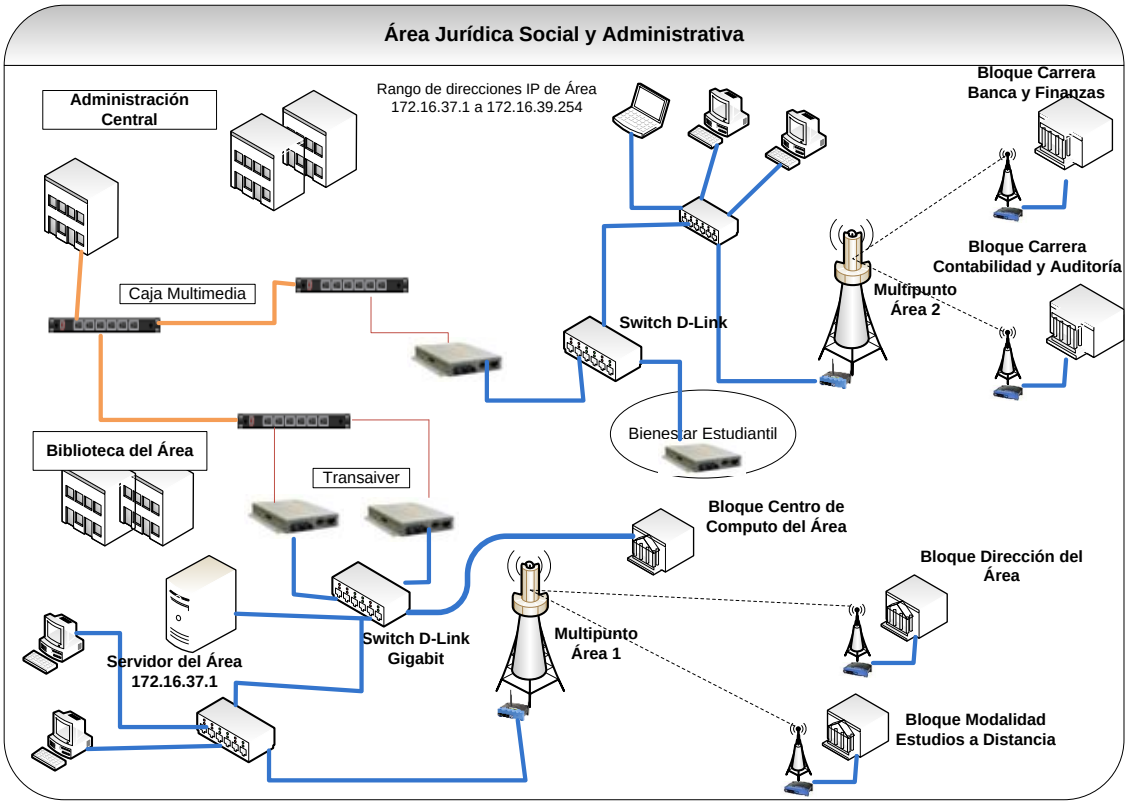


Figura 8.29 Red de Datos Área Jurídica, Social y Administrativa

8.2.5.6. Área de la Salud Humana, Instituto de Idiomas, Editorial Universitaria

Con el Área de la Salud Humana se tiene una conexión inalámbrica. Lo siguiente equipos existen instalados:

- Un radio Cannopy conectado al Switch D-Link.
- Un Switch D-Link (Swtich Principal) conectado al servidor y a un radio D-Link.
- Un radio D-Link multipunto, que permite tener comunicación con el Instituto de Idiomas y la Editorial Universitaria.
- Un Servidor que tiene instalado: Squid y Danguardian para el control de contenido del internet a los usuarios del Área. Las características del servidor son:
    - Sistema Operativo Linux Fedora 3
    - Intel(R) Pentium (r) 4 cpu 2.8ghz
    - Memoria 512Mb
    - Disco 80Gb

- Una antena omnidireccional que permite la comunicación inalámbrica con:
    - Bloque de Postgrado del Área
    - Editorial Universitaria
    - Instituto de Idiomas

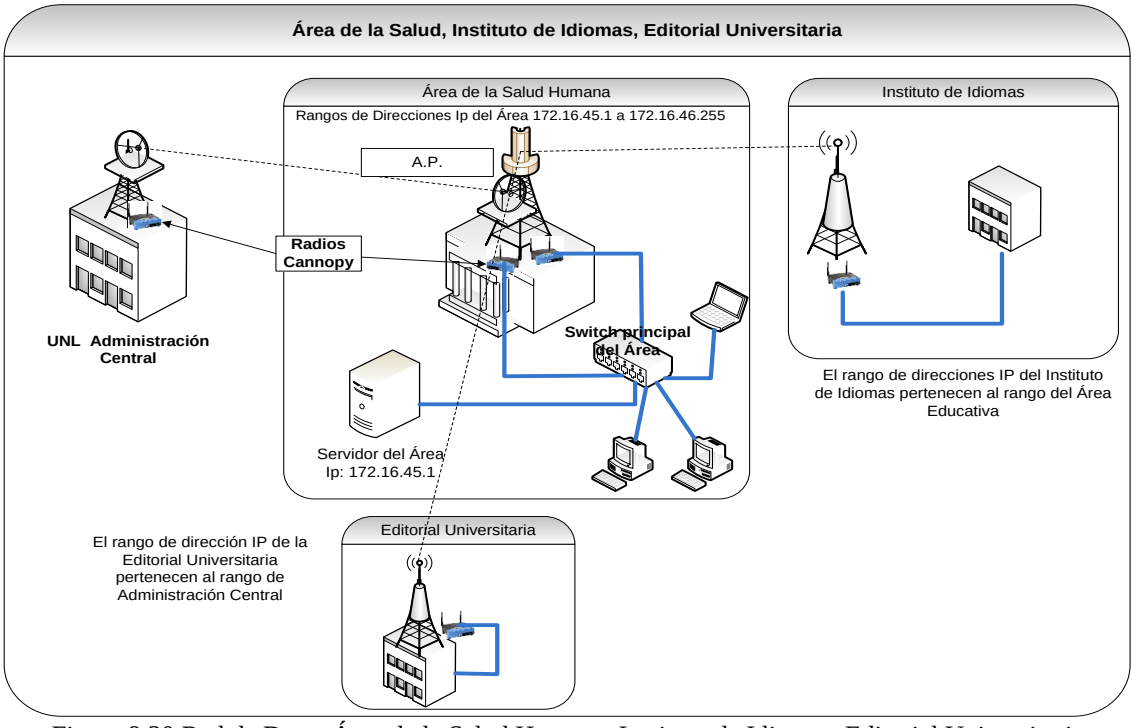


Figura 8.30 Red de Datos Área de la Salud Humana, Instituto de Idiomas, Editorial Universitaria

Bienestar Estudiantil

La interconexión con Bienestar Estudiantil es por intermedio de fibra óptica.

- Una caja multimedia donde llega la fibra óptica.
- Un transaiver D-Link def-855 conectado a la caja multimedia y a un Switch D-Link
- Un Switch D-Link que distribuye la red a los host del departamento.

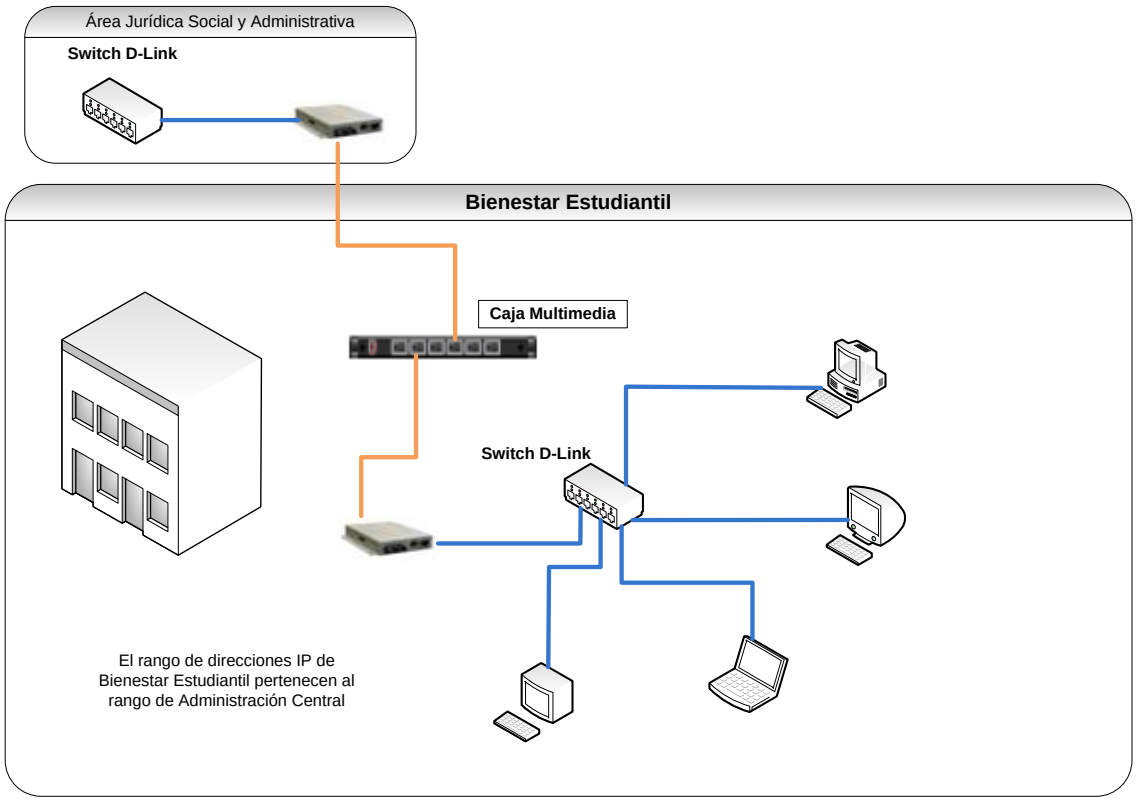


Figura 8.31 Red de Datos Bienestar Estudiantil

8.3. SELECCIÓN DE LA MEJOR ALTERNATIVA DE SEGURIDAD PARA REDES CABLEADAS E INALAMBRICAS, EN BASE A LOS REQUERIMIENTOS DE LA UNIVERSIDAD NACIONAL DE LOJA"

8.3.1. Estudio de los mecanismos de seguridad

8.3.1.1. Estudio de los mecanismos de seguridad para redes inalámbricas

Muchas prácticas se han establecido como recomendables para minimizar los riesgos asociados al acceso indebido en redes inalámbricas.

Para solucionar los problemas que presenta implementar WLAN en distintos escenarios se evalúa las tres principales técnicas:

- **Virtual Private Network (VPN):**[33] Una VPN (red privada virtual) es una técnica de encapsulación y encriptación de los paquetes de datos a distintos puntos de la red a través de infraestructuras públicas de transporte. El escenario más común de esta tecnología es la de unir oficinas o la de permitir al personal que se encuentra de viaje acceder a la red interna de sus empresas, permitiéndole a éste obtener los servicios propios de la red interna.

En el caso de una red inalámbrica, la utilización de una VPN permite autenticar al usuario, cifrar los datos, pero a costa de un aumento del ancho de banda utilizado y de un cuello de botella en la red.

El esquema típico es montar la red inalámbrica fuera del cortafuego de la red interna, se toma entonces a esta red como una red insegura. De esta manera se puede ofrecer acceso público a visitantes y se utiliza VPN para cifrar el tráfico inalámbrico, autenticar a los usuarios y permitirles a estos acceder a los recursos propios de la red interna.

[33] http://es.wikipedia.org/wiki/Red_privada_virtual

A continuación describimos como se conectan los usuarios de la red inalámbrica (WLAN) a la red interna (LAN) a través del concentrador VPN, y hacia Internet lo hacen de forma directa sin pasar por la red interna.

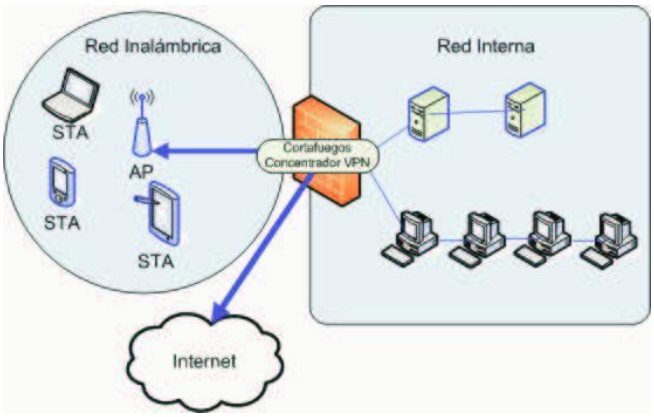


Figura 8.32 Diagrama de red WLAN y LAN con VPN

- **Proxy-Web**: Una de las alternativas más populares por su bajo costo, es la implementación de un Proxy-Web. La idea es realizar autenticación y autorización de los usuarios en escenarios como en Hoteles y aeropuertos, donde se requiere entregar acceso público con algún tipo de restricción en el acceso. Proxy-Web no requiere de la instalación de ningún software adicional por parte del cliente.

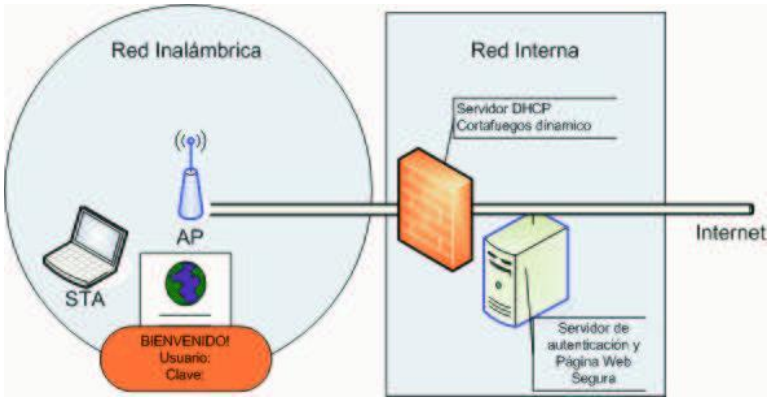


Figura 8.33 Diagrama de Proxy-Web para autenticación en redes

En la figura podemos apreciar el cortafuegos dinámico que es el encargado primero de redirigir el tráfico Web de los usuarios sin autenticar hacia el Servidor de autenticación y página Web segura, una vez que se supera la etapa de autenticación, el

cortafuegos dinámico en base a la dirección IP y dirección física del adaptador de red (MAC) modifican las reglas para permitir el acceso a la red interna e Internet.

- **IEEE 802.11i** (11)**:** El Instituto de Ingenieros Eléctricos y Electrónicos IEEE propone el protocolo IEEE 802.11i o Wireless Protected Access 2 (WPA2) como la solución definitiva al problema de seguridad en redes inalámbricas de área local ante las debilidades encontradas en 802.11 y WEP.

Este protocolo especifica los requerimientos para las redes inalámbricas de área local (LAN) a nivel de capa MAC y capa física (PHY), fue recientemente ratificado a principios de octubre del año 2004.

IEEE 802.11i incluye varias mejoras, las principales son tres nuevos algoritmos de encriptación: TKIP basado en RC4 compatible con el hardware actual, CCMP y WRAP ambos basados sobre Advanced Encription System (AES) el cual es un algoritmo más robusto pero requiere de un mayor poder de calculo que RC4. También propone a 802.1x/EAP para la autenticación para cualquiera de los tres modos de encriptación.

Una primera versión llamada Wireless Protected Access (WPA) basada en IEEE 802.11i, era la encargada de ofrecer una WLAN segura hasta la ratificación IEEE 802.11i. Esta ofrece mejoras bajo el hardware que actualmente poseen los usuarios (equipos Wi-Fi, que mediante un update de drivers o firmware se compatibilizan con lo que WPA propone). WPA utiliza como mecanismo de encriptación, autenticación basada en **802.1X**/EAP. Para escenarios donde no se quiere implementar 802.1X se tiene un modo llamado Pre-Shared Key (PSK) que al igual que WEP utiliza una llave preconocida y compartida entre AP y STA, pero realiza una permanente rotación de llaves.

8.3.1.2.Estudio de los mecanismos de seguridad para redes cableadas

En el día a día, los departamentos de Informática se enfrentan a una serie de cuestiones de seguridad para decidir el nivel de protección necesario de los sistemas de la

organización. Así, mientras la protección de la red por sí sola es esencial y proporciona una fácil justificación para hacer todo lo necesario para protegerla, el camino está lleno de obstáculos.

La razón más importante para tener la seguridad en su sitio es proteger la información confidencial de la organización. Para solucionar los problemas que presenta implementar redes LAN en distintos escenarios se evalúa las tres principales técnicas:

- **Criptografía: L**a criptografía robusta sirve para proteger información importante de corporaciones y gobiernos, aunque la mayor parte de la criptografía fuerte se usa en el campo militar. La criptografía se ha convertido en un gran negocio últimamente ya que es una de las pocas defensas que pueden tener las personas en una sociedad vigilante.

El encriptamiento y el desencriptamiento requieren el uso de una llave y un método de codificación de tal forma que el método de encriptamiento pueda ser modificado únicamente por el usuario.

- **Firewall / Cortafuegos:** Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

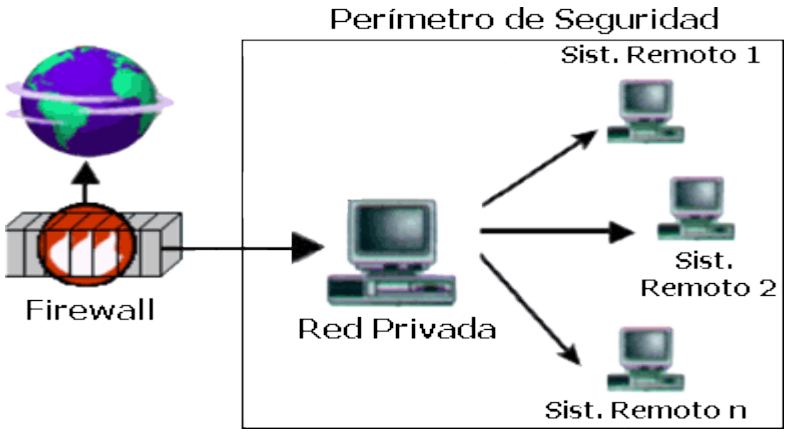


Figura 8.34 Firewall

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación.

- **802.1:** *Definición Internacional de Redes.* Define la relación entre los estándares 802 del IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI) de la ISO (Organización Internacional de Estándares). Por ejemplo, este Comité definió direcciones para estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única. Los vendedores de tarjetas de interface de red están registrados y los tres primeros bytes de la dirección son asignados por el IEEE. Cada vendedor es entonces responsable de crear una dirección única para cada uno de sus productos.

8.3.2. Selección del mecanismo de seguridad

En base a al estudio de las tecnologías que se utilizan para dar seguridad y control de acceso en las redes LAN y WLAN se decide basar el diseño utilizando IEEE 802.1x, ya que es la solución más completa al problema de seguridad por que contempla una serie de mejoras, como autenticación de usuarios, rotación de las llaves de encriptación (siendo esto un proceso en que el usuario no interviene).

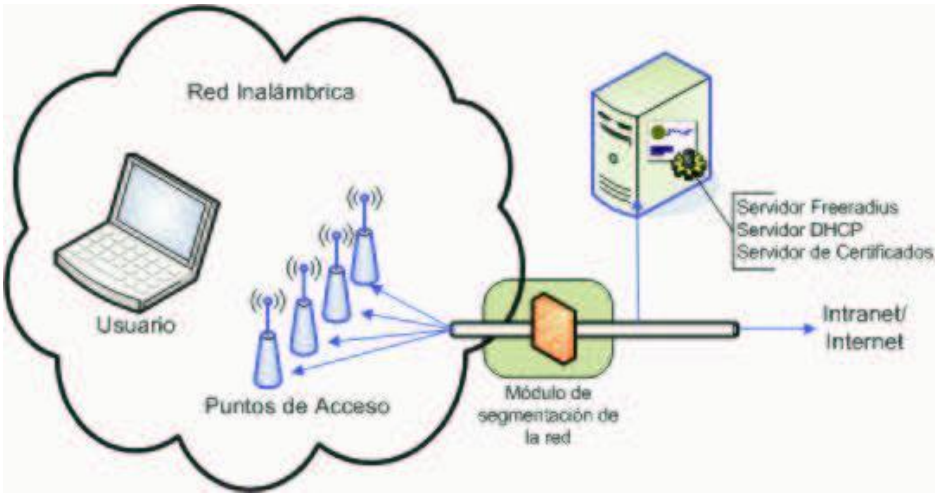


Figura 8.35 Diagrama de la solución

8.3.3. Análisis del estándar IEEE 802.1x para redes cableadas e inalámbricas[34]

8.3.3.1. Análisis del estándar IEEE 802.1x para redes cableadas

La especificación IEEE 802.1x es un estándar de control de acceso y autenticación, basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.

El estándar fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. El estándar 802.1x involucra tres participantes

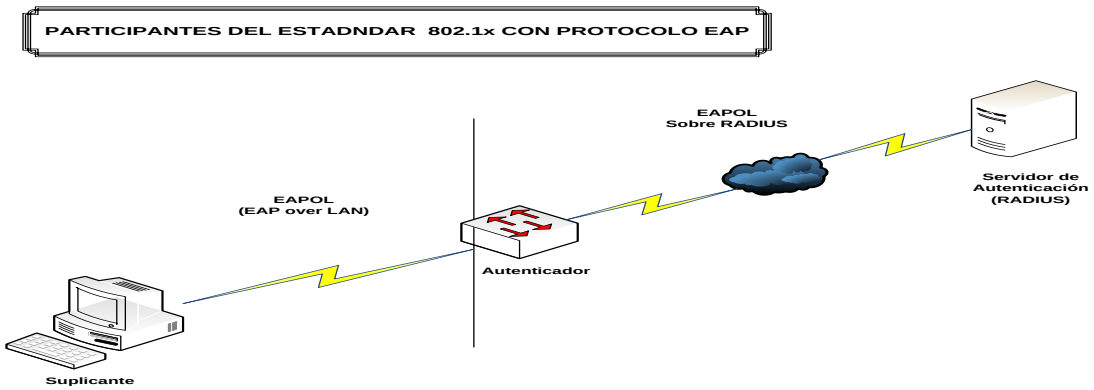


Figura 8.36 Participantes del estándar 802.1x con protocolo EAPOL

[34] http://www.sans.org/reading_room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlan-039-s_1607

- **El Suplicante**, o equipo del cliente, que desea conectarse con la red.

- **El Servidor de Autorización/Autenticación**, que contiene toda la información necesaria para saber cuáles equipos o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las redes de área local alambradas e inalámbricas.

- **El Autenticador**, que es el equipo de red (switch, ruteador, servidor de acceso remoto, punto de acceso) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

- **Servidores de Autenticación,** Aunque en la especificación 802.1x se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los criterios del marco AAA (Authentication, Authorization and Accounting). Este marco define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema. Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o bien reenviar la petición a otro servidor AAA.

RADIUS es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red (como los puntos de acceso). Estos elementos envían información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que

éste trate al cliente de la manera adecuada. Toda la comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red. Otro servidor de autenticación AAA es **DIAMETER,** el cual introduce algunas ventajas significativas respecto a RADIUS en materia de gestión de elementos de acceso complejos, si bien se encuentra aún en un estado menos avanzado de definición.

8.3.3.1.1. Protocolo EAP-EAPOL[35]

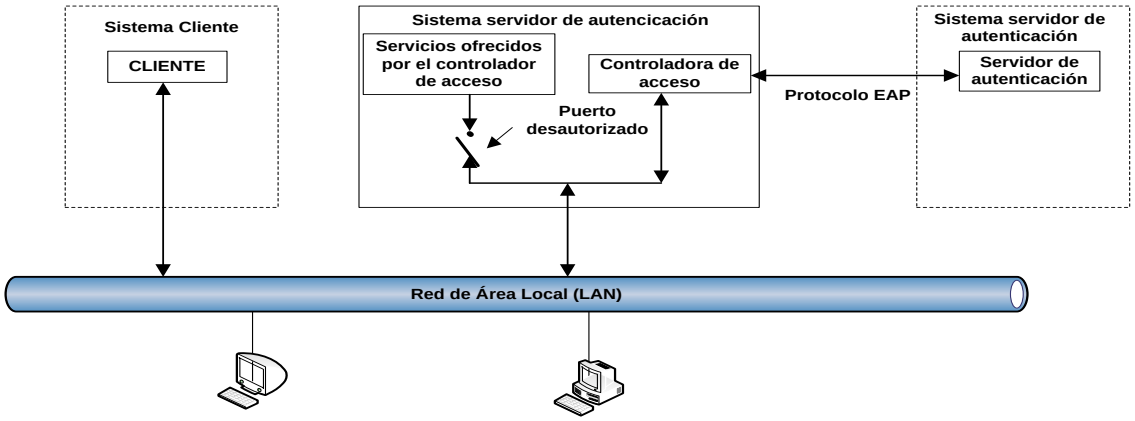


Figura 8.37 Arquitectura lógica del estándar 802.1x con protocolo EAP

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.
- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación. El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/ Identity.
- La estación se identifica mediante un mensaje EAP-Response/ Identity.

[35] http://technet.microsoft.com/es-es/library/cc782851%28WS.10%29.aspx

- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access-Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje RADIUS-Access- Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.
- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.
- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS. En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-Access-Accept un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

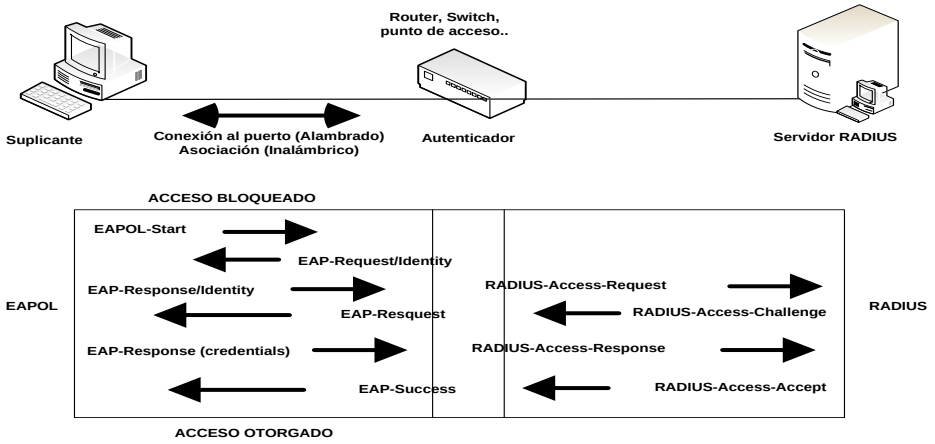


Figura 8.38 Proceso de validación con protocolo EAP-EAPOL

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

8.3.3.2. Análisis de Autenticación basada en 802.1x para redes WIFI

Como se mencionó anteriormente, los componentes básicos de una implementación 802.1x son: el suplicante (cliente), el autenticador (AP) y el servidor de autenticación (Radius). En la figura 8.39 se muestra, un esquema donde se integra la autenticación del esquema 802.1x con la ayuda de la base de datos de usuarios de la universidad.

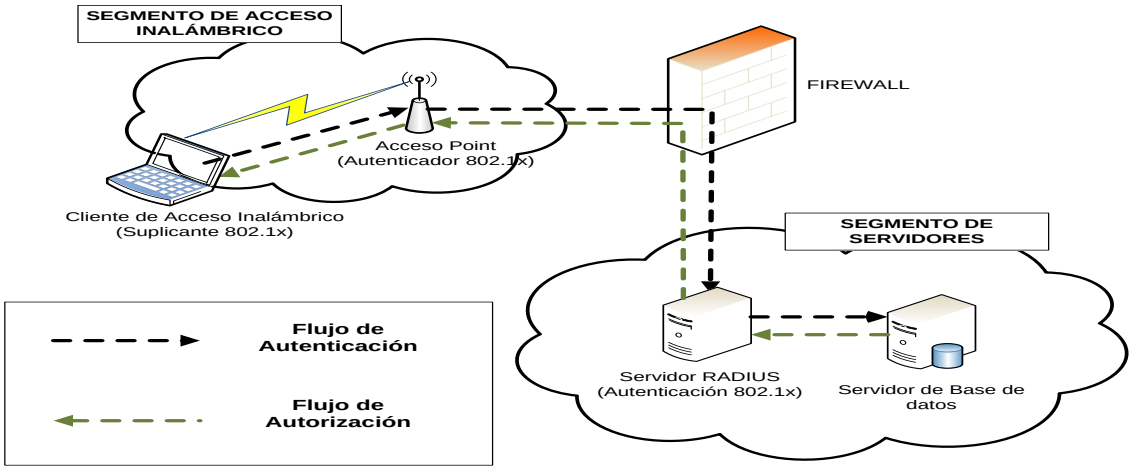


Figura 8.39 Esquema de autenticación basada en 802.1x

Como se puede ver, es importante considerar en el diseño todos los elementos que se involucrarán con el esquema a implementar, para así considerar los requerimientos en cada uno de ellos y terminar de definir adecuadamente el plan de implementación.

8.3.3.3. Requerimientos técnicos de la solución[36]

Es necesario delimitar los posibles tipos de autenticación a implementar, es importante validarlos y seleccionar el más indicado con base en los requerimientos técnicos que implica la implementación de estos posibles tipos de autenticación.

[36] http://www.sans.org/reading_room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlan-039-s_1607

En el momento de la implementación el Área de Energía, las Industria y Recursos Naturales No Renovables ya puede contar con un servicio de autenticación de usuarios (como un servidor RADIUS, por ejemplo), el cual se requiere mantener y poder integrar a la nueva infraestructura de acceso cableado e inalámbrico. Para esto, se deben validar si estos servicios de autenticación son compatibles con 802.1x, y si es así, determinar los tipos de autenticación EAP que soportan.

Sin embargo, si el servicio de autenticación a la red con el que se cuenta no es compatible con los nuevos requerimientos para asegurar el acceso cableado e inalámbrico, se debe verificar si realizando una actualización del servicio este quede habilitado para implementar 802.1x, o si por el contrario se requiere implementar uno nuevo de las muchas alternativas comerciales y gratuitas disponibles que brindan amplias capacidades y compatibilidad con 802.1x. Para el caso se optará por la implementación basada en los proyectos open source llamado freeradius**.**

Otro punto importante es considerar la estructura de dominio de usuarios con la que se cuenta y si se pretende utilizar la misma base de datos de usuarios para validar la autenticación a la red en la implementación de 802.1x a realizar. Generalmente, la mayoría de servidores de autenticación que soportan 802.1x permiten integrarse con las bases de datos de usuarios de la organización (directorios LDAP, dominios NT, bases de datos distribuidos u otras). El servidor del Sistema de Gestión Académica SGA implementado en la Universidad Nacional de Loja, permite utilizar las mismas credenciales almacenadas en este, para la autenticación a nivel de acceso a la red. Sin embargo, es necesario verificar esta compatibilidad en el servidor de autenticación que se pretende utilizar u optar por manejar una base de datos alterna, implementada sobre el mismo servidor, de acuerdo a las opciones que este brinde para realizar dicho proceso.

8.3.3.3.1. En los usuarios

Desde el punto de vista de los clientes de acceso cableado e inalámbrico, exactamente sobre los requerimientos de la conexión, se debe validar si las plataformas utilizadas en los clientes soportan el tipo de autenticación elegido o si por el contrario requieren un

componente de software que los habilite para realizarla. A continuación se presenta la Tabla 8.22 con el tipo de soporte disponible en algunos sistemas operativos (los más comunes a nivel de cliente) para los métodos de autenticación EAP que se implementarían:

Tabla 8.22 Soporte EAP para algunos S.O. como cliente

Sistema Operativo	EAP-TLS	EAP-TTLS
Windows XP, 2000, Vista	Cliente nativo	Cliente de Tercero
Windows 9x	Cliente de Tercero	Cliente de Tercero
Linux	Cliente de Tercero	Cliente de Tercero
MacOS	Cliente de Tercero	Cliente de Tercero

Al manejar diferentes plataformas a nivel de clientes (Windows, Linux, MacOS) se hace necesario implementar un mismo cliente 802.1x para tener un sistema homogéneo y facilitar la administración.

8.3.3.3.2. En los Acces Point y Switchs

Entre los principales requerimientos, sobre estos dispositivos, para poder implementar un mecanismo de seguridad para el control del acceso inalámbrico, se encuentran:

- Compatibilidad con 802.11 y soporte de cifrado WPA
- Capacidad de implementar el servicio de control de acceso 802.1x
- Configuración del protocolo 802.1q para vlans.

8.3.3.3.3. En el servidor de autenticación

Finalmente, los principales requerimientos en este componente, para poder implementar la solución de seguridad basada en 802.1x, son:

- Compatibilidad con 802.1x

- Soporte de diversos tipos de autenticación EAP (TLS, TTLS, PEAP)

- Capacidad de registro (Accounting)

- Flexibilidad para validar a los suplicantes mediante varios métodos (Base de datos de usuarios local, directorio de usuarios LDAP, certificados, entre otros)

8.3.3.4. Selección del Servidor

La elección del servidor RADIUS es de esencial importancia, ya que es capaz de soportar, dentro del estándar 802.11x, al autenticador, al hot Spot con portal cautivo y al servidor de bases de datos.

El control de acceso por dirección física (MAC) y por usuario-contraseña puede ser satisfecho utilizando un servidor RADIUS en interacción con un servidor de bases de datos y con un Hot Spot con portal cautivo.

RADIUS es un protocolo de autenticación, autorización y accounting para aplicaciones de acceso a la red o movilidad IP.

Cuando se realiza la conexión con un ISP (Proveedor de Servicio de Internet) mediante módem, DSL, Ethernet cableada o inalámbrica, 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) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación 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, etc.

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. El uso de un servidor RADIUS es común en el control de acceso a usuarios y ampliamente recomendado.

8.3.4. Fase de autenticación

8.3.4.1. Selección del mecanismo de autenticación

De acuerdo a los requerimientos de seguridad y funcionalidad, se debe seleccionar el método de autenticación EAP adecuado, es posible que en pequeñas empresas, con un número de usuarios pequeño y recursos limitados se seleccione un método de autenticación como PEAP, el cual, por ejemplo, no requiere del uso de certificados digitales, significando esto menos complejidad y menores costos.

Por el contrario, para la universidad que cuenta con gran cantidad de usuarios puede ser más funcional el integrar certificados para así poder tener un mejor control sobre los usuarios y equipos que se conectan a la red.

Los requerimientos técnicos y funcionales han permitido definir el método EAP-TTLS como el tipo de autenticación que es soportado por los elementos que conforman la solución, además debido a que las credenciales no son observables en el canal de comunicación entre el nodo cliente y el proveedor de servicio se tiene mayor protección contra ataques de diccionario y suplantaciones, y en general las consideraciones que se presentan a continuación que respaldan la selección del mismo:

- **Anonimato y Privacidad**: No transmite el nombre de usuario en claro en la primera petición de identidad.

- **Confianza en el servidor EAP-TTLS**: Métodos de autenticación con passwords no susceptibles a ataques de diccionario.

- **Compromiso del certificado del servidor EAP-TTLS**: Empleo de métodos de revocación de certificados para evitarlo.

- **Negociación y encriptación del enlace**: Negociación segura de la "Cipher suite de datos" (sistema de cifrado de la comunicación)

- **Listado de las preferencias del cifrado de datos:** Cliente selecciona la del servidor como su primera opción y la del punto de acceso. Maximizar grado de seguridad.

Igualmente, y como se explicó anteriormente, es posible realizar la validación de la identidad (autenticación) que realiza el servidor de autenticación mediante varios métodos, de manera local en el servidor RADIUS o con respecto a una base de datos externa que puede ser de varios tipos, lo más común son las bases de datos de usuarios del domino tipo LDAP. Este tipo de sistema de usuarios es manejado en la universidad y los servicios de acceso cableado e inalámbrico son para los usuarios que hacen parte del sistema, es recomendable integrar la autenticación del RADIUS con la base de datos que maneja estos usuarios (tipo LDAP) para establecer un proceso más transparente para el usuario con el manejo de menos claves para más servicios así como para aprovechar las características de estos sistemas que permiten realizar una mejor administración y autorización sobre el uso de los recursos informáticos que los usuarios manejen.

8.3.4.1.1. Validación por dirección física del dispositivo de red (MAC)

De acuerdo a lo establecido, se determinó que la mejor alternativa para el control de acceso a la red del proyecto por dirección física (MAC), es el uso de un servidor RADIUS trabajando con el estándar 802.1x y utilizando el servidor de bases de datos LDAP. Esto permite la escalabilidad del sistema al no quedar restringido el ingreso de usuarios, ya que la información de validación (la MAC del usuario principalmente) será almacenada en el servidor de bases de datos y no en el autenticador del sistema, cuya capacidad de almacenamiento es limitada.

Además cumple con la transparencia en la validación, es decir, cuando el usuario levanta la conexión con la red de servicio, automáticamente será validado por el servidor RADIUS sin necesitar intervención alguna del usuario en cuestión. El uso de

bases de datos permitirá integrar una interfaz de gestión de usuarios que será tratada posteriormente.

El esquema para la validación por dirección física se muestra en la figura siguiendo el estándar 802.1x.

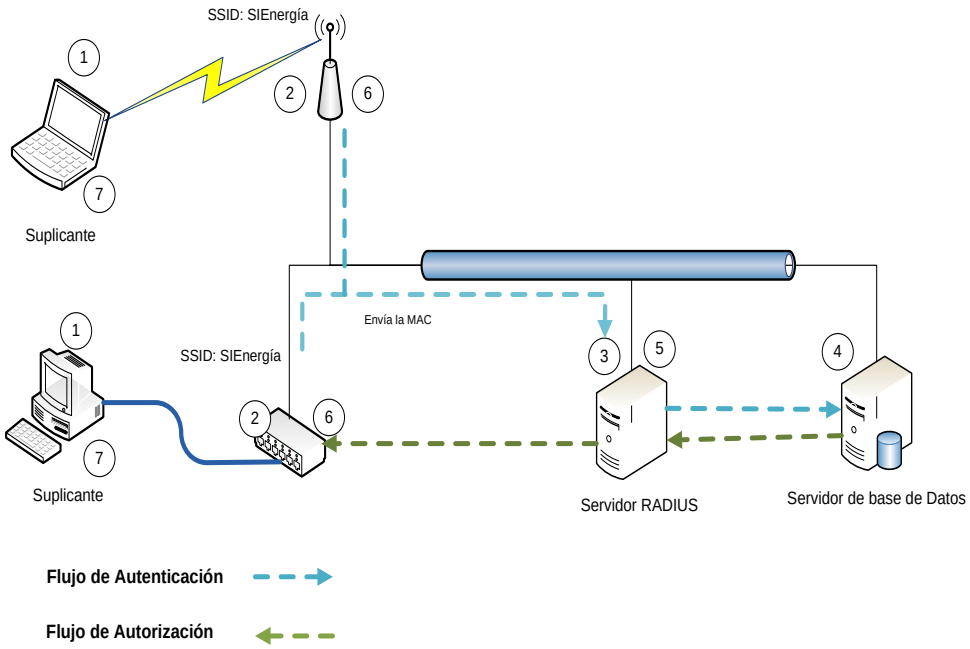


Figura 8.40 Esquema para validación por MAC

El proceso de validación es el siguiente para un caso favorable:

- El suplicante levanta su tarjeta de red (alámbrica o inalámbrica), enviando las características de su equipo al autenticador en forma automática.

- El autenticador recibe el paquete con la información proveniente del suplicante y envía la MAC de este al servidor RADIUS, manteniéndose todos los puertos de comunicación con la red de servicio cerrados para el suplicante.

- El servidor RADIUS consulta a la base de datos, la existencia de la MAC del suplicante en las tablas de almacenamiento de estas.

- El servidor de bases de datos chequea que la MAC del suplicante se encuentra en las tablas de MAC válidas. Si corresponde, envía esta información al servidor RADIUS.
- El servidor RADIUS válida al suplicante y autoriza al suplicante a hacer uso de la red de servicio, enviando la decisión al autenticador.
- El autenticador recibe la decisión del servidor RADIUS y abre los puertos para que el suplicante pueda hacer uso de la red de servicio.
- El suplicante puede hacer uso de la red de servicio.

El proceso de validación es el siguiente para un caso no favorable:

- El suplicante levanta su tarjeta de red (alámbrica inalámbrica), enviando las características de su equipo al autenticador en forma automática.

- El autenticador recibe el paquete con la información proveniente del suplicante y envía la MAC de este al servidor RADIUS, manteniéndose todos los puertos de comunicación con la red de servicio cerrados para el suplicante.

- El servidor RADIUS consulta a la base de datos, la existencia de la MAC del suplicante en las tablas de almacenamiento de estas.

- El servidor de bases de datos chequea que la MAC del suplicante se encuentra en las tablas de MAC válidas. Como no corresponde, envía esta información al servidor RADIUS.

- El servidor RADIUS no válida al suplicante, y por lo tanto, no autoriza al suplicante a hacer uso de la red de servicio, enviando la decisión al autenticador.
- El autenticador recibe la decisión del servidor RADIUS y desconecta al suplicante de la red.

- El suplicante no puede hacer uso de la red de servicio.

Todo el proceso es completamente automático y transparente para el usuario, cumpliendo con los requerimientos que el proyecto requiere.

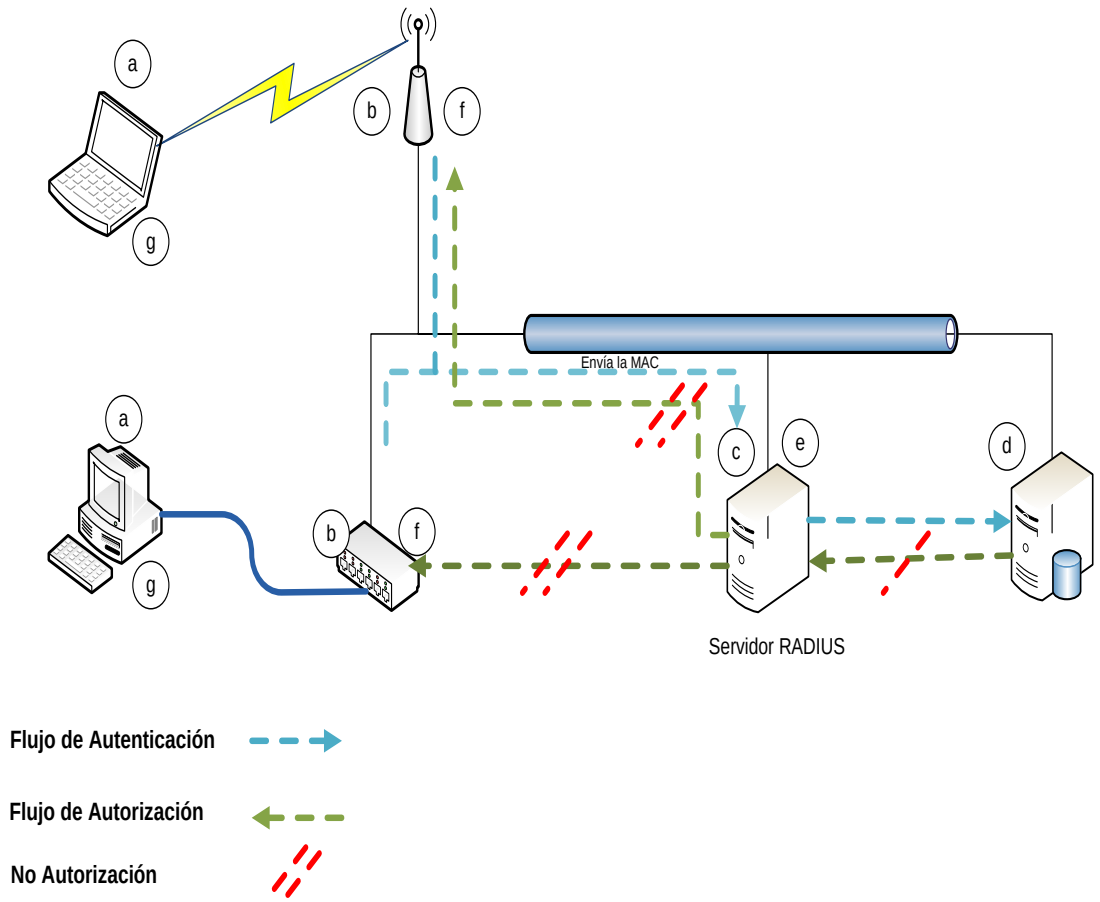


Figura 8.41 Esquema para validación por MAC no Favorable

8.3.4.1.2. Validación por usuario – contraseña

Anteriormente se determinó que la mejor solución para el control de acceso a la red es el uso de un servidor RADIUS trabajando con el estándar 802.1x, utilizando un servidor de bases de datos LDAP y Hot Spot.

El servidor RADIUS elegido y cuya instalación será tratada posteriormente, permite interactuar con el Hot Spot.

La interacción de estos más el servidor de bases de datos, son las herramientas necesarias para satisfacer los requerimientos de control de acceso por usuario-contraseña que el proyecto requiere.

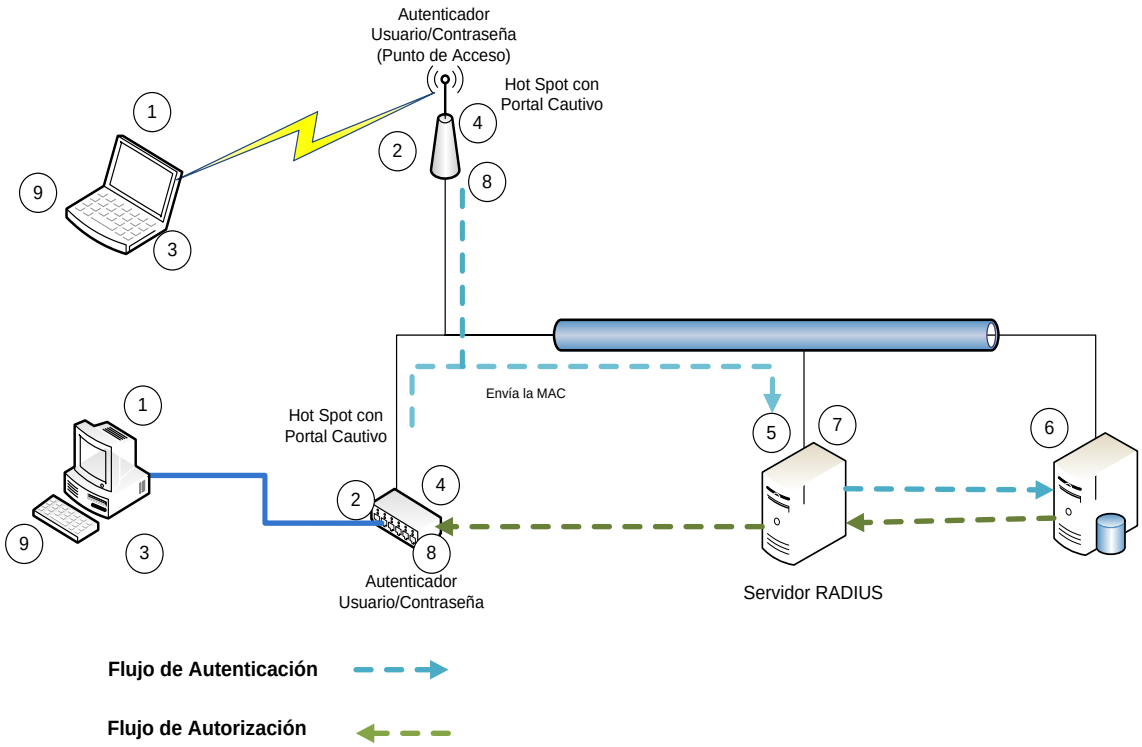


Figura 8.42 Esquema para validación por usuario-contraseña

El autenticador juega un rol importante en el proceso de validación por usuario-contraseña, ya que además de servir como autenticador bajo el estándar 802.1x, es quien contiene el Hot Spot, encargado de entregar al usuario la página en formato web donde deberá ingresar el usuario - contraseña. Dicha página está alojada en el servidor web.

El proceso de validación es el siguiente para un caso favorable:

- El suplicante levanta su tarjeta de red (alámbrica o inalámbrica), enviando las características de su equipo al autenticador en forma automática.

- El Hot Spot (o autenticador) recibe el paquete con la información proveniente del suplicante y le entrega la configuración de su dispositivo de red, por medio del protocolo de asignación dinámica de servidores (DHCP), mientras aguarda por la información de validación (usuario-contraseña).

- El suplicante recibe el paquete, quedando configurada su interfaz de red. Luego, debe abrir el explorador de Internet (puede abrir cualquier página inicial, distinta

de la página en blanco “about:blank”) siendo re direccionado, por el portal cautivo, a la página de validación donde ingresará el usuario-contraseña que le corresponda. El usuario-contraseña es enviado al Hot (autenticador).

- El autenticador recibe el paquete con la información proveniente del suplicante, y envía el usuario-contraseña de este al servidor RADIUS, manteniéndose todos los puertos de comunicación con la red de servicio cerrados para el suplicante.

- El servidor RADIUS consulta a la base de datos, la existencia de usuario y contraseña del suplicante en las tablas de almacenamiento de estas.

- El servidor de bases de datos, chequea que el usuario y contraseña del suplicante se encuentre en las tablas de validación. Si corresponde, envía esta información al servidor RADIUS.

- El servidor RADIUS válida al suplicante y lo autoriza a hacer uso de la red de servicio, enviando la decisión al autenticador.

- El autenticador recibe la decisión del servidor RADIUS, y abre los puertos para que el suplicante pueda hacer uso de la red de servicio.
- El suplicante puede hacer uso de la red de servicio.

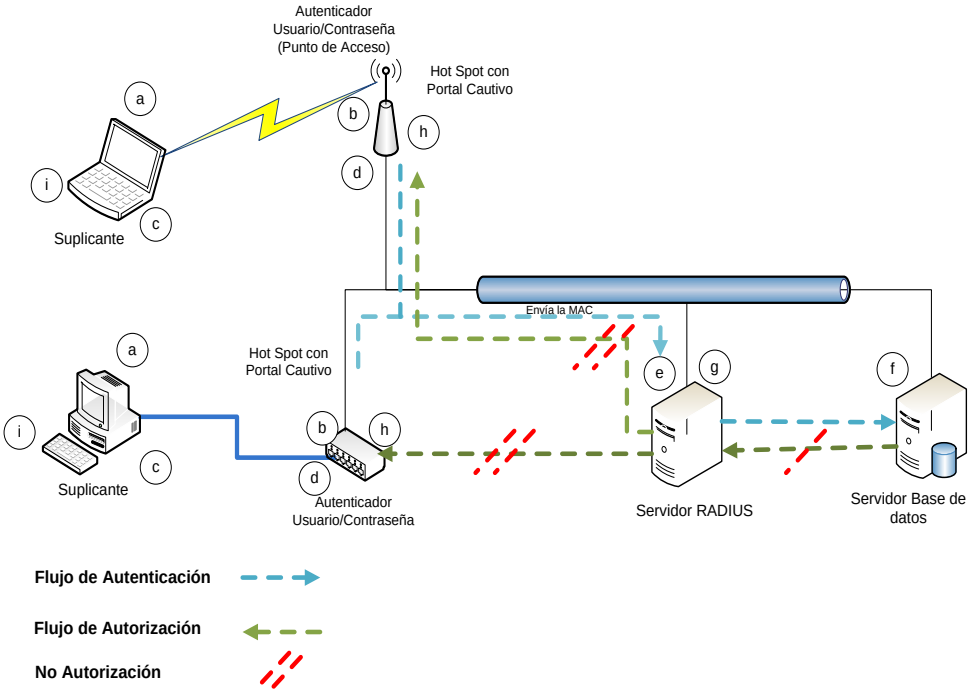


Figura 8.43 Esquema para validación por usuario-contraseña no favorable

- El suplicante levanta su tarjeta de red (alámbrica o inalámbrica), enviando las características de su equipo al autenticador en forma automática.
- El Hot (o autenticador) recibe el paquete con la información proveniente del suplicante, y le entrega la configuración de su dispositivo de red por medio del protocolo de asignación dinámica de servidores (DHCP), mientras aguarda por la información de validación (usuario-contraseña).
- El suplicante recibe el paquete, quedando configurada su interfaz de red. Luego, abre el explorador de Internet (puede abrir cualquier página inicial distinta de la página en blanco “about:blank”) siendo redireccionado, por el Hot, a la página de validación donde ingresará el usuario-contraseña que le corresponda, que en este caso es erróneo. El usuario-contraseña es enviado al Hot Spot con portal cautivo (autenticador).
- El autenticador recibe el paquete con la información proveniente del suplicante y envía el usuario-contraseña de este al servidor RADIUS, manteniéndose todos los puertos de comunicación con la red de servicio cerrados para el suplicante.
- El servidor RADIUS consulta a la base de datos la existencia de usuario y contraseña del suplicante en las tablas de almacenamiento de estas.

- El servidor de bases de datos chequea que el usuario y contraseña del suplicante se encuentran en las tablas de validación. Como no corresponde, envía esta información al servidor RADIUS.
- El servidor RADIUS no válida al suplicante, y por lo tanto, no lo autoriza a hacer uso de la red de servicio, enviando la decisión al autenticador.
- El autenticador recibe la decisión del servidor RADIUS y mantiene los puertos de comunicación con la red de servicio cerrados para el suplicante y espera por un usuario-contraseña nuevo, repitiéndose el proceso anterior.
- El suplicante no puede hacer uso de la red de servicio.
- El proceso cumple con los requerimientos que el proyecto necesita para el control de acceso por usuario-contraseña.

8.4. IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PLANTEADO EN EL AREA DE ENERGIA, LAS INDUTRIAS Y RECURSOS NATURALES NO RENOVABLES COMO PLAN PILOTO.

A la hora de realizar la implementación surgen consideraciones importantes para el éxito de la solución. De manera general, la implementación de este tipo de sistemas requiere un conocimiento específico del estándar 802.1x y de tecnologías cableadas e inalámbricas seleccionadas, por lo cual hay que verificar que se cuente con los recursos debidamente calificados para llevar a cabo esta implementación o si se requiere adquirir los servicios de un tercero.

Una vez se cuente con los recursos y se cumpla con los requerimientos técnicos es necesario realizar una planeación de la implementación considerando todos los componentes que intervienen en este proceso, y de esta manera establecer que procedimientos, cómo y cuando se desarrollarán y así informarlo, pedir autorización y evitar impactos negativos considerables.

Es recomendable realizar, de manera previa, la implementación de la solución en un ambiente de desarrollo donde se realizan todas las pruebas necesarias para verificar la correcta funcionalidad en el uso de los servicios informáticos que se acceden. Posteriormente, se debe comenzar con la implementación de la solución en el ambiente de producción de manera gradual, es decir realizarla sobre un primer grupo de usuarios los cuales presenten un bajo impacto sobre los procesos del AEIRNNR como podría ser en el mismo departamento de redes. En el momento de implementación de la solución en cada uno de los elementos que la conforman, existen igualmente consideraciones particulares a tener en cuenta.

A continuación se presentan las principales consideraciones para la implementación de 802.1x en cada uno de estos componentes:

8.4.1. Instalación del servidor

Se debe configurar el tipo de autenticación seleccionado, en este caso EAP, así como los demás parámetros asociados a este mecanismo. Se ha decido integrar la autenticación con una base de datos externa (LDAP), para lo cual se debe habilitar esta opción y establecer los parámetros adecuados como son, tipo de base de datos, servidores a integrar, entre otros. También se deben definir los autenticadores (APs) que van a trabajar con el servidor de autenticación.

El servidor puede instalarse en cualquier computador con sistema operativo Linux y contempla los siguientes pasos:

Instalación de servidor Radius Freeradius[37] de Código licencia libre, el mismo que puede ser obtenido de su página oficial.

Instalación previa de paquetes: Openssl[38], ldap[39], krb5[40], gdbm[41], sasl(lib)[42], pam(lib)[43], iodbc[44], mysql[45], postgresql[46] y unixodbc[47].

Instalación de Openssl para:

- Creación de claves privadas y certificados para servidor y root. Para este propósito se puede hacer uso de los scripts obtenidos desde la página:

  http://karman.homelinux.net/blog/descargas/cascripts.tar.gz

- Generar archivo “dh” (Diffie-Hellman) para encriptación.

[37] http://www.freeradius.org
[38] http://www.openssl.org/
[39] http://www.openldap.org/
[40] http://web.mit.edu/kerberos/
[41] http://www.gnu.org/software/gdbm/
[42] http://www.gnu.org/software/gsasl/
[43] http://www.kernel.org/pub/linux/libs/pam/
[44] http://www.iodbc.org/
[45] http://www.mysql.com/
[46] http://www.postgresql.org/
[47] http://www.unixodbc.org/

- Generación arbitraria de archivo “random” para creación de claves.

Es necesario disponer del archivo de extensiones OID[48], que se distribuye en el paquete de scripts anteriormente mencionados.

8.4.1.1.Implementación del servidor FREERADIUS

FreeRADIUS es una implementación en software libre de RADIUS y se caracteriza por soportar múltiples mecanismos de autenticación, tales como PAP, CHAP, MD5, EAP, etc.

En el siguiente cuadro se presenta los requerimientos para implementar un servidor.

Tabla 8.23 Requerimientos del Servidor Freeradius

Requerimientos	Mínimos	Óptimos
Procesador	Intel Pentium II, 400 MHz o superior	Intel Dual Core, 1.6 GHz
Sistema Operativo	Linux	Linux
Capacidad de Disco	5.3Gb	160Gb
Memoria	256Mb	1Gb

Lo primero a analizar es la manera de instalación del servidor FreeRADIUS. Al tratarse de una plataforma como la de Ubuntu, nos permite realizarlo de dos maneras: o bien descargando el archivo precompilado e instalarlo (opción utilizando al comando apt-get con el parámetro install, por ejemplo: #apt-get install freeradius) o descargar el código fuente (por ejemplo: con el comando wget: #wget ftp://ftp.freeradius.org/pub/freeradius/freeradiusserver- 2.0.3.tar.bz2), modificarlo de acuerdo a las funcionalidades que deseamos tener, prepararlo (#./configure), compilarlo y por último instalarlo (#make y #make install). Se ha elegido la segunda opción porque requerimos realizar una modificación en el código fuente para poder habilitar la funcionalidad del FreeRADIUS para que trabaje con los servidores OpenLDAP y MySQL para realizar la autenticación de los usuarios y llevar a cabo la contabilidad del sistema, respectivamente.

[48] OID, Identificador de Objeto, es una secuencia de números que se asignan jerárquicamente y que permite identificar objetos en la red, siendo usados con gran cantidad de protocolos.

Luego, se procede con modificar los archivos de configuración de FreeRADIUS. Estos son principalmente 04 archivos, todos ubicados en la carpeta /etc/freeradius:

- radiusd.conf
- eap.conf
- clients.conf
- sql.conf
- ldap.attrmap

Una vez realizado todos estos pasos procedemos a poner en marcha el servicio de FreeRADIUS dentro del servidor utilizando el siguiente comando:

#service freeradius start

En el caso en que se desee iniciar el proceso en modo de depuración (debug), puede utilizarse el siguiente comando:

#/usr/sbin/freeradius –x –f

8.4.1.2. Implementación del servidor OPENLDAP

OpenLDAP es una implementación en software libre del protocolo LDAP[49], utilizado muchas veces para la administración de usuarios en una red IP mediante servicios de directorio. De igual forma que con el servidor FreeRADIUS, podemos instalar OpenLDAP de dos maneras: mediante el archivo precompilado o descargando el código fuente. Sin embargo, podemos instalarlo mediante el archivo precompilado, ya que no requerimos realizar ninguna modificación especial.

Los requerimientos del servidor a continuación:

[49] LDAP (Lightweight Directory Access Protocol): (Protocolo ligero de acceso a directorio)

Tabla 8.24 Requerimientos del Servidor OpenLDAP

Requerimientos	Mínimos	Óptimos
Procesador	Intel Pentium II, 400 MHz o superior	Intel Dual Core, 1.6 GHz
Sistema Operativo	Linux	Linux
Capacidad de Disco	5.3Gb	160Gb
Memoria	256Mb	4Gb

Luego de haber instalado OpenLDAP se procede con instalar una aplicación que ayudará en su gestión: phpldapadmin. Mediante dicha aplicación será posible gestionar por una sencilla interfaz Web todo lo referente al servidor OpenLDAP; desde la creación del dominio hasta la creación y configuración de los usuarios. Esto simplificará la configuración del servidor; especialmente con el único archivo de configuración con el que se trabajará:

slapd.conf.

8.4.1.3. Implementación del servidor MYSQL

De igual forma que con los anteriores servidores, podemos instalar MySQL de dos maneras: mediante el archivo precompilado o descargando el código fuente. Sin embargo, podemos instalarlo mediante el archivo precompilado, ya que no requerimos realizar ninguna modificación especial.

Una vez instalado el servicio, procederemos a crear una tabla en la que llevaremos a cabo todo el registro de accesos de los usuarios de la red inalámbrica. Para ello, crearemos antes el esquema de trabajo “radius” y dentro de este esquema crearemos la tabla “radacct” con los siguientes campos:

AcctSessionId
AcctUniqueId
UserName
Realm
NASIPAddress
NASPortId
NASPortType

AcctStartTime
AcctStopTime
AcctSessionTime
AcctAuthentic
ConnectInfo_start
ConnectInfo_stop
AcctInputOctets
AcctOutputOctets
CalledStationId
CallingStationId
AcctTerminateCause
ServiceType
FramedProtocol
FramedIPAddress
AcctStartDelay
AcctStopDelay
XascendSessionSvrKey

De todos estos campos, pasaremos a explicar a continuación los que se utilizarán para almacenar información del usuario:

- AcctUniqueId: Identificador único por cada sesión iniciada de accounting entre el servidor de autenticación y el de base de datos.

- UserName: El nombre de usuario registrado por el sistema y que ha hecho acceso a la red inalámbrica.

- NASIPAddress: Dirección IP del punto de acceso inalámbrico desde el cual el usuario ha accedido a la red.

- AcctStartTime: Fecha y hora en la que el usuario ha iniciado su acceso a la red. El formato de la fecha es el siguiente: aaaa-mm-dd; teniendo por aaaa el año,

mm el mes y dd el día. Mientras que el formato de la hora es el siguiente: hh:mm:ss, teniendo por hh la hora, mm el minuto y ss el segundo.

- AcctStopTime: Fecha y hora en la que el usuario ha finalizado su acceso a la red. Los formatos de la fecha y hora son los mismos que los de AcctStartTime.

- AcctSessionTime: Campo en el que se registra el tiempo que estuvo conectado el cliente a la red. Se contabiliza en segundos.

- AcctInputOctets: Número de octetos (bytes) que el usuario ha enviado hacia el punto de acceso, o también conocido como el tráfico de subida del usuario.

- CalledStationId: La dirección MAC y el SSID registrados en el punto de acceso por el cual el usuario ha accedido a la red. El formato en el que se guarda la información es el siguiente: aa-bb-cc-dd-ee-ff:ssid, para el cual el primer parámetro representa la dirección MAC del AP y el segundo el identificador (essid) de la red inalámbrica a la que accedió el usuario.

- CallingStationId: La dirección MAC del equipo desde el cual el usuario ha accedido a la red. El formato es el mismo al anteriormente descrito.

- AcctTerminateCause: La causa por la cual se finalizó de contabilizar y se terminó la conexión del usuario a la red inalámbrica. Se pueden tener dos posibles causas: NAS-Request (a solicitud del AP), o Lost- Carrier. El primer caso se suele dar cuando el usuario ha terminado la conexión, ya sea cerrándola manualmente o apagando su equipo; mientras que el segundo caso se da cuando el usuario ha dejado el área de cobertura del AP.

- AcctStartDelay: Registra si es que ocurrió algún retraso en atender un inicio de contabilizar una sesión. El tiempo que retraso que hubo se almacena en segundos.

- AcctStopDelay: Registra si es que ocurrió algún retraso en atender un fin de contabilizar una sesión. El tiempo que retraso que hubo se almacena en segundos.

Los requerimientos para la implementación del servidor mysql se da a continuación:

Tabla 8.25 Requerimientos del Servidor MySQL

Requerimientos	Mínimos	Óptimos
Procesador	Intel Pentium II, 400 MHz o superior	Intel Dual Core, 1.6 GHz
Sistema Operativo	Linux	Linux
Capacidad de Disco	5Gb	160Gb
Memoria	512Mb	1Gb

8.4.1.4. Implementación del servidor de gestión WEB

Para el servidor de gestión Web se contempla la implementación de dos servicios: el servidor Web Apache y el complemento para procesar páginas PHP por parte de dicho servidor.

De igual forma que con los anteriores servidores, podemos instalar el servidor de gestión Web de dos maneras: mediante el archivo precompilado o descargando el código fuente. Sin embargo, podemos instalarlo mediante el archivo precompilado, ya que no requerimos realizar ninguna modificación especial.
Los requerimientos para la implementación del servidor de gestionWeb son:

Tabla 8.26 Requerimientos del Servidor Web

Requerimientos	Mínimos	Óptimos
Software	Apache 1	Apache 2.2.3
Procesador	Intel Pentium II, 250 MHz o superior	Intel Dual Core, 1.6 GHz
Sistema Operativo	Linux	Linux
Capacidad de Disco	8Gb	160Gb
Memoria	256Mb	1Gb

8.4.2. Instalación de OPENSSL y generación de certificados

Esta es la herramienta que proporciona las herramientas necesarias para crear los certificados y claves que aportan seguridad al sistema IEEE 802.1X. Estos certificados y claves son utilizados para realizar la autenticación de los clientes inalámbricos, pero también se utiliza para aportar seguridad a los servidores Openldap y Apache.

8.4.2.1. Instalación

Se ha conseguido la versión disponible de openssl que es openssl-0.9.7k. La instalación es bastante sencilla. A continuación se muestra la instalación que se ha utilizado:

[root@radius]# cd openssl-0.9.7k
[root@radius open1x]# ./config
[root@radius open1x]# make clean
[root@radius open1x]# make
[root@radius open1x]# make install

8.4.2.2. Generación de Certificados

Lo primero que haremos será crear los certificados apropiados con la ayuda de scripts que se los puede obtener en la siguiente página:

www.karman.homelinux.net /blog/descargas/cascripts.tar.gz

Primero crearemos el certificado raíz: #./CA.root [password], el argumento "password" es opcional, nos pedirá una serie de datos que realmente no son necesarios, con llenar los tres primeros es suficiente, cuando se pregunta por "**common name"**, se debe dejar en blanco. Si todo ha salido bien, nos habrá creado los archivos root.der, root.p12 **y** root.pem.

El siguiente certificado es el del servidor. #./CA.server server-name [password [root-password]], donde server-name es el nombre del servidor RADIUS. password y root-

password son opcionales, pero se recomienda ponerlos, donde password será la contraseña para el certificado que esta creando y root-password es la clave que especifica al crear el certificado raíz, si no se ubico ninguno el solo buscara el archivo root.pass.

Volverán a preguntar una serie de cosas, **cuando se te pregunte por "common name" deberás ubicar el fully-qualified domain name (FQDN)** para saberlo (hostname-fqdn),o (uname-n).

#./CA.server RADIUS, si todo ha ido bien nos habrá creado los archivos RADIUS.pem RADIUS.p12 RADIUS.der, Ahora crearemos el certificado por cada usuario ejecutando e script con dos argumentos, el usuario y la contraseña.

#./CA.client client-name [password [root-password]], donde client-name puede ser el nombre del cliente (lo mejor sería el FQDN del equipo cliente). **Cuando se le pregunte por el "common name"** introduce lo mismo que pusiste en el client-name al invocar el script.

.#/CA.client stalin 123, obviamente, se creara los archivos stalin.der stalin.pem stalin.p12

8.4.2.2.1. Scripts Generación de Certificados

8.4.2.2.1.1. Autoridad Certificadora: CA.root

```
#!/bin/sh
# needed if you need to start from scratch otherwise the CA.pl -newca command doesn't
copy the new
# private key into the CA directories
rm -rf demoCA
echo
"**********************************************************************
**********"
```

```
echo "Creating self-signed private key and certificate"
echo "When prompted override the default value for the Common Name field"
echo
"**********************************************************************
***********"
echo
# Generate a new self-signed certificate.
# After invocation, newreq.pem will contain a private key and certificate
# newreq.pem will be used in the next step
openssl req -new -x509 -keyout newreq.pem -out newreq.pem -passin pass:whatever -
passout pass:whatever
echo
"**********************************************************************
***********"
echo "Creating a new CA hierarchy (used later by the "ca" command) with the
certificate"
echo "and private key created in the last step"
echo
"**********************************************************************
***********"
echo
echo "newreq.pem" | /usr/local/etc/raddb/certs/CA.pl -newca >/dev/null
echo
"**********************************************************************
***********"
echo "Creating ROOT CA"
echo
"**********************************************************************
***********"
echo
# Create a PKCS#12 file, using the previously created CA certificate/key
# The certificate in demoCA/cacert.pem is the same as in newreq.pem. Instead of
```

```
# using "-in demoCA/cacert.pem" we could have used "-in newreq.pem" and then omitted
# the "-inkey newreq.pem" because newreq.pem contains both the private key and certificate
openssl pkcs12 -export -in demoCA/cacert.pem -inkey newreq.pem -out root.p12 -cacerts -passin pass:whatever -passout pass:whatever
# parse the PKCS#12 file just created and produce a PEM format certificate and key in root.pem
openssl pkcs12 -in root.p12 -out root.pem -passin pass:whatever -passout pass:whatever
# Convert root certificate from PEM format to DER format
openssl x509 -inform PEM -outform DER -in root.pem -out root.der
#Clean Up
rm -rf newreq.pem
```

8.4.2.2.1.2. Servidor: CA.server

```
#!/bin/sh
echo
"**********************************************************************
***********"
echo "Creating server private key and certificate"
echo "When prompted enter the server name in the Common Name field."
echo
"**********************************************************************
***********"
echo
# Request a new PKCS#10 certificate.
# First, newreq.pem will be overwritten with the new certificate request
openssl req -new -keyout newreq.pem -out newreq.pem -passin pass:whatever -passout pass:whatever
# Sign the certificate request. The policy is defined in the openssl.cnf file.
# The request generated in the previous step is specified with the -infiles option and
# the output is in newcert.pem
```

The -extensions option is necessary to add the OID for the extended key for server authentication

openssl ca -policy policy_anything -out newcert.pem -passin pass:whatever -key whatever -extensions xpserver_ext -extfile xpextensions -infiles newreq.pem

Create a PKCS#12 file from the new certificate and its private key found in newreq.pem

and place in file specified on the command line

openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -out $1.p12 -clcerts -passin pass:whatever -passout pass:whatever

parse the PKCS#12 file just created and produce a PEM format certificate and key in certsrv.pem

openssl pkcs12 -in $1.p12 -out $1.pem -passin pass:whatever -passout pass:whatever

Convert certificate from PEM format to DER format

openssl x509 -inform PEM -outform DER -in $1.pem -out $1.der

Clean Up

rm -rf newert.pem newreq.pem

8.4.2.2.1.3. Cliente: CA.client

#!/bin/sh

echo

"**********"

echo "Creating client private key and certificate"

echo "When prompted enter the client name in the Common Name field. This is the same"

echo " used as the Username in FreeRADIUS"

echo

"**********"

echo

Request a new PKCS#10 certificate.

First, newreq.pem will be overwritten with the new certificate request

openssl req -new -keyout newreq.pem -out newreq.pem -passin pass:whatever -passout pass:whatever

Sign the certificate request. The policy is defined in the openssl.cnf file.
The request generated in the previous step is specified with the -infiles option and
the output is in newcert.pem
The -extensions option is necessary to add the OID for the extended key for client authentication

openssl ca -policy policy_anything -out newcert.pem -passin pass:whatever -key whatever -extensions xpclient_ext -extfile xpextensions -infiles newreq.pem
Create a PKCS#12 file from the new certificate and its private key found in newreq.pem
and place in file specified on the command line
openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -out $1.p12 -clcerts -passin pass:whatever -passout pass:whatever
parse the PKCS#12 file just created and produce a PEM format certificate and key in certclt.pem
openssl pkcs12 -in $1.p12 -out $1.pem -passin pass:whatever -passout pass:whatever
Convert certificate from PEM format to DER format
openssl x509 -inform PEM -outform DER -in $1.pem -out $1.der
clean up
rm -rf newcert newreq.pem

8.4.2.2.1.4. CA.pl

#!/usr/bin/perl
#
CA - wrapper around ca to make it easier to use ... basically ca requires
some setup stuff to be done before you can use it and this makes
things easier between now and when Eric is convinced to fix it :-)
#
CA -newca ... will setup the right stuff

```
# CA -newreq[-nodes] ... will generate a certificate request
# CA -sign ... will sign the generated request and output
#
# At the end of that grab newreq.pem and newcert.pem (one has the key
# and the other the certificate) and cat them together and that is what
# you want/need ... I'll make even this a little cleaner later.
#
#
# 12-Jan-96 tjh    Added more things ... including CA -signcert which
#                  converts a certificate to a request and then signs it.
# 10-Jan-96 eay    Fixed a few more bugs and added the SSLEAY_CONFIG
#                  environment variable so this can be driven from
#                  a script.
# 25-Jul-96 eay    Cleaned up filenames some more.
# 11-Jun-96 eay    Fixed a few filename missmatches.
# 03-May-96 eay    Modified to use 'ssleay cmd' instead of 'cmd'.
# 18-Apr-96 tjh    Original hacking
#
# Tim Hudson
# tjh@cryptsoft.com
#

# 27-Apr-98 snh    Translation into perl, fix existing CA bug.
#
#
# Steve Henson
# shenson@bigfoot.com

# default openssl.cnf file has setup as per the following
# demoCA ... where everything is stored
$SSLEAY_CONFIG=$ENV{"SSLEAY_CONFIG"};
$DAYS="-days 365";
$REQ="openssl req $SSLEAY_CONFIG";
```

```
$CA="openssl ca $SSLEAY_CONFIG";
$VERIFY="openssl verify";
$X509="openssl x509";
$PKCS12="openssl pkcs12";

$CATOP="./demoCA";
$CAKEY="cakey.pem";
$CACERT="cacert.pem";
$DIRMODE = 0777;
$RET = 0;

foreach (@ARGV) {
        if ( /^(-\?|-h|-help)$/ ) {
           print STDERR "usage: CA -newcert|-newreq|-newreq-nodes|-newca|-sign|-
verify\n";
           exit 0;
        } elsif (/^-newcert$/) {
           # create a certificate
           system ("$REQ -new -x509 -keyout newreq.pem -out newreq.pem $DAYS");
           $RET=$?;
           print "Certificate (and private key) is in newreq.pem\n"
        } elsif (/^-newreq$/) {
           # create a certificate request
           system ("$REQ -new -keyout newreq.pem -out newreq.pem $DAYS");
           $RET=$?;
           print "Request (and private key) is in newreq.pem\n";
        } elsif (/^-newreq-nodes$/) {
           # create a certificate request
           system ("$REQ -new -nodes -keyout newreq.pem -out newreq.pem $DAYS");
           $RET=$?;
           print "Request (and private key) is in newreq.pem\n";
        } elsif (/^-newca$/) {
                # if explicitly asked for or it doesn't exist then setup the
```

```
        # directory structure that Eric likes to manage things

    $NEW="1";

    if ( "$NEW" || ! -f "${CATOP}/serial" ) {
        # create the directory hierarchy
        mkdir $CATOP, $DIRMODE;
        mkdir "${CATOP}/certs", $DIRMODE;
        mkdir "${CATOP}/crl", $DIRMODE ;
        mkdir "${CATOP}/newcerts", $DIRMODE;
        mkdir "${CATOP}/private", $DIRMODE;
        open OUT, ">${CATOP}/serial";
        print OUT "01\n";
        close OUT;
        open OUT, ">${CATOP}/index.txt";
        close OUT;
    }
    if ( ! -f "${CATOP}/private/$CAKEY" ) {
        print "CA certificate filename (or enter to create)\n";
        $FILE = <STDIN>;

        chop $FILE;

        # ask user for existing CA certificate
        if ($FILE) {
           cp_pem($FILE,"${CATOP}/private/$CAKEY", "PRIVATE");
           cp_pem($FILE,"${CATOP}/$CACERT", "CERTIFICATE");
           $RET=$?;
        } else {
           print "Making CA certificate ...\n";
           system ("$REQ -new -x509 -keyout " .
                "${CATOP}/private/$CAKEY      -out      ${CATOP}/$CACERT
$DAYS");
```

```
            $RET=$?;
        }
    }
} elsif (/^-pkcs12$/) {
    my $cname = $ARGV[1];
    $cname = "My Certificate" unless defined $cname;
    system ("$PKCS12 -in newcert.pem -inkey newreq.pem " .
                "-certfile ${CATOP}/$CACERT -out newcert.p12 " .
                "-export -name \"$cname\"");
    $RET=$?;
    exit $RET;
} elsif (/^-xsign$/) {
    system ("$CA -policy policy_anything -infiles newreq.pem");
    $RET=$?;

} elsif (/^(-sign|-signreq)$/) {
    system ("$CA -policy policy_anything -out newcert.pem " .
                                        "-infiles newreq.pem");
    $RET=$?;
    print "Signed certificate is in newcert.pem\n";
} elsif (/^(-signCA)$/) {
    system ("$CA -policy policy_anything -out newcert.pem " .
                                "-extensions v3_ca -infiles newreq.pem");
    $RET=$?;
    print "Signed CA certificate is in newcert.pem\n";
} elsif (/^-signcert$/) {
    system ("$X509 -x509toreq -in newreq.pem -signkey newreq.pem " .
                                                "-out tmp.pem");
    system ("$CA -policy policy_anything -out newcert.pem " .
                                        "-infiles tmp.pem");
    $RET = $?;
    print "Signed certificate is in newcert.pem\n";
} elsif (/^-verify$/) {
```

```
        if (shift) {
            foreach $j (@ARGV) {
                system ("$VERIFY -CAfile $CATOP/$CACERT $j");
                $RET=$? if ($? != 0);
            }
            exit $RET;
        } else {
                system ("$VERIFY -CAfile $CATOP/$CACERT newcert.pem");
                $RET=$?;
                exit 0;
        }
    } else {
        print STDERR "Unknown arg $_\n";
        print STDERR "usage: CA -newcert|-newreq|-newreq-nodes|-newca|-sign|-
verify\n";
        exit 1;
    }
}

exit $RET;

sub cp_pem {
my ($infile, $outfile, $bound) = @_;
open IN, $infile;
open OUT, ">$outfile";
my $flag = 0;
while (<IN>) {
    $flag = 1 if (/^-----BEGIN.*$bound/) ;
    print OUT $_ if ($flag);
    if (/^-----END.*$bound/) {
            close IN;
            close OUT;
            return;
```

8.4.3. Configuración de OpenLDAP como base de datos de usuario

Lo primero que hay que hacer es instalar el demonio slapd del servidor OPENLDAP e instalar ldap-utils, un paquete que contiene utilidades de administración de LDAP.
La instalación se hace con el comando:

sudo apt-get install slapd ldap-utils

Sólo bastará con digitar la contraseña de administración y el paquete se instalará correctamente.

8.4.3.1. Configuración de LDAP

Desde las últimas versiones de ldap el archivo de configuración que habitualmente estaba ubicado en /etc/openlap/ldap.conf, no se incluye, por el contrario la configuración es automática durante la instalación del ldap-utils, además para que el servidor trabaje sobre protocolo seguro anteriormente era necesario configurar SSL (SSL permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes.), pero en las nuevas versiones no es necesario ya que el paquete trae incluido dicha opción, sin embargo es recomendable reconfigurar el servidor para adecuarlo aún más a lo que deseamos, esto se lleva a cabo con la siguiente instrucción:

sudo dpkg-reconfigure slapd

Una vez digitamos esta instrucción se abren una serie de opciones para configurar adecuadamente el servidor.

En este cuadro de diálogo debemos escoger la opción de lo contrario no podríamos modificar las opciones de configuración del servidor

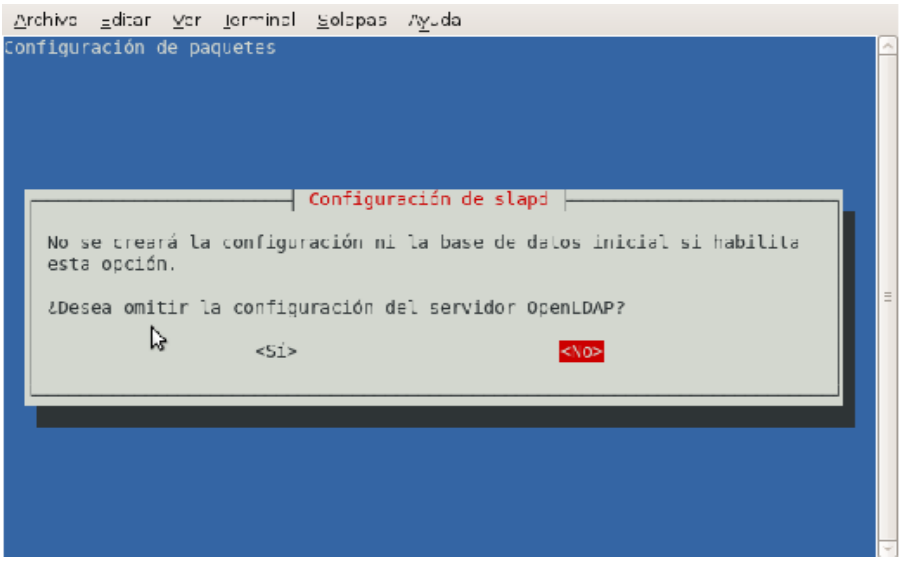


Figura 8.44 Configuración de slapd: Configuración del servidor OpenLDAP

En este cuadro de diálogo digitamos el dominio de nuestro servidor radius.com

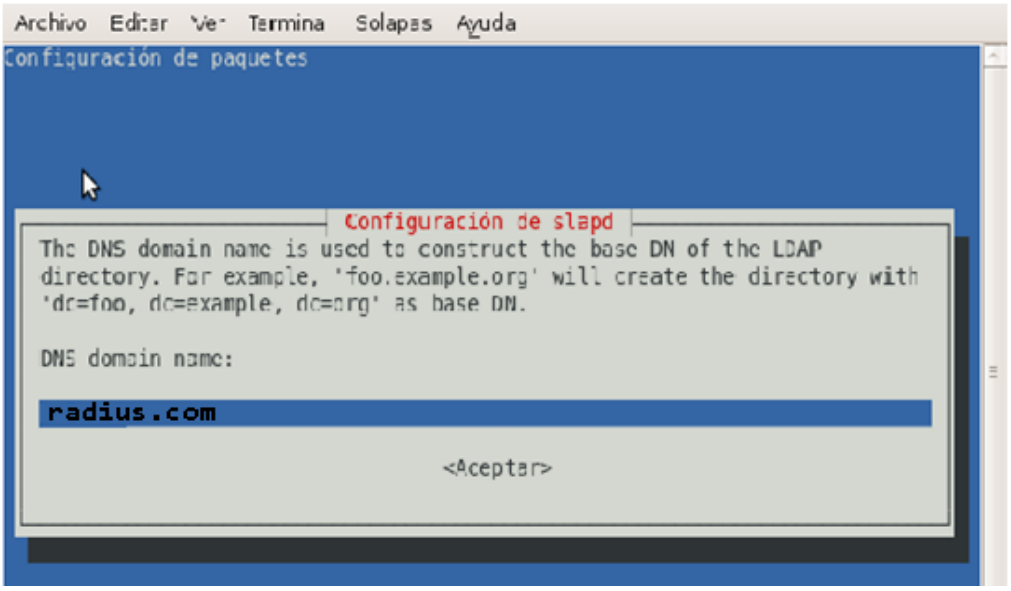


Figura 8.45 Configuración de slapd: Dominio del servidor

Ahora se nos pide el nombre de la organización que para este caso es igualmente radius.com

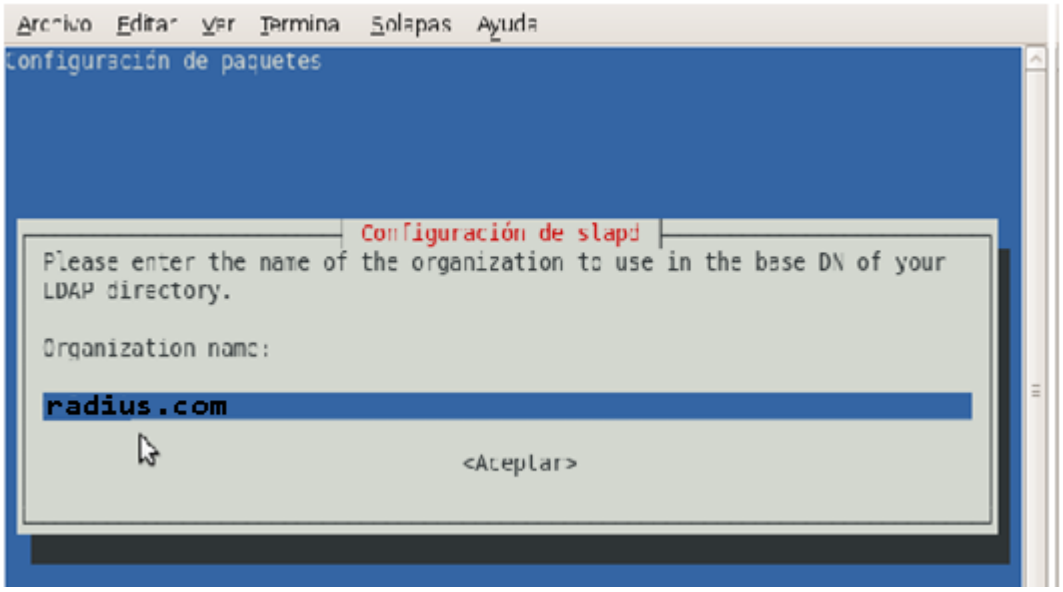


Figura 8.46 Configuración de slapd: Nombre de la Organización

En esta instancia se nos pide escoger el tipo de base de datos backbend (dorsal o base de datos de segundo plano)

Si se lee la explicación que da el cuadro de diálogo se observa que se recomienda utilizar la base de datos HDB y no la BDB, y también la justificación de porque escoger dicha opción.

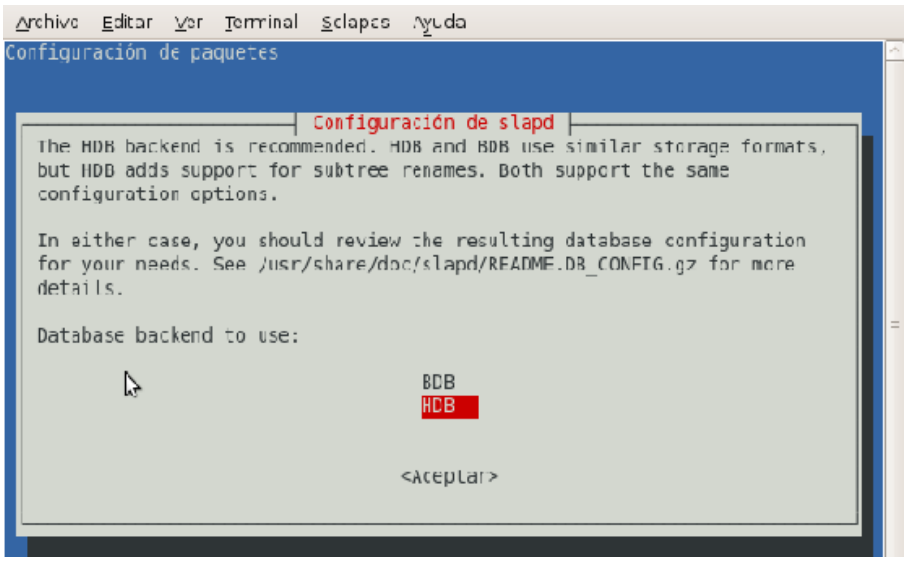


Figura 8.47 Configuración de slapd: Utilización de las Bases de Datos

Ante la pregunta de si desea que se borre la base de datos cuando se purgue el paquete slapd, se escoge que no.

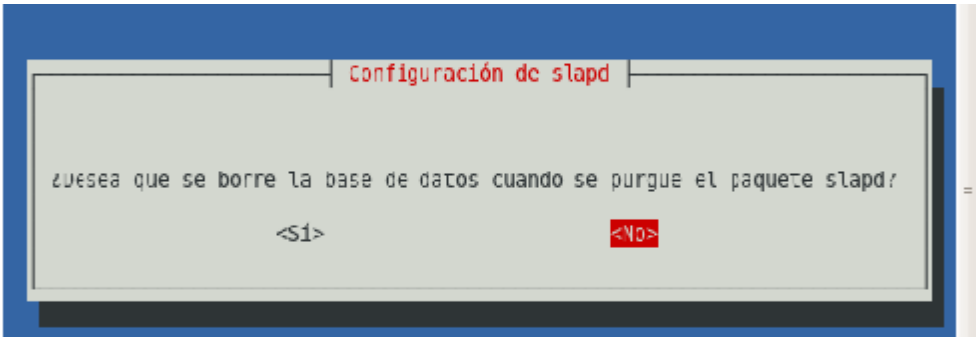


Figura 8.48 Configuración de slapd: Eliminación de datos del paquete slapd

En este nuevo cuadro de diálogo se escoge la opción NO

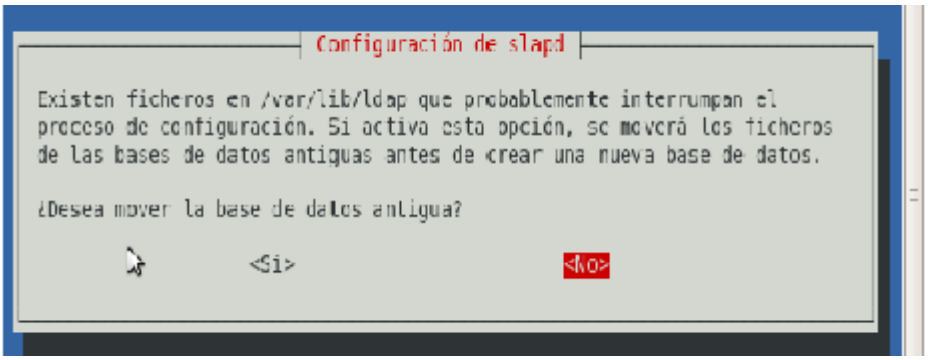


Figura 8.49 Configuración de slapd: Se desea mover la Base de Datos antigua

Digitamos la contraseña del administrador (root)

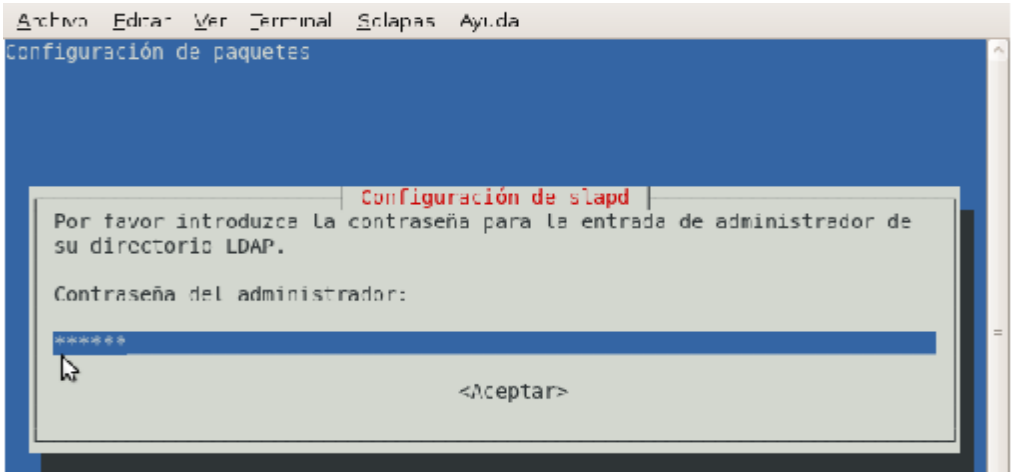


Figura 8.50 Configuración de slapd: Contraseña del Administrador

Confirmamos la contraseña

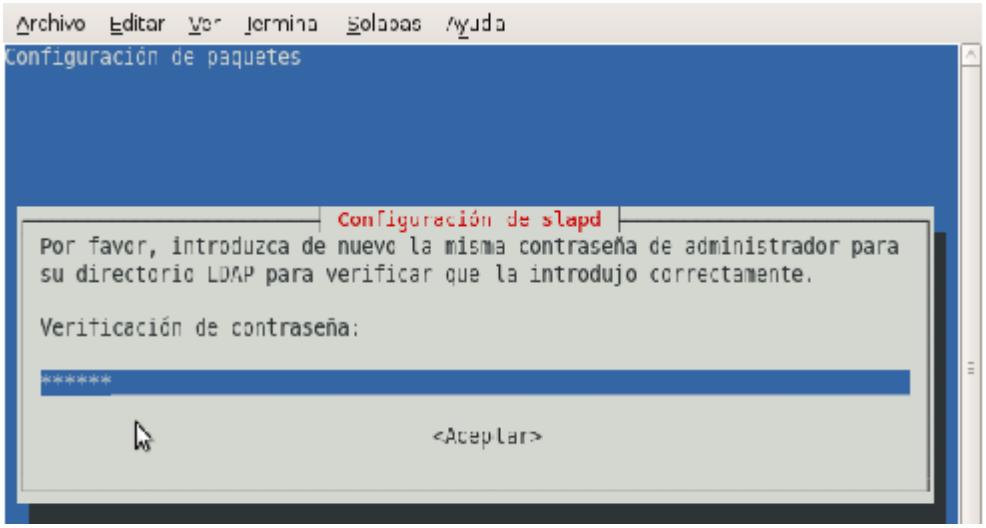


Figura 8.51 Configuración de slapd: Confirmación de contraseña

Con esto hemos terminado de configurar ldap

8.4.3.2. Construcción del Árbol Ldap

Tras haber configurado el servidor ldap procedemos a construir el árbol ldap. La estructura y los datos del árbol ldap, se almacenan en un fichero con formato .ldif. El árbol para es el siguiente:

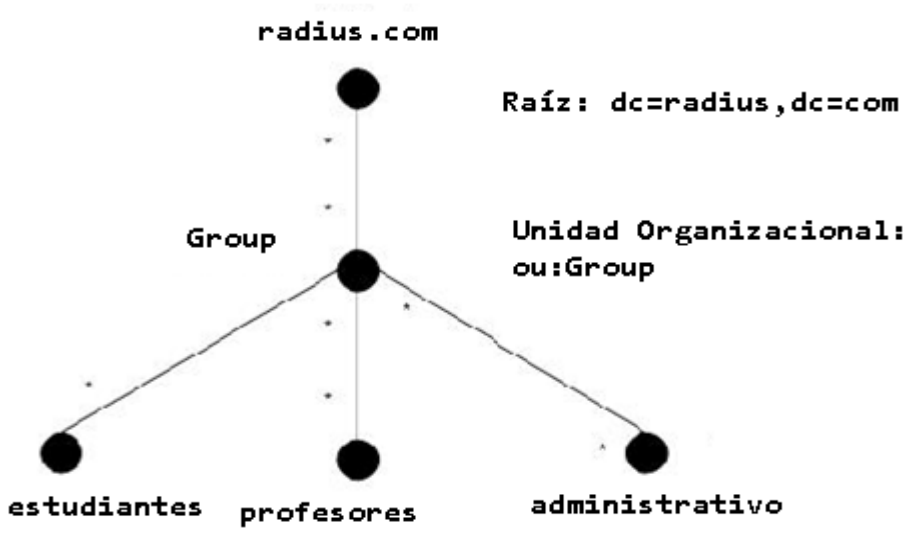


Figura 8.52 Construcción de Árbol LDAP

Abrimos un editor bien sea con vi o con nano, y comenzamos a construir el fichero .ldif:

sudo nano radius.com.ldif

Comenzamos a llenar el árbol digitando primero la raíz (dc=radius,dc=com), la unidad organizacional (ou=Group), y los objetos persona (objectClass=person)

#Se define la raíz del árbol

dn: dc=radius,dc=com
dc=radius,dc=com
objectClass: top
objectClass: organization
#Se define la unidad organizacional para el árbol
dn: ou=usuarios,dc=radius,dc=com
objectClass: organizationalUnit
ou: usuarios

#Se define el conjunto de usuarios

dn: uid=saguilar,ou=estudiante,dc=radius,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
uid: saguilar
sn: Aguilar
givenName: Puchaicela
cn: Stalin Aguilar
displayName: Stalin Aguilar
uidNumber: 1001
gidNumber: 1001
userPassword: {CRYPT}mb/RUPYgkZ11o

gecos: Stalin Aguilar
loginShell: /bin/bash
homeDirectory: /home/ichiro
mail: saguilar@radius.com

#Aca se agregara a un nuevo usuario: Jhanet Moncayo

dn: uid=jMoncayo,ou=estudiante,dc=radius,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
uid: jMoncayo
sn: Moncayo
givenName: Jhanet
cn: Jhanet Moncayo
displayName: Jhanet Moncayo
uidNumber: 1003
gidNumber: 1003
userPassword: {CRYPT}mbq1AsI5f3xq.
gecos: Jhanet Moncayo
loginShell: /bin/bash
homeDirectory: /home/ichiro
mail: jMoncayo@radius.com

Tras digitar esto en el archivo lo almacenamos con el nombre de radius.com.ldif, o con el nombre que se desee.

Ahora ejecutamos la orden:

ldapadd -x -D cn=admin,dc=radius,dc=com -W -f radius.com.ldif

Esto lo hacemos con el fin de agregar el fichero al directorio LDAP

8.4.3.2.1. Hacer Búsquedas

Teniendo ya la información de nuestro árbol en el directorio ldap, podemos hacer búsquedas, estas se hacen con el comando ldapsearch, por ejemplo para mostrar la información de todos los usuarios:

ldapsearch -xLLL -b "dc=radius, dc=com", esto muestra la información del árbol, todos los usuarios, con todos sus datos, para buscar el mail, el common name cn, surname, de un usuario específico. Si el usuario fuese Jhanet Corredor. Se digita:

ldapsearch -xLLL -b "dc=radius,dc=com" uid=aCorredor mail cn sn

De esta manera podemos hacer cualquier tipo de búsqueda en nuestro directorio ldap, de acuerdo a la estructura que hayamos definido ldap-utils ofrece una serie de herramientas para modificar, agregar, consultar, entre otras acciones en el directorio ldap:

ldapadd: ldapadd abre una conexión a un servidor LDAP, enlaza y añade entradas.
ldapcompare: ldapcompare abre una conexión a un servidor LDAP, enlaza y hace una comparación usando los parámetros especificados.
ldapdelete: ldapdelete abre una conexión a un servidor LDAP, enlaza y borra una o mas entradas.
ldapmodify: ldapmodify abre una conexión a un servidor LDAP, enlaza y modifica entradas.
ldapmodrdn: ldapmodrdn abre una conexión a un servidor LDAP, enlaza y modifica el RDN de las entradas.
ldappasswd: ldappasswd es una herramienta para establecer la contraseña de un usuario LDAP.
ldapsearch: ldapsearch abre una conexión a un servidor LDAP, enlaza y hace una búsqueda usando los parámetros especificados.
ldapwhoami: ldapwhoami abre una conexión a un servidor LDAP, enlaza y realiza una operación whoami.

8.4.3.2.2. Iniciar, Detener, Reiniciar El Servidor Ldap

Muchas veces necesitaremos detener, reniciar y iniciar el servidor para que ciertos cambios surjan efecto, los comandos para realizarlo son los siguientes

- Reiniciar el servidor:

sudo /etc/init.d/slapd restart

- Detener el servidor:

sudo /etc/init.d/slapd stop

- Iniciar el servidor:

sudo /etc/init.d/slapd start

8.4.3.3. Ingreso de datos en la base de datos LDAP

Inicie su programa navegador web (Internet Explorer, Netscape Navigator ™, Mozilla Firefox). Escriba la dirección IP y HTTP en el puerto del Ldap en el campo de la dirección (http://127.0.0.1/phpldapadmin/) y pulse Enter.

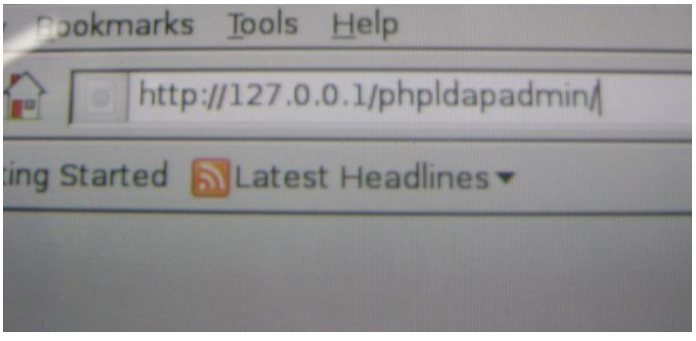


Figura 8.53 Dirección IP del Ldap

Después de establecida la conexión, verá la ventana de identificación del usuario como se muestra.

- Escriba cn = admin, dc = radius, dc = com en el campo Login DN
- Escribir la contraseña en el campo de password
- Haga clic en Authenticate

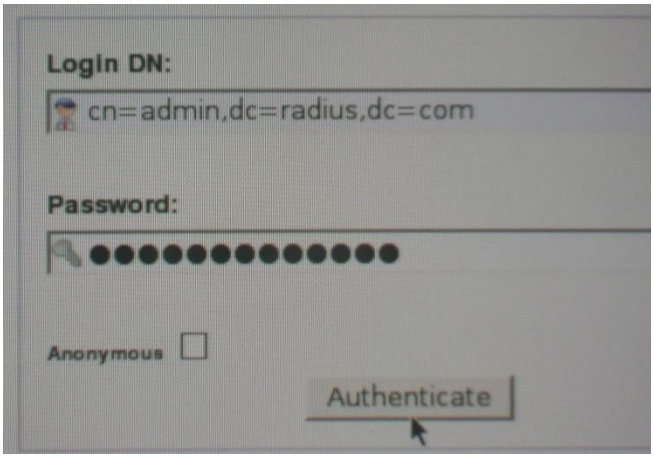


Figura 8.54 Autenticación del LDAP

Luego se muestran los grupos que existen en la base de datos LDAP.

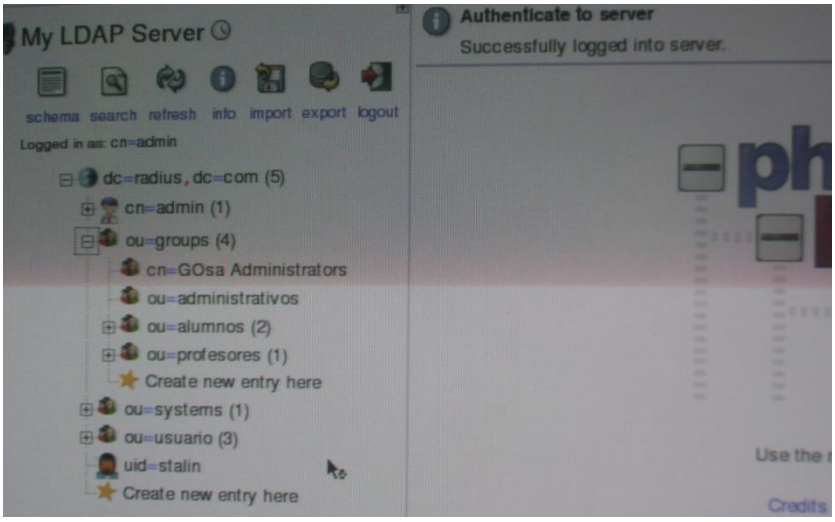


Figura 8.55 Grupos existentes en la base de datos LDAP

Se escoge un grupo y se pone **CREATE NEW ENTRY HERE** para crear un nuevo usuario en ese grupo

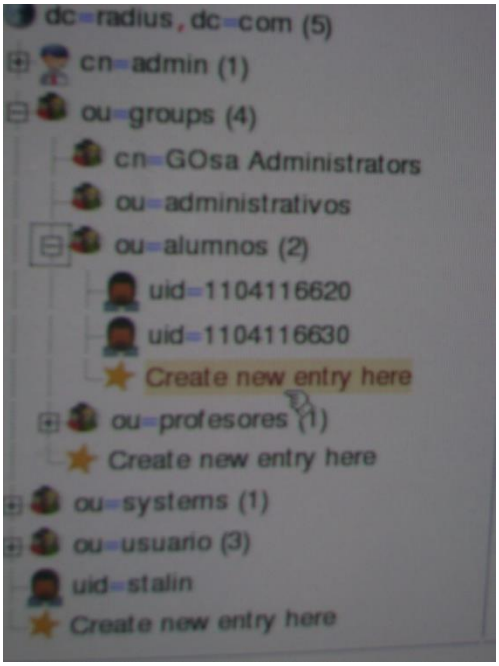


Figura 8.56 Creación de un nuevo usuario en la base de datos l LDAP

Luego se llenan los espacios de **USER NAME Y PASSWORD** y finalmente se hace clic en **CREATE OBJECT** y el nuevo usuario esta agregado en el grupo escogido

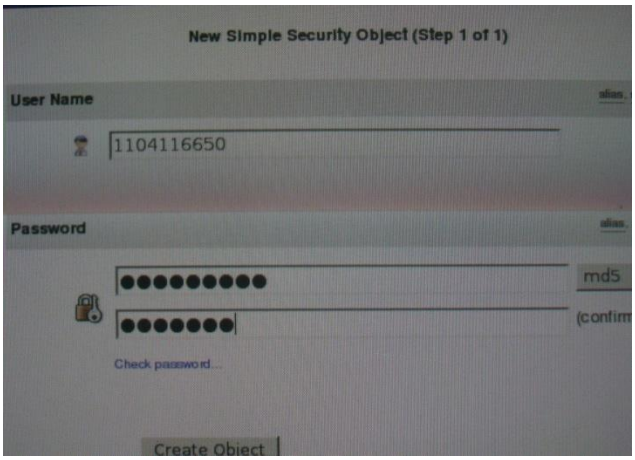


Figura 8.57 Ingreso de datos del nuevo usuario

8.4.4. Instalación de MYSQL

Ya que tenemos instalado y funcionando freeradius, instalaremos MySQL con el fin de reemplazar la configuración de usuarios y clientes y los logs de accounting que por defecto se hacen en archivos de texto, por una base de datos que permita una mejor administración de estos.

Primero debemos proceder a instalar MySQL. En esta ocasión instalaremos la versión 5.1 utilizando apt-get:

```
root@radius:~# apt-get install mysql-server-5.1
```

Luego de instalar MySQL debemos crear la base de datos que utilizará freeradius. Para esto ingresamos a la shell de MySQL ejecutando como root:

```
root@radius:~# mysql –u root –p
Insert password:*******

Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 4 to server version: 4.1.15-log
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql>
```

Luego ejecutamos las siguientes instrucciones SQL, debe crear una base de datos con el nombre radius, un usuario con nombre radius con todos los permisos sobre esta base de datos y la asignación de un password=radius:

```
mysql> create database radius;
mysql> grant all privileges on radius.* to radius@localhost;
mysql> set password for radius@localhost = old_password('radius');
```

Ahora debemos proceder a crear la base de datos. Para esto freeradius provee un script sql que puede ser encontrado en el directorio freeradius-server 1.1.1/doc/examples/mysql.sql.

Para ejecutar el script, podemos hacerlo directamente desde MySQL:

```
mysql> connect radius;
mysql> \. /home/user/freeradius-server 1.1.1/doc/examples/mysql.sql
```

Para ver la estructura de las tablas podemos utilizar los siguientes comandos:

mysql> show tables;

Ahora debemos poblar la base de datos con algún usuario y cliente (NAS) de prueba:
mysql> insert into radgroupcheck values (", 'admin', 'Auth-Type', ':=', 'Local');
mysql> insert into radgroupreply values (", 'admin', 'Framed-Protocol', ':=', 'PPP');
mysql> insert into radgroupreply values (", 'admin', 'Service-Type', ':=', 'Framed-User');
mysql> insert into radgroupreply values (", 'admin', 'Framed-Compression', ':=', 'Van-Jacobsen-TCP-IP');
mysql> insert into usergroup values ('saguilar', 'admin',");
mysql> insert into radcheck values (", 'saguilar', 'Password', '==', 'saguilar');
mysql> insert into radreply values (", 'saguilar', 'Framed-IP-Address', ':=', '192.168.100.50');
mysql> insert into nas values (", 'test',NULL, '3coml',NULL, 'radiusAEIRNNR', NULL, NULL);

Con esto hemos creado un usuario saguilar con password saguilar, el cual pertenece al grupo admin que posee un conjunto de atributos determinados. Además hemos agregado un NAS de nombre test, tipo 3coml, y secret radiusAEIRNNR.

Debemos configurar el acceso a la base de datos, indicándole a freeradius cual es la IP del servidor MySQL, el usuario y el password. Esto lo haremos en el archivo sql.conf, en donde deberemos modificar las siguientes líneas:

# Connect info
server = "localhost"
login = "radius"
password = "radius"

# Database table configuration
radius_db = "radius"

Donde localhost corresponde a la dirección del servidor MySQL, login es el nombre de usuario y su password para acceder a la base de datos, y radius_db corresponde al

nombre de la base de datos que hemos creado para freeradius. Luego en el archivo radius.conf configuraremos freeradius para que deje de ocupar los archivos y comience a ocupar MySQL. Para esto modificaremos las siguientes secciones del archivo, las cuales se encuentran al final de este:

authorize {
preprocess
chap
mschap
suffix
eap
sql
}
authenticate {
Auth-Type PAP {
pap
}
Auth-Type CHAP {
chap
}
Auth-Type MS-CHAP {
mschap
}
}
preacct {
preprocess
acct_unique
suffix
}
accounting {
detail
radutmp
sql

```
}
session {
radutmp
sql
}
post-auth {
sql
}
pre-proxy {
}
post-proxy {
eap
}
```

Finalmente echamos a correr nuestro freeradius con MySQL.

Ahora que tenemos todo en su sitio haremos el correcto funcionamiento, ejecutando #radiusd –X

Lo que nos dará una salida detallada del arranque.

```
Starting - reading configuration files ...
Using deprecated naslist file. Support for this will go away soon.
Module: Loaded exec
rlm_exec: Wait=yes but no output defined. Did you mean output=none?
Module: Instantiated exec (exec)
Module: Loaded expr
Module: Instantiated expr (expr)
Module: Loaded PAP
Module: Instantiated pap (pap)
Module: Loaded CHAP
Module: Instantiated chap (chap)
Module: Loaded MS-CHAP
```

Module: Instantiated mschap (mschap)
Module: Loaded SQL
rlm_sql (sql): Driver rlm_sql_mysql (module rlm_sql_mysql) loaded and linked
rlm_sql (sql): Attempting to connect to radius@localhost:/radius
rlm_sql (sql): starting 0
rlm_sql (sql): Attempting to connect rlm_sql_mysql #0
rlm_sql_mysql: Starting connect to MySQL server for #0
rlm_sql (sql): Connected new DB handle, #0
Initializing the thread pool...

Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.

8.4.4.1. Ingreso de datos en la base de datos MYSQL

Inicie su programa navegador web (Internet Explorer, Netscape Navigator ™, Mozilla Firefox). Escriba la dirección IP y HTTP en el puerto del Mysql en el campo de la dirección (http://127.0.0.1/daloradius) y pulse Enter.

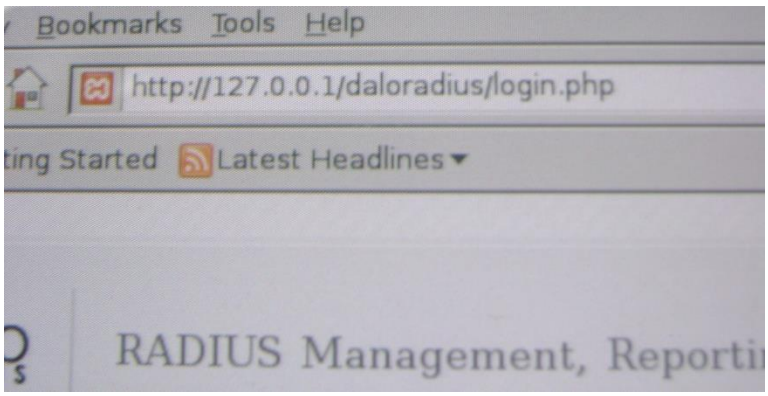


Figura 8.58 Dirección IP del MYSQL

Después de establecida la conexión, verá la ventana de identificación del usuario como se muestra.

- Escriba administrador en el campo user name

- Escribir la contraseña en el campo de password
- Haga clic en login

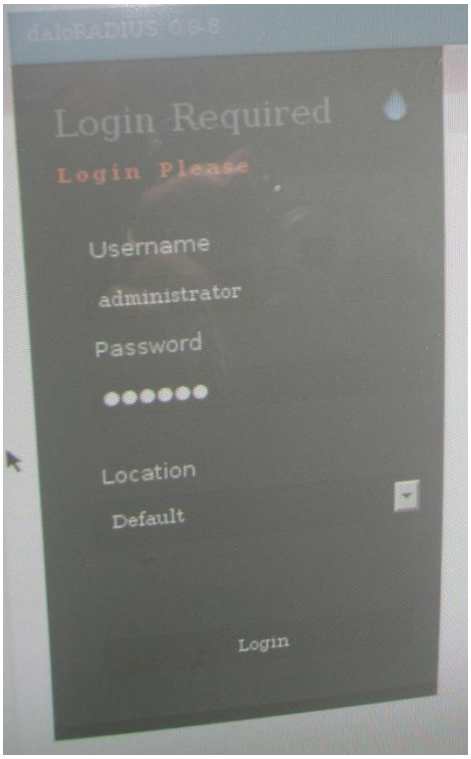


Figura 8.59 Autenticación de la base de datos MYSQL

Luego se muestran la pantalla en la cual se debe escoger new users para crear el nuevo usuario.

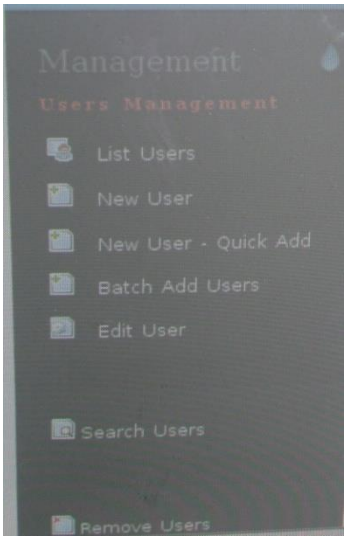


Figura 8.60 Creación de un nuevo usuario

Luego se llenan los espacios de User name y password y el grupo (ya sea administrativo, profesor o alumno), finalmente se hace clic en apply y el nuevo usuario esta agregado en el grupo escogido

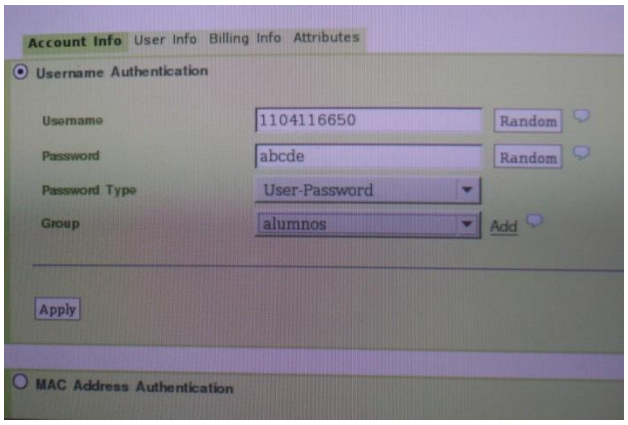


Figura 8.61 Ingreso de datos del nuevo usuario en la base de datos Mysql

8.4.5. Instalación de FRERADIUS como servidor AAA

8.4.5.1. Instalación

Para montar Frerradius se ha utilizado Debian 5. La implementación se puede llevar a cabo en todas las distribuciones Linux, aquí solo se centrara en instalar y configurar en Debian, con lo que es posible que algunos comandos cambien, así como la localización de muchos archivos.

Existen dos formas de instalar Freeradius en Debian

1. Desde repositorios oficiales

apt-get install freeradius

Aunque esta forma no es la mas indicada ya que por un problema con la licencia de OpenSSL el binario oficial de debían no incluye soporte para SSL.

2. Desde las fuentes (RECOMENDADO)

Esta es la manera mas indicada para instalar. Para ello debes seguir estos pasos:
Necesita instalar dpkg-dev, gcc, libc6, make para ello:

apt-get install dpkg-dev
apt-get install libssl-dev gcc libc6-dev make

Lo que se instala es en el sistema es el compilador gcc (GNU Compiler Collection, antes GNU C Compiler), además la libreriac6-dev Library Development Libraries and Header Files con esto el sistemas quedara en condiciones de crear los archivos ejecutables, finalmente instalamos make para que las compilaciones se puedan ejecutar.
Instalamos dependencias de freeradius con:

apt-get install build-essential fakeroot,
apt-get build-dep freeradius

Descargar las fuentes freeradius-server desde la versión 2.1.1

Una vez descargado:

[root@pfc05 open1x]#tar xfvz freeradius-server-2.1.1.tar.gz
[root@pfc05 open1x]#cd freeradius-2.1.1

El proceso de instalación del servidor es como sigue, como en el caso de openssl, se ha conseguido la versión más nueva de Freeradius disponible.

[root@pfc05 open1x]#./ configure --prefix=/ --with-openssl-includes=/Dir_Base/open1x/openssl/include --with-openssl-libraries=/Dir_Base/open1x/openssl/lib
[root@pfc05 open1x]# make clean
[root@pfc05 open1x]# make
[root@pfc05 open1x]# make install

8.4.5.2. Configuración

Los archivos de configuración del servidor Freeradius están en el directorio etc/raddb.

clients.conf

Cambio del SECRET:
secret = test
Esta es la palabra secreta que se utilizará para encriptar la comunicación con el cliente, que en este caso será el punto de acceso.

A continuación, se introduce el cliente con el que se conectará el servidor, es decir, el punto de acceso:

```
client 10.0.0.1
{
secret = test
shortname = ap1
}

client 127.0.0.1
{
secret = test
}
```

Asi es como hay que configurar un cliente. Ya viene con 127.0.0.1, que podemos modificar o borrar para que sirva a nuestros propósitos. En todo caso, con el que el clients.conf tenga solamente las líneas anteriormente mostradas será suficiente para funcionar. Nótese de cambiar la ip en el campo client por la del punto de acceso y cambiar el campo secret por una contraseña que se desee ubicar.

radiusd.conf

Se va a utilizar LDAP para la autorización y la autenticación, por lo que se debe descomentar la opción de ldap tanto en la parte de authorize como en la de authenticate:

```
authorize
{
eap
ldap
}
authenticate
{
Auth-Type LDAP
{
ldap
}
eap
}
```

Ahora se deben introducir los datos de LDAP en el apartado de LDAP de radiusd.conf:

```
Ldap
{
server = "127.0.0.1"
identity = "cn=root,dc=radius,dc=com"
password = radius
basedn = "dc=radius,dc=com"
}
```

eap.conf

Este archivo no existía en versiones anteriores de freeradius, sino que se encontraba dentro del archivo radius.conf. En este archivo se configura la parte concerniente a EAP.

En principio, se pondrá por defecto el modo de autenticación eap-ttls, pero más adelante se puede cambiarlo en función de lo que nos pueda interesar:
default_eap_type = ttls

En este proyecto se utiliza el tipo ttls, así que se necesita modificar los módulos tls y ttls. A continuación se introduce la parte del archivo eap.conf perteneciente a tls.

```
md5
{
}
tls
{
private_key_password = client
private_key_file = ${raddbdir}/certs/RADIUS.pem
certificate_file = ${raddbdir}/certs/RADIUS.pem
CA_file = ${raddbdir}/certs/root.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
fragment_size = 1024
include_length = yes
}
```

Sera conveniente hacer un usuario para el servidor radius añadiendo las siguientes líneas a nuestro password, shadow y group

```
nano /etc/password:  freerad:x:106:106:/etc/raddb:/bin:false
nano /etc/shadow:  freerad:!:13611:0:99999:7:::
nano /etc/group:  freerad:x:106:
```

Y de cambiar de usuario y los permisos de todos los archivos de /etc/raddb:

```
#chmod  700 –R /etc/raddb
#chown  -R  frerad:freerad  /etc/raddb
```

Por defecto el servidor crea un cliente de nombre y password test y un secret =testing123

Ahora podemos realizar un pequeño test de conexión con la utilidad **radtest** que viene con freeradius:

#radtest test test localhost 0 testing123
Sending Access-Request of id 88 to 127.0.0.1 port 1812
User-Name = "test"
User-Password = "test"
NAS-IP-Address = 255.255.255.255
NAS-Port = 0
Re-sending Access-Request of id 88 to 127.0.0.1 port 1812
User-Name = "test"
User-Password = "test"
NAS-IP-Address = 255.255.255.255
NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1:1812, id=88, length=20

Radtest envía un Access-Request, el cual fue recibido por freeradius y contestado con un Access-Reject. Con esto podemos verificar que el servidor se está ejecutando de manera correcta.

8.4.6. Implementación de la Solución Inalámbrica

Para implementar la solución inalámbrica se tuvo que hacer primero un análisis costo-beneficio acerca de los equipos existentes en cada área y cuáles serían los más óptimos para poder realizar la implementación en cada una de ellas.

8.4.6.1. Análisis costo-beneficio de la solución inalámbrica de la Universidad Nacional de Loja.

La intención de realizar un análisis costo-beneficio dentro de esta tesis trae consigo el poder identificar que características tienen los distintos equipos (puntos de acceso) de las diferentes áreas que tiene la Universidad Nacional de Loja y de acuerdo a estas

características poder reconocer cuales de éstas aportan un beneficio significativo para la solución y cuanto sería la diferencia en costos con respecto a la que no lo tenga.

A continuación se detallara el análisis de los equipos existentes en diferentes Área de la Universidad Nacional de Loja, de esta forma se determinara el grado de seguridad con la que cuentas los mismos.

8.4.6.1.1. Análisis costo-beneficio del Área Agropecuaria y de Recursos Naturales Renovable.

Dentro de la red de datos del AARNR se considerarán equipos pertenecientes fabricantes de networking: DLink debido a la fuerte inclinación de esta área por dichos equipos.

En la fase de análisis se menciono los equipos inalámbricos existentes que posee esta Área, para ello analizaremos 2 tipos de equipos acordes a las necesidades de seguridad en el AARNR.

Tabla 8.27 Resumen Comparativo entre distintos equipos inalámbricos que posee el AARNR.

Características	D-Link DWL-2100	Linksys WRT54G
Precio Local (US$)	60	110
Estándares	IEEE 802.11b, IEEE 802.11g, 802.11 Super G	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Numero de Puertos Fast Ethernet	1	4+1
Máxima potencia de trasmisión (dBm)	14	18
Ganancia de antena (dBi)	2	2
Máximo EIRP (dBm)		20
Seguridad Inalámbrica	WEP de 128 bits,	WPA-Personal

	encriptación de 64 bits WEP, WEP de 152 bits, TKIP, WPA, WPA-PSK	WPA-Enterprise WPA2-Personal WPA2-Enterprise Cifrado WEP de 64/128 bits Lista de control de acceso por direcciones MAC
Capacidad de RADIUS	Si	Autenticación
Modos de operación	Punto Acceso Bridge PtP , Bridge PtMP y Cliente	AP Router Firewall (DMZ)
Soporta VLAN	No	No
Máximo Numero de usuarios simultáneos	- -	12-14
Administración	Interfaz Web HTTP	Interfaz Web HTTP Secure HTTP (HTTPS) UPnP

Para seguridad inalámbrica, de acuerdo a la información presentada, los equipos recomendados por cada uno de los fabricantes cumplen con los requerimientos, por este motivo para la selección de la o las mejores alternativas se tomará en cuenta las características técnicas y el grado de confiabilidad que presentan los equipos. Se prevé que los puntos críticos en la seguridad inalámbrica son la autenticación y la contabilidad (Accouting) de servidor (RADIUS), debido a que si se presenta fallas en cualquiera de las dos secciones, el sistema de autenticación dejaría de funcionar. El ARNRR posee 4 D-Link DWL-2100 lo que no permite que el sistema de autenticación marche correctamente.

Se sugieren 6 equipos Linksys para cubrir en su totalidad esta Área su ventaja esta enmarcado en su poder de manejo en un número mayor de beneficiarios simultáneos, además ayuda a controlar las autenticaciones de los usuarios. Se puede obtener ganancias en el cambio de sus antenas por ejemplo hasta 24 DBI, además permite actualizar su firmware tanto del fabricante como de terceros ya que incluye el sistema GNU/Linux. Se puede actualizar con los fireware de Linksys para Linux o DD-WRT.

- **Inversión de la solución**

Los precios de referencia son tomadas de la marca conocida el Linksys. Para obtener un rango de cobertura en su totalidad en esta Área se detalla en el siguiente cuadro.

Tabla 8.28 Precio de equipos inalámbricos.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
Linksys WRT	6	110.00	660.00
		$ TOTAL	**1100.00**

8.4.6.1.2. Análisis costo-beneficio del Área de Energía, las Industrias y Recursos Naturales No Renovables

En primera instancia el desarrollo e implementación del esquema de seguridad en redes wi-fi se la realizara en esta Área, para ello daremos a conocer 3 equipos existentes que posee este espacio, al final proporcionaremos una conclusión del mejor equipo para seguridad.

En la fase de Análisis de la situación actual de la UNL el AEIRNNR posee los siguientes equipos: 4 D-Link DWL-2100, 2 D-link DWL-3200Ap, lo que en la siguiente tabla se detallan sus características.

Tabla 8.29 Resumen Comparativo entre distintos equipos inalámbricos que pose el AEIRNNR.

Características	D-Link DWL-2100	Linksys WRT54G	D-Link DWL-3200AP
Precio Local (US$)	60	110	240
Estándares	IEEE 802.11b, IEEE 802.11g, 802.11 Super G	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b	IEEE 802.3, IEEE 802.3u, IEEE 802.3af, IEEE 802.11g, IEEE 802.11b
Numero de Puertos Fast Ethernet	1	4+1	1
Máxima potencia de trasmisión (dBm)	14	18	21
Ganancia de antena (dBi)	2	2	5
Máximo EIRP (dBm)		20	26
Seguridad Inalámbrica	WEP de 128 bits, encriptación de 64 bits WEP, WEP de 152 bits, TKIP, WPA, WPA-PSK	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise Cifrado WEP de 64/128 bits Lista de control de acceso por direcciones MAC	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise 64/128/152-bit WEP Deshabilitación de broadcast de SSID Detección de Rogue AP Lista de control de acceso por direcciones MAC

			Configuración de seguridad aislada para cada SSID
Capacidad de RADIUS	Si	Autenticación	Autenticación y Accounting
Modos de operación	Punto Acceso Bridge PtP , Bridge PtMP y Cliente	AP Router Firewall (DMZ)	AP WDS con AP WDS/Bridge
Soporta VLAN	No	No	Si
Máximo Numero de usuarios simultáneos	- -	12-14	16-18
Administración	Interfaz Web HTTP	Interfaz Web HTTP Secure HTTP (HTTPS) UPnP	Interfaz Web HTTP Secure HTTP (HTTPS) AP Manager II Soporta SNMPv3 D-View Module Private MIB Interfaz por línea de comandos Telnet Secure (SSH) Telnet

- **Inversión de la solución**

Los precios de referencia son tomadas de la marca conocida el D-Link. Para obtener un rango de cobertura en su totalidad en esta Área se sugiere que se cuente con unos 4 D-Link DWL-3200, sus ventajas de alcance se describen anteriormente, adicionalmente 8 linksys para ayudar a su cobertura.

Tabla 8.30 Precio de equipos inalámbricos.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
D-Link DWL-3200.	4	240.00	960.00
Linksys WRT54G	8	110.00	880.00
		$ TOTAL	**1840.00**

8.4.6.1.3. Análisis costo-beneficio del Área de la Educación el Arte y la Comunicación.

Esta área cuenta con equipos inalámbricos de la marca D-Link, en el siguiente cuadro se presenta las características del equipamiento y la alternativa para obtener un sistema de autenticación.

Tabla 8.31 Resumen Comparativo entre distintos equipos inalámbricos que pose el AEAC.

Características	D-Link DWL-2100	Linksys WRT54G
Precio Local (US$)	60	110
Estándares	IEEE 802.11b, IEEE 802.11g, 802.11 Super G	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Numero de Puertos Fast Ethernet	1	4+1
Máxima potencia de trasmisión (dBm)	14	18
Ganancia de antena (dBi)	2	2
Máximo EIRP (dBm)		20
Seguridad Inalámbrica	WEP de 128 bits, encriptación de 64 bits WEP, WEP de 152 bits, TKIP, WPA, WPA-PSK	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise

		Cifrado WEP de 64/128 bits Lista de control de acceso por direcciones MAC
Capacidad de RADIUS	Si	Autenticación
Modos de operación	Punto Acceso Bridge PtP , Bridge PtMP y Cliente	AP Router Firewall (DMZ)
Soporta VLAN	No	No
Máximo Número de usuarios simultáneos	- -	12-14
Administración	Interfaz Web HTTP	Interfaz Web HTTP Secure HTTP (HTTPS) UPnP

Se sugiere que se haga uso del Linksys WRT ya que es el mejor medio para poder autenticar, sus ventajas ya se dieron a conocer anteriormente permitiendo de esta forma obtener una autenticación segura a los usuarios. Otra alternativa en cuanto a costo es la utilización del mismo con respecto a equipos más costosos, cabe señalar algo importante que de este equipo que contiene un sistema GNU/Linux permitiéndole que sea robusto y con muchas funcionalidades, su principal limitación es algo que no podrá modificarse su potencia máxima de trasmisión.

- **Inversión de la solución**

Los precios de referencia son tomadas de la marca conocida el Linksys. Para obtener un rango de cobertura en su totalidad en esta Área se sugiere que se posea 8 Linksys.

Tabla 8.32 Precio de equipos inalámbricos.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
Linksys WRT	8	110.00	880.00
		$ TOTAL	**13200.00**

8.4.6.2.Análisis costo-beneficio del Área de Jurídica Social y Administrativa

Como el Área anterior esta cuenta con similares equipos de la marca D-Link, además dentro de su equipamiento posee dos Lynksys WRT lo que facilitaría el esquema de seguridad, lo que en este caso haría falta de un servidor RADIUS para las autenticaciones.

Las ventajas que posee los Linksys se menciono anteriormente es por ello que el equipo es idóneo para autenticación de usuarios.

- **Inversión de la solución**

Los precios de referencia son tomadas de la marca conocida el Linksys. Se sugiere que se opte por 9 Lynksys por ser una de las Áreas de mayor espacio, los mismos que cubrirán el espacio de esta Área, de esta manera obtener un sistema de autenticación eficaz.

Tabla 8.33 Precio de equipos inalámbricos.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
Linksys WRT	9	110.00	990.00
		$ TOTAL	**1320.00**

8.4.6.3.Análisis costo-beneficio del Área de Salud Humana

Esta Área cuenta con equipos Lynksys WRT, los cuales se deberían utilizar para autenticar, como se menciono anteriormente se debería implementar un servidor Radius para hacer uso al máximo del este equipo.

Las características ya se conoce del mismo, lo que podemos concluir que, si bien el equipo WRT54G por si solo es un equipo que ofrece ciertas características que mejoran a los D-Link DWL 2100, con el cambio de su firmware se vuelve una poderosa herramienta capaz de ser comparado con equipos de mucho mayor costo al contar con mucho mas funcionalidades.

- **Inversión de la solución**

Dentro de la inversión de equipos se recomienda que opte por 5 Lynksys, esta Área tendrá la cobertura en su totalidad.

Tabla 8.34 Precio de equipos inalámbricos.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
Linksys WRT	5	110.00	550.00
		$ TOTAL	**880.00**

8.4.6.4. Análisis Costo-Beneficio de la Solución Inalámbrica

Para el análisis costo beneficio de la solución inalámbrica podemos encontrar varios equipos Wi-Fi en el mercado; para los cuales hemos tenido la oportunidad de analizar hasta 03 diferentes equipos: Cisco Aironet AIR-11300AG, Linksys WRT54G, D-Link DWL-3200AP.

A continuación, pasaremos a detallar el análisis costo-beneficio que se realizó con estos tres equipos, mostrando primero una tabla de comparaciones de acuerdo a sus especificaciones técnicas y luego pasando a presentar una explicación en la que se indicará para cuales escenarios cada uno de los equipos se ubicaría mejor.

Tabla 8.35Resumen Comparativo entre distintos equipos inalámbricos.

Características	Cisco Aironet 11300AG	Linksys WRT54G	D-Link DWL-3200AP
Precio Local (US$)	375	110	240

Estándares	IEEE 802,11b/g, 802,1x, 802,11i.	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b	IEEE 802.3, IEEE 802.3u, IEEE 802.3af, IEEE 802.11g, IEEE 802.11b
Numero de Puertos Fast Ethernet	4	4+1	1
Máxima potencia de trasmisión (dBm)	16	18	21
Ganancia de antena (dBi)	13	2	5
Seguridad Inalámbrica	Autenticación: IEEE 802.1x (incluye LEAP, EAP, PEAP, EAP MD5, EAPTLS). Encripción: - WPA (Cisco TKIP o WPA TKIP, MIC y broadcast key rotation). WPA2: AES (802.11i).	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise Cifrado WEP de 64/128 bits Lista de control de acceso por direcciones MAC	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise 64/128/152-bit WEP Deshabilitación de broadcast de SSID Detección de Rogue AP Lista de control de acceso por direcciones MAC Configuración de seguridad aislada para cada SSID
Capacidad de RADIUS	Autenticación	Autenticación	Autenticación y Accounting
Modos de operación	AP	AP Router Firewall (DMZ)	AP WDS con AP WDS/Bridge
Soporta VLAN	No	No	Si
Administración	Interfaz Web	Interfaz Web HTTP Secure HTTP	Interfaz Web HTTP Secure HTTP

		(HTTPS) UpnP	(HTTPS) AP Manager II Soporta SNMPv3 D-View Module Private MIB Interfaz por línea de comandos Telnet Secure (SSH) Telnet

- **Cisco Aironet AIR-11300AG[50]**

El Cisco Aironet 1130AG puede ser configurado para soportar Enterprise Wireless Mesh proporcionando conectividad inalámbrica para las áreas interiores que son difíciles o imposibles de alambre. Los Puntos de acceso de malla no requieren de conexiones cableadas, sino que utiliza el 2.4-GHz de frecuencia para ofrecer acceso a la red a los usuarios duro-a-llegar a las zonas y la banda de 5 GHz para el tráfico de retorno a puntos de acceso tradicionales conectados a los puertos Ethernet.

Está diseñado para la cobertura de oficinas y entornos de RF similares, este punto de acceso discreta características integradas antenas y doble IEEE 802.11a / g de radio para una cobertura completa y fiable, proporcionando una capacidad combinada de 108 Mbps.

Figura 8.62 ZYXEL PRESTIGE 660HW-T1.

- **LINKSYS WRT54G**

El Linksys WRT54G es un wireless router con capacidad de firewall (soporte de SPI o Stateful Packet Inspection). Cuenta con una mayor potencia de transmisión que el

[50] http://www.digitalairwireless.com/cisco_wireless_networks.asp

equipo anterior, logrando poder atravesar más obstáculos y brindar así un área de cobertura mayor. Si bien este equipo cuesta poco más del doble que el equipo anterior, su capacidad de poder manejar un mayor número de usuarios simultáneos y brindar una mayor cobertura lo hacen una buena opción para redes medianas. Sin embargo, su incapacidad de reportar la contabilidad de los accesos hacia un servidor RADIUS hace que se tome como una gran desventaja que juega en su contra.

Lamentablemente, el firmware con el que viene de fábrica no le permite realizar dicha tarea. Adicionalmente, el acceso vía Web con HTTPS es una característica adicional que aporta una capa de seguridad en la administración del sistema

Figura 8.63 LINKSYS WRT54G[51]

- **DD-WRT V24**

Se mencionó anteriormente que una de las limitaciones del equipo resultaba ser el firmware que trae de fábrica. El equipo ofrece la capacidad de poder actualizar su firmware por otros que saque la compañía que lo realizó. Sin embargo, el trabajo arduo de una comunidad denominada DD-WRT permitió obtener un firmware válido para poder cambiar por el de fábrica. Dicho firmware se encuentra basado en Linux y con ello le permite al equipo poder habilitar muchos de los servicios de red que se pueden obtener con Linux; logrando así contar con un equipo mucho más robusto y con muchas más funcionalidades que el original.

De esta manera, podemos concluir que, si bien el equipo WRT54G por sí solo es un equipo que ofrece ciertas características que mejoran por muy poco al equipo visto

[51] http://es.wikipedia.org/wiki/WRT54G

anteriormente, con el cambio de firmware se vuelve una poderosa herramienta capaz de ser comparado con equipos de mucho mayor costo al contar con mucho más funcionalidades. Sin embargo, algo que no podrá modificarse será la potencia máxima de transmisión que ofrece el equipo, limitación del hardware de éste.

- **D-LINK DWL-3200AP**[52]

El D-Link DWL-3200AP es el equipo con mayor potencia de transmisión que se ha podido examinar para los propósitos de esta tesis. Con sus 21 dBm de potencia de transmisión y sus 5 dBi de ganancia en sus antenas duales reemplazables (utilizan conectores BNC) le permiten aparecer como el equipo de más alto rango de los tres que se han analizado. Logra una amplia cobertura en interiores, llegando incluso a brindar cobertura hasta en dos pisos y soportando una gran cantidad de usuarios simultáneos.

Además, las funcionalidades con las que cuenta como el soporte de VLAN, detección de rogue APs y soporte de gestión vía SNMPv3 representan una gran ventaja frente a las demás opciones. Así mismo, cuenta con soporte para autenticación y contabilidad con RADIUS. Este equipo resulta de gran ventaja para redes grandes y con una gran cantidad de usuarios.

Figura 8.64 D-LINK DWL-3200AP

Adicionalmente a los equipos inalámbricos se debe adquirir servidores para los servicios de autenticación (RADIUS). Para implementar este servicio se ha seleccionado el servidor HP ML110 G5.

Tabla 8.36 Característica del Servidor

Procesador	RAM	Ranuras de Expansión	Controlador de Red
Xeon 2.13 GHz,	1GB	(2) PCI-Express (1x4	Broadcom 5721

[52] http://www.dlinkla.com/home/productos/producto.jsp?idp=793

1066 Hz, Cache L2 de 2Mb		y 1x8)/ (2) PCI 3.3 V de 32 bits/33MHZ	Gigabit NIC 10/100/1000
Intel (R) Pentium (r) 4 cpu 3.0 GHz	1 GB	2 PCI express	Gigabit NIC 10/100/1000

Dentro de los objetivos de la presente tesis se planteo que el AEIRNNR sería el marco inicial para el esquema de seguridad, es por ello que los equipos existentes dentro del mismo permiten desenvolvernos con facilidad.

El equipo LINKSYS WRT54G no cumple con los requerimientos técnicos en cuanto al grado de confiabilidad de las secciones críticas anteriormente mencionadas; por lo cual, se basará en este criterio para establece que la alternativa LINKSYS WRT54G no es recomendable de implementar. La solución D-LINK DWL 3200 está acorde con las exigencias técnicas y presenta un alto grado de confiabilidad, es un excelente equipo como se logra observar en el cuadro cuenta con múltiples funciones con respecto a los anteriores. Sus antenas duales reemplazables utilizan BNC lo que se puede conectar a otra tipo de antena para alcanzar ganancias de 26 Bdi., en conclusión es una alternativa óptima.

Además se hizo el estudio que el equipo más óptimo para poder realizar la implementación de la seguridad inalámbrica utilizando Radius es el AP cisco aironet 11300ag, para lo cual se presenta también la configuración de dichos equipos para la solución de seguridad wifi.

8.4.6.5.Configuración de los Acces Point d-link 3200ap con protocolo 802.1x

El D-Link DWL-3200AP es un poderoso, robusto y fiable Access Point para operar en entornos empresariales con diversos negocios. Este Access Point provee opciones avanzadas de seguridad para los administradores de red, permitiéndoles desplegar una administración muy robusta en redes wireless. El Access Point DWL-3200AP soporta Power Over Ethernet (PoE) y provee dos antenas de alta ganancia para una óptima cobertura wireless.

Sin lugar a dudas es un dispositivo indispensable en cualquier grupo de trabajo que desee entrar en la nueva era Wireless por la puerta principal.

8.4.6.5.1. Especificaciones:

- **General**

Marca: D-Link

Modelo: DWL-3200

Tipo de Dispositivo: Punto de acceso inalámbrico.

- **Conexión de Red**

Factor de forma: Externo

Tecnología de conectividad: Inalámbrico

Velocidad de transferencia de datos: 54 Mbps

Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11g

Banda de frecuencia: 2.4 GHz

Algoritmo de cifrado: AES, WPA

Cumplimiento de normas: IEEE 802.11b, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x

- **Antena**

Cantidad de antenas: 2

- **Expansión/Conectividad**

Interfaces: 1xred -Radio-Ethernet

1 x red / energía - Ethernet 10Base-T/100Base-TX - RJ-45

8.4.6.5.2. Menú de Configuración

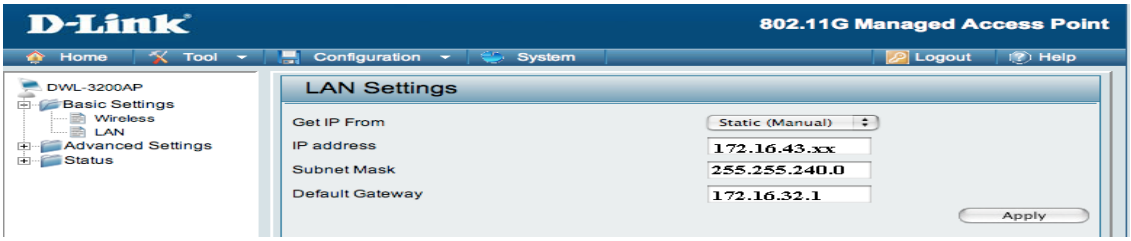


Figura 8.65 Configuración de Lan en D-LINK

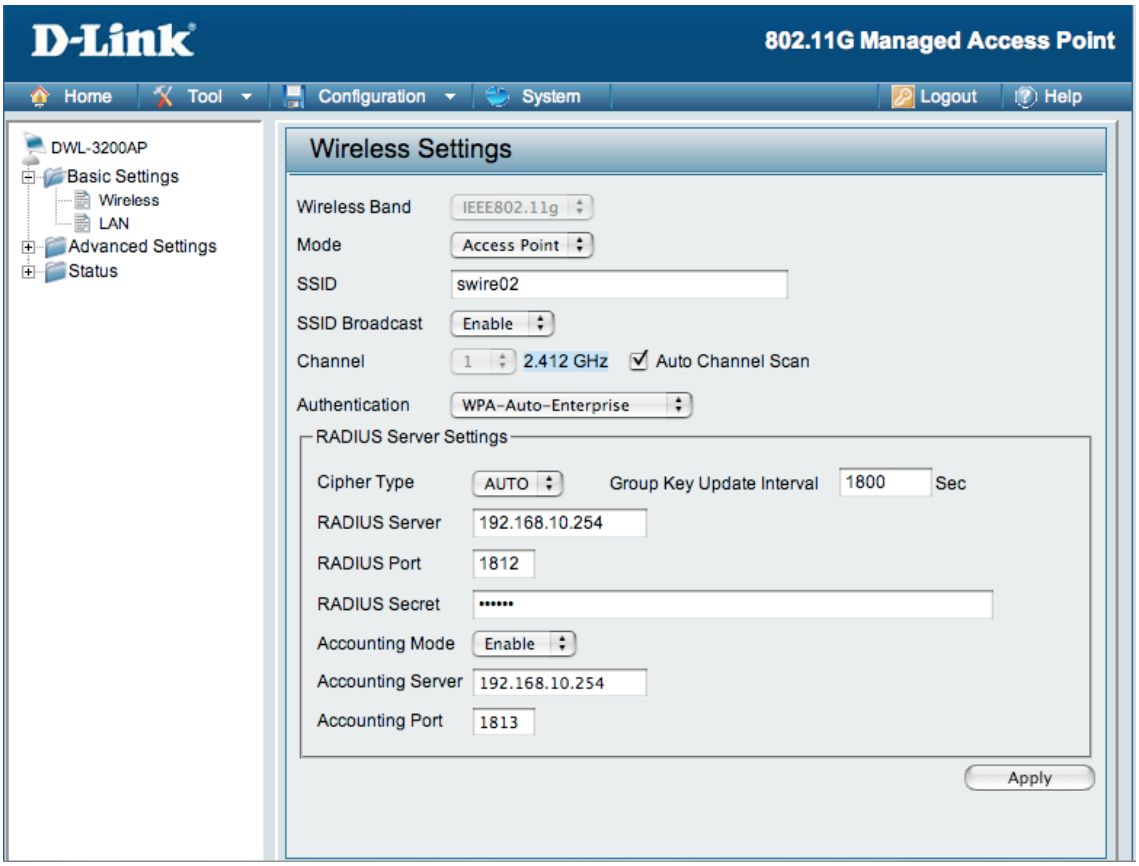


Figura 8.66 Configuración de Wireless en D-LINK

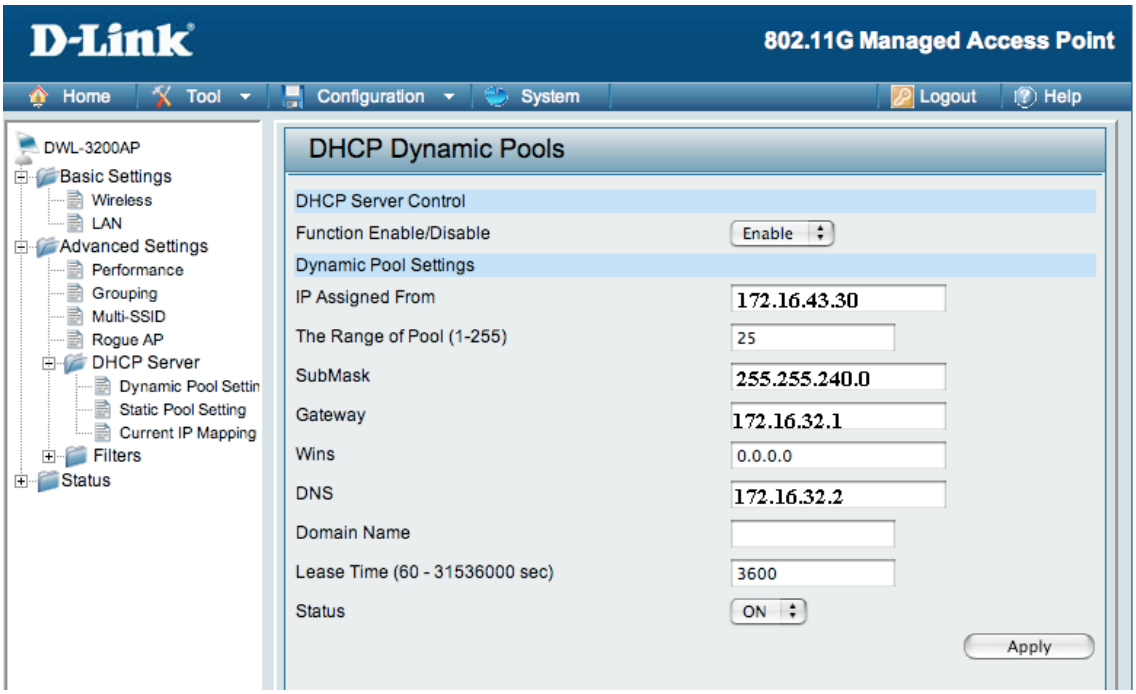


Figura 8.67 Configuración de DHCP Dymanic Pools en D-LINK

8.4.6.5.3. Utilización del AP MANAGER

El AP Manager es una herramienta conveniente para administrar la configuración de su red desde un ordenador central. Con AP Manager no hay necesidad de configurar dispositivos de forma individual.

Para iniciar el Administrador de AP Manager:

• Vaya al menú Inicio
• Seleccione Programas
• Seleccione D-Link AirPremier AP Manager
• Seleccione DWL-3200AP

8.4.6.5.3.1.Encontrar Dispositivos

Haga clic en este botón para encontrar los dispositivos disponibles en la red.

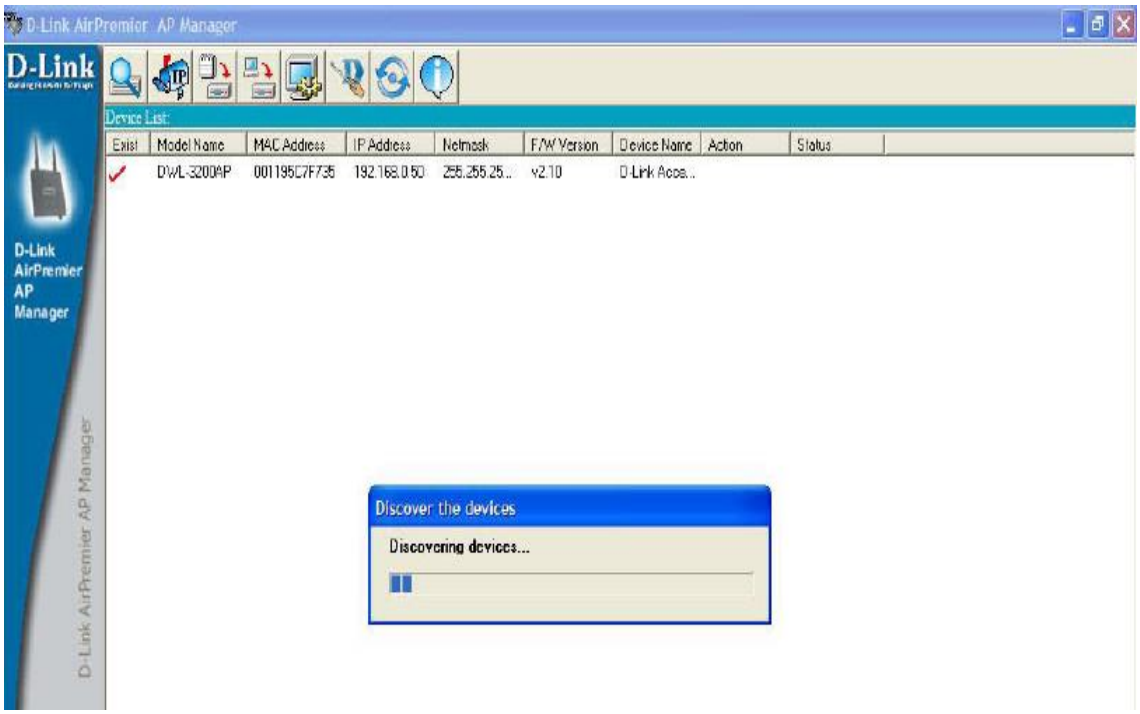


Figura 8.68 Pantalla para encontrar dispositivos

8.4.6.5.3.2. Selección de dispositivos

El AP Manager le permite configurar múltiples dispositivos a la vez. Para seleccionar un único dispositivo, simplemente haga clic en el dispositivo que desea seleccionar. Para seleccionar varios dispositivos, mantenga pulsada la tecla Ctrl mientras hace clic en cada dispositivo adicional. Para seleccionar una lista completa, mantenga pulsada la tecla Mayús, haga clic en el punto de primera en la lista y, a continuación, haga clic en el punto de último en la lista.

8.4.6.5.3.3. Configuración IP

Puede asignar una dirección IP a un AP o asignar direcciones IP a múltiples AP haciendo clic en este botón después de seleccionar el dispositivo (s).

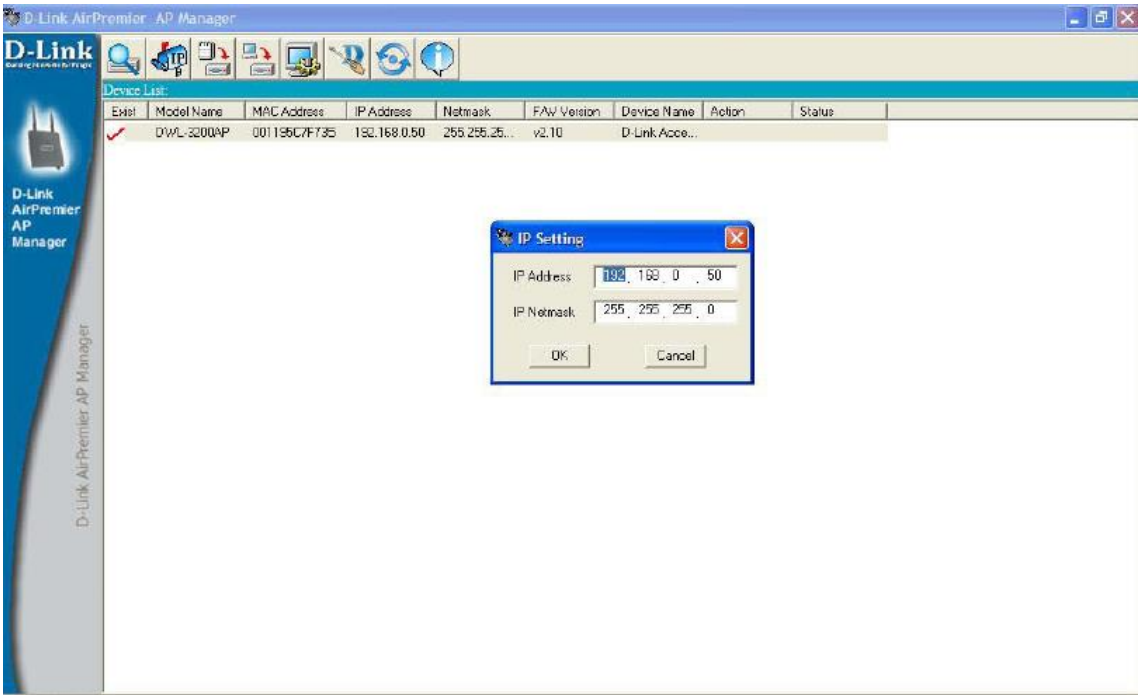


Figura 8.69 Pantalla para configurar la dirección IP

Seleccione el AP que desea asignar una dirección IP y haga clic en el botón de IP. Escriba la dirección IP y máscara de red IP para el dispositivo seleccionado y haga clic en Aceptar.

Puede configurar varios AP con las direcciones IP de todos a la vez. Haga clic en el botón de IP después de que haya seleccionado todos los AP que desea asignar una dirección IP. Introduzca la dirección IP que desea asignar a la primera unidad y el AP Manager asignará automáticamente direcciones IP secuenciales.

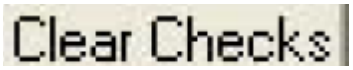
8.4.6.5.3.4.Configuración de dispositivos

Haga clic en este botón para encontrar los dispositivos disponibles en la red.

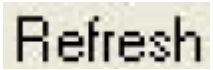
Haga clic en este botón para acceder a las propiedades de configuración del dispositivo seleccionado (s).

La ventana de configuración del dispositivo le permite configurar los ajustes, pero en realidad no se aplican los ajustes para el dispositivo a menos que haga clic en el botón Aplicar. También puede guardar y cargar archivos de configuración de esta ventana. Cuando se carga un archivo de configuración, debe hacer clic en Aplicar si desea que la configuración se aplique al dispositivo seleccionado (s).

El botón Check All seleccionará todas las opciones configurables. Cualquier ajuste que tiene una marca de verificación junto a ella se aplica al dispositivo o guardar en el archivo de configuración.



El botón Clear Checks anula todas las opciones configurables. Esta característica es útil si sólo desea cambiar algunas opciones de configuración. Deseleccionar todos los artículos y sólo comprobar los elementos que desea modificar



Refresh volverá a la configuración del dispositivo real del dispositivo seleccionado (s).

Para guardar la configuración en el dispositivo, debe hacer clic en el botón **Apply**. Sólo los ajustes que tienen una marca de verificación junto a ellos se aplicarán.

El botón Open se utiliza para cargar un archivo de configuración guardado previamente. Después de abrir un archivo de configuración, debe hacer clic en el botón Apply para guardar los ajustes para el dispositivo seleccionado (s).

El botón Save le permite guardar un archivo de configuración de los ajustes del dispositivo seleccionado. Sólo los ajustes que tienen una marca de verificación se salvan. No se puede guardar un archivo de configuración si se ha seleccionado más de un dispositivo en la lista de dispositivos.

El botón **Exit** cerrará la ventana de configuración del dispositivo. Cualquier configuración que no se han aplicado se perderá.

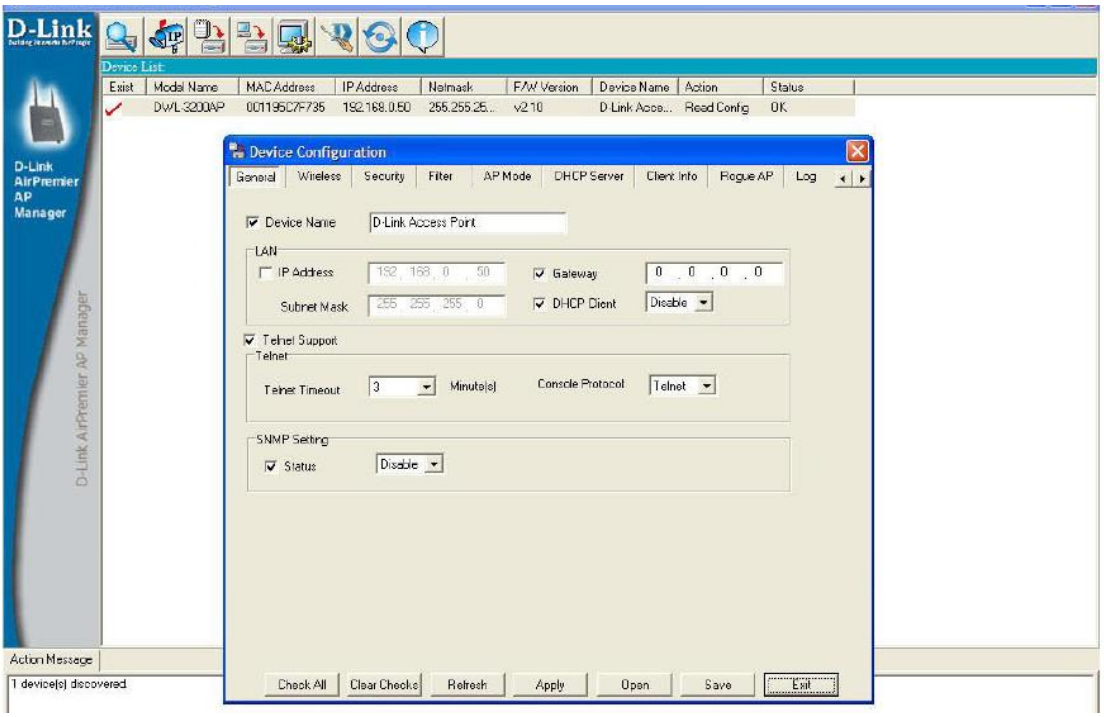


Figura 8.70 Pantalla de configuración de dispositivos

8.4.6.5.3.5. Firmware

Para actualizar el firmware, haga clic en este botón después de seleccionar el dispositivo (s).

Para actualizar el firmware:

- Descargar la última actualización de firmware de http://support.dlink.com a un lugar fácil de encontrar en su disco duro.
- Haga clic en el botón de firmware como se muestra arriba.
- Una ventana emergente aparecerá. Busque el archivo de actualización del irmware y clickOpen.

¡IMPORTANTE!: NO DESCONECTE la corriente de la unidad mientras firmware se está actualizando.

8.4.6.5.3.6. System Settings

Usted puede personalizar la configuración básica del sistema para el DWL-3200AP haciendo clic en este botón.

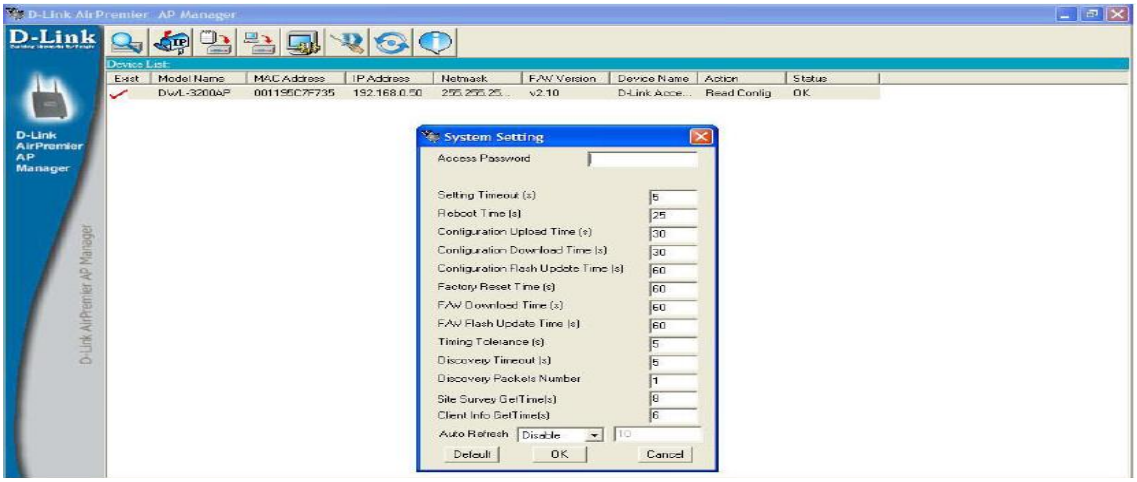


Figura 8.71 Pantalla System Settings

Clave de acceso: Establece la contraseña de administrador para el dispositivo seleccionado(s).

Auto Actualizar: Esta opción le permite activar Auto actualizar la lista de dispositivos de red. Por defecto esta opción está desactivada. Si usted habilita esta opción, debe introducir el intervalo de actualización en segundos.

8.4.6.5.3.7. Setup Wizard

Este botón iniciará el Asistente para la instalación que le guiará a través de la configuración de dispositivos.

8.4.6.5.3.8.Refresh

Haga clic en este botón para actualizar la lista de dispositivos disponibles en la red.

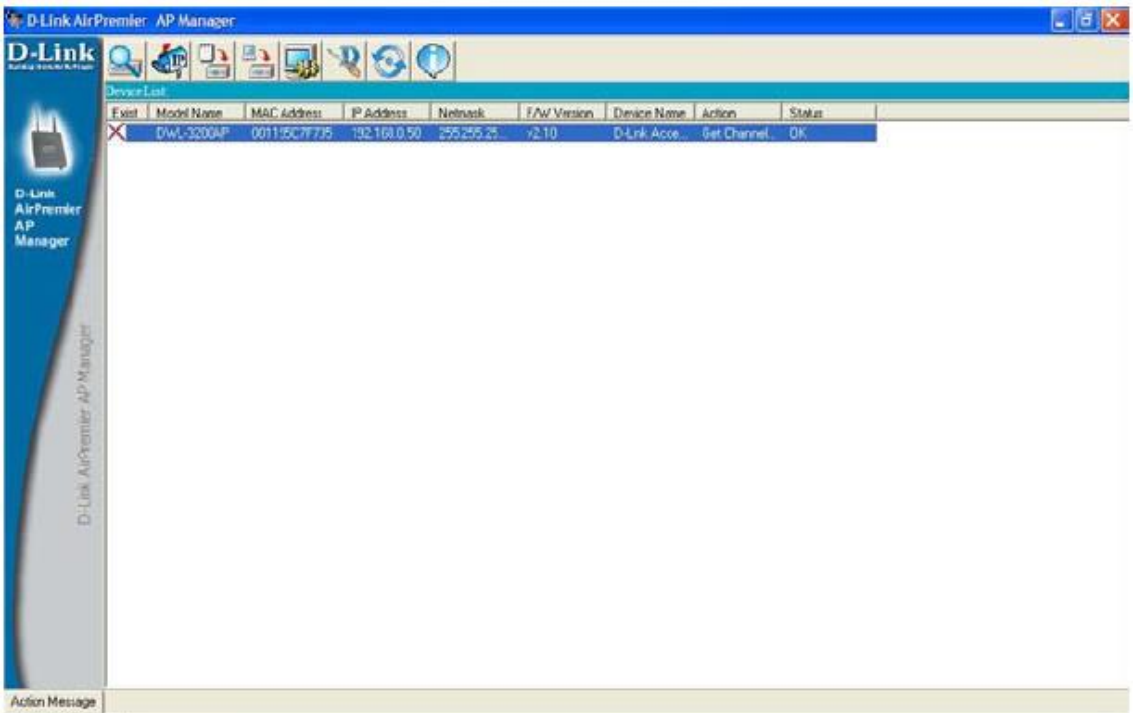


Figura 8.72 Pantalla de refresh

Los dispositivos con una marca de verificación al lado de ellos todavía están disponibles en la red. Los dispositivos con una "X" ya no están disponibles en la red.

8.4.6.5.3.9. About

Haga clic en este botón para ver la versión de AP Manager.

Figura 8.73 Pantalla de ayuda

8.4.6.6. Configuración de los Acces Point cisco aironet 11300 ag con protocolo 802.1x

Adicionalmente se sugiere que los equipos óptimos para una seguridad integra serian los Cisco Aironet de las siguientes características:

8.4.6.6.1. Características

- **General**

MPN: AIR-LAP1131AG-E-K9

Tipo de dispositivo: Punto de acceso inalámbrico

Anchura: 19.1 cm

Profundidad: 3.3 cm

Altura: 19.1 cm

Peso: 0.7 kg

- **Procesador / memoria / almacenamiento**

RAM instalada (máx.): 32 MB

Memoria flash instalada (máx.): 16 MB Flash

- **Conexión de redes**

Factor de forma: Externo

Tecnología de conectividad: Inalámbrico

Velocidad de transferencia de datos: 54 Mbps

Formato código de línea: CCK, OFDM

Protocolo de interconexión de datos: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g

Método de espectro expandido: OFDM, DSSS

Protocolo de gestión remota: SNMP, Telnet, HTTPS

Alcance máximo en interior: 137 m

Alcance máximo al aire libre: 290 m

Indicadores de estado: Activo, error, estado

Características: Auto-sensor por dispositivo, soporte BOOTP

Algoritmo de cifrado: LEAP, AES, WEP de 128 bits, WEP de 40 bits, TLS, PEAP, TKIP, WPA, WPA2

Método de autentificación: Secure Shell (SSH), MS-CHAP

Cumplimiento de normas: IEEE 802.3, IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, Wi-Fi CERTIFIED

8.4.6.6.2. Configuración de AP aironet con protocolo 802.1x

!

version 12.3

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RADIUS
!
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 172.16.43.118 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
 server 172.16.43.118 auth-port 1812 acct-port 1813
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
```

```
!
aaa group server radius dummy
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
dot11 ssid AEIRNNRSegWifi
   vlan 71
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   accounting acct_methods
   guest-mode
!
dot11 ssid AEIRNNRSegWifi2
   vlan 6
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   accounting acct_methods
!
dot11 ssid AEIRNNRSegWifi3
```

```
  vlan 30
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa
!
dot11 ssid AEIRNNRSegWifi4
  vlan 3
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa
!
dot11 ssid batman
  vlan 1
  authentication open
!
dot11 network-map
!
!
username admin password 7 1304131F0202
username batman098 privilege 15 password 7
094E470B150C18060E0F052B2F29213D
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
```

```
no ip route-cache
!
encryption vlan 71 mode ciphers tkip
!
encryption vlan 6 mode ciphers tkip
!
encryption vlan 30 mode ciphers tkip
!
encryption vlan 3 mode ciphers tkip
!
ssid AEIRNNRSegWifi
!
ssid AEIRNNRSegWifi2
!
ssid AEIRNNRSegWifi3
!
ssid AEIRNNRSegWifi4
!
ssid batman
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
```

```
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
!
interface Dot11Radio0.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 bridge-group 6 subscriber-loop-control
 bridge-group 6 block-unknown-source
 no bridge-group 6 source-learning
 no bridge-group 6 unicast-flooding
 bridge-group 6 spanning-disabled
```

```
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface Dot11Radio0.71
 encapsulation dot1Q 71
 no ip route-cache
 bridge-group 71
 bridge-group 71 subscriber-loop-control
 bridge-group 71 block-unknown-source
 no bridge-group 71 source-learning
 no bridge-group 71 unicast-flooding
 bridge-group 71 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 encryption vlan 71 mode ciphers tkip
```

```
 encryption vlan 6 mode ciphers tkip
 encryption vlan 30 mode ciphers tkip
 encryption vlan 3 mode ciphers tkip
 ssid batman
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
```

```
!
interface Dot11Radio1.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 bridge-group 6 subscriber-loop-control
 bridge-group 6 block-unknown-source
 no bridge-group 6 source-learning
 no bridge-group 6 unicast-flooding
 bridge-group 6 spanning-disabled
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface Dot11Radio1.71
 encapsulation dot1Q 71
 no ip route-cache
 bridge-group 71
 bridge-group 71 subscriber-loop-control
```

```
 bridge-group 71 block-unknown-source
 no bridge-group 71 source-learning
 no bridge-group 71 unicast-flooding
 bridge-group 71 spanning-disabled
!
interface FastEthernet0
 bandwidth 1
 ip address 192.168.1.1 255.255.255.0
 no ip route-cache
 duplex auto
 speed auto
 hold-queue 160 in
!
interface FastEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
 bridge-group 3 spanning-disabled
```

```
!
interface FastEthernet0.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 no bridge-group 6 source-learning
 bridge-group 6 spanning-disabled
!
interface FastEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
!
interface FastEthernet0.71
 encapsulation dot1Q 71
 no ip route-cache
 bridge-group 71
 no bridge-group 71 source-learning
 bridge-group 71 spanning-disabled
!
interface BVI1
 ip address 172.16.1.121 255.255.255.0
 no ip route-cache
!
```

```
ip default-gateway 172.16.1.10
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
snmp-server view dot11view ieee802dot11 included
snmp-server view ieee802dot11 ieee802dot11 included
snmp-server community utpl RO
snmp-server location upsi
snmp-server contact jv
radius-server attribute 32 include-in-access-req format %h
radius-server host 172.16.31.161 auth-port 1812 acct-port 1813 key 7
09584B1A0D0C19155A5E57
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
line con 0
line vty 0 4
!
End
```

8.4.6.7. Ubicación de los Acces Point's en cada área

8.4.6.7.1. Alcance

Como dato muy importante son las distancias de los dispositivos Wireless 802.11g, que son de 100 metros para "espacios cerrados" y hasta 400 metros en "espacios abiertos".

El alcance depende principalmente de la potencia de emisión de los equipos, dato que nos suele suministrar el fabricante en mWatios o en dB, y de los "objetos a atravesar", no es lo mismo una oficina con paredes finas, a un edificio antiguo con paredes gruesas de piedra.

8.4.6.7.2. Cálculo de potencias

dBm es la potencia de radio expresada en dB referida a 1mW. La potencia máxima permitida de emisión para la banda ISM (2,4GHz) es de 100mW (20dB).

Esta potencia de emisión es el resultado de sumar la potencia de salida de la tarjeta WIFI, con la ganancia de la antena y teniendo en cuenta las perdidas del cable y conectores.

Para convertir mW a dBm, tenemos que multiplicar por 10 el logaritmo de la potencia expresada en mW. Por ejemplo, si la potencia máxima son 100mW:

$$10 \times \log 100mW = 20\ dBm$$

La potencia máxima legal de emisión es de 100mW o 20 dBm.

La mayoría de los dispositivos Wireless emiten en un rango de 20 a 50mW:

$$10 \times \log 50mW = 17\ dBm$$

Adicionalmente esta tabla será útil para el cálculo de pérdida adicional cuando se deban atravesar obstáculos:

Tabla 8.37 Cálculo de pérdida adicional cuando se deban atravesar obstáculos

Obstáculo	**Perdida en dB**	**Perdida de Señal**
Espacio Abierto	0	0%
Ventanas	De 3 a 8	De 30% a 50%
Paredes Finas	De 5 a 8	50%
Paredes Gruesas	De 15 a 20	80%
Suelos y Techos	De 15 a 20	80%
Maderas	10	70%

8.4.6.7.3. Antena omnidireccional[53]

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal

[53] http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/438/1/LUCERNA.pdf

extensa en los alrededores. Las antenas sectoriales se suelen utilizan cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa.

Si necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque o institución pública por ejemplo) lo más probable es que utilice una antena omnidireccional. Si tiene que dar cobertura de red inalámbrica en un punto muy concreto (por ejemplo un PC que está bastante lejos) utilizará una antena direccional, finalmente, si necesita dar cobertura amplia y a la vez a larga distancia, utilizará antenas sectoriales.

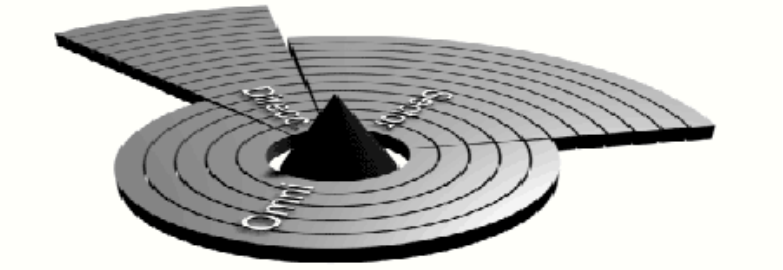


Figura 8.74 Antena Omnidireccional

Tipo	OmniDireccional	
Apta para interiores	Si	
Apta para exteriores	Si	
Herrajes incluidos	Si	
Ganancia		12 dBi
Cobertura vertical		8 grados
Cobertura horizontal		360 grados
Alcance		1500 metros *
Dimensiones : Alto		120 cm
Dimensiones : Ancho		1 cm
Dimensiones : Profundo		1 cm

Conectores y cables incluidos: A — N-H

La antena tiene un cable de 0.15 metros terminado en un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail

Figura 8.75 Características de una antena omnidireccional

La antena omnidireccional es una de las mejores opciones la cual brinda una radiación de señal de ganancia de 12dBi, que es dar coberturas a toda la comunidad estudiantil del AEIRNNR y una de las características más importantes de esta antena es que es de largo alcance y su radiación es de 360 grados optamos por colocar un a antena omnidireccional lo cual podemos bañar toda el área.

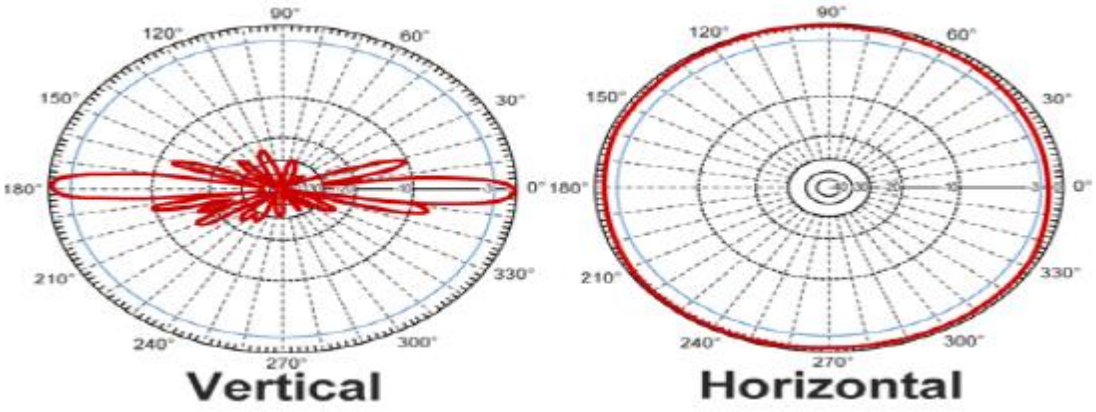


Figura 8.76 Radiación de una antena omnidireccional[54]

8.4.6.7.4. Ubicación de los Access Point

Para la ubicación adecuada de los Puntos de Acceso, se colocaron en lugares donde se tiene una mayor densidad de usuarios es decir los lugares donde se encuentran la mayoría de alumnos que requieren de una conexión a la red, estos lugares son los siguientes.

[54] http://aire.ec/~aire235/uploads/Datasheet_2_4GHz_Omnidirectional_Antennas_VPOL_Spanish.pdf

8.4.6.7.4.1. Ubicación de los Acces Point's el Área Agropecuaria y de Recursos Naturales Renovables

Figura 8.77 Ubicación de los Acces Point's el Area Agropecuaria y de Recursos Naturales Renovables

8.4.6.7.4.2. Ubicación de los Acces Point's el Área Energía, Industrias y Recursos Naturales no Renovables.

Figura 8.78 Ubicación de los Acces Point's el Área Energía, Industrias y Recursos Naturales no Renovables.

8.4.6.7.4.3. Ubicación de los Acces Point's el Área de la Educación, el Arte y la Comunicación

Figura 8.79 Ubicación de los Acces Point's el Área de la Educación, el Arte y la Comunicación

8.4.6.7.4.4. Ubicación de los Acces Point's el Área Jurídica, Social y Administrativa

Figura 8.80 Ubicación de los Acces Point's el Área Jurídica, Social y Administrativa

8.4.6.7.4.5.Ubicación de los Acces Point's el Área de la Salud Humana

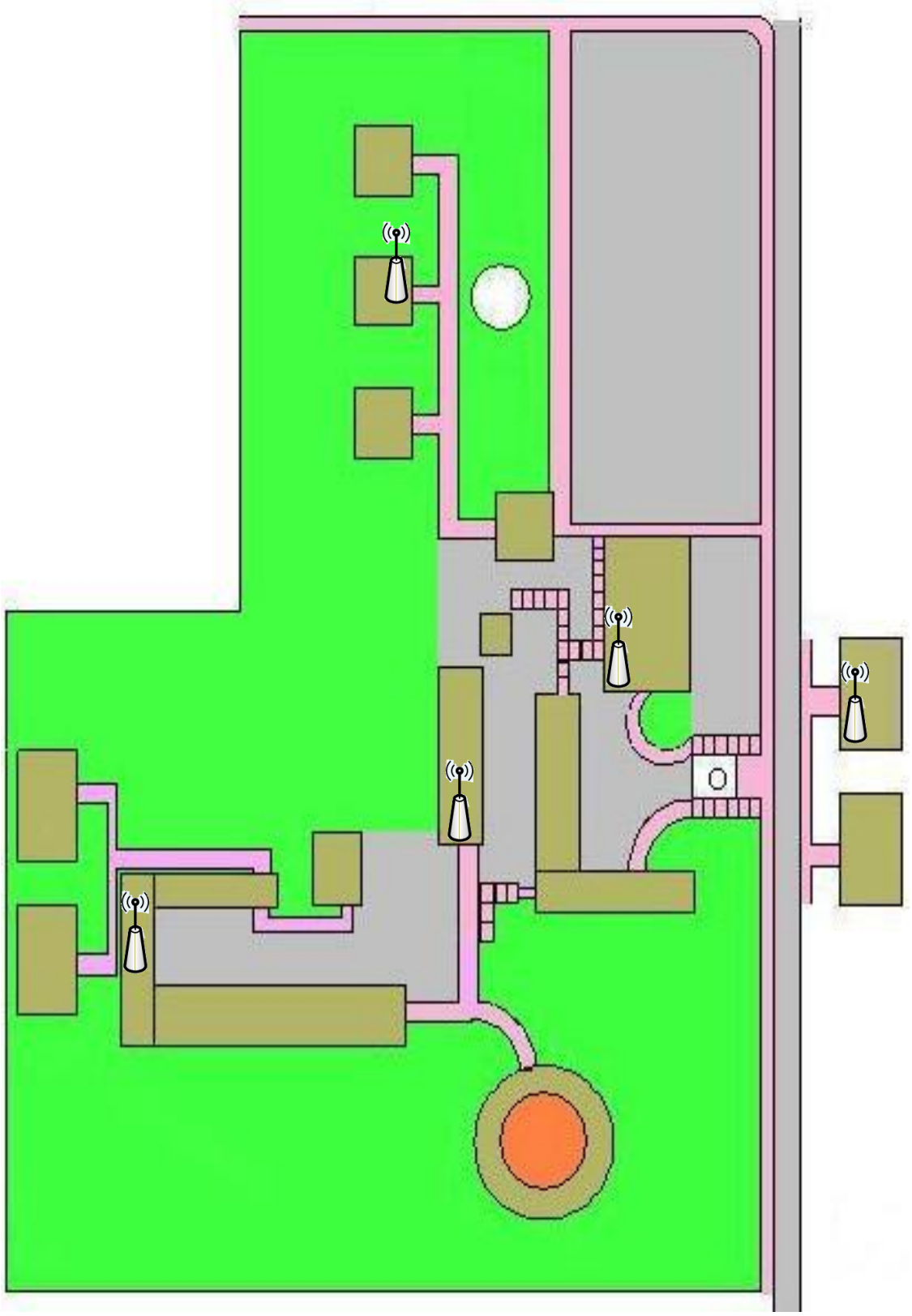


Figura 8.81 Ubicación de los Acces Point's el Área de la Salud Humana

8.4.7. Implementación de la solución cableada

8.4.7.1. Análisis del sistema de cableado estructurado

Para el sistema de cableado estructurado, se emplean los siguientes tipos de medios de transmisión:

- Fibra óptica multimodo (62,5/125 μm).
- Cable UTP de 100 _, categoría 5e.
- Medios inalámbricos.
- Cable UTP, categoría 3 (red de voz).

El cable UTP categoría 5e es el más empleado en todos el campus para el cableado horizontal, debido a su recomendación en las normas de cableado estructurado para redes de datos, ya que este tipo de cable es altamente difundido y comercializado. La fibra óptica, los medios inalámbricos son empleados, para la interconexión entre las distintas Áreas del campus, lo cual es conocido como cableado vertical.

Se tienen medios inalámbricos, especialmente debido a la presencia de línea de vista entre los Áreas a conectarse y a la facilidad que proveen este tipo de enlaces.

El Área de la Salud es el único campus alejado de la Universidad, por lo cual se les conecta atreves de medios inalámbricos (Kanoppic), haciendo al enlace más seguro.

8.4.7.1.1. Cableado Vertical

Para el cableado vertical se emplean medios de transmisión que cumplen con las especificaciones detalladas en la norma ANSI/TIA/EIA 568 B.2 de cableado estructurado.

Tabla 8.38 Enlaces implementados en la red de datos de la UNL

CABLEADO VERTICAL (CONEXIÓN ENTRE LAS ÁREAS)	MEDIOS DE TRANSMISIÓN	NUMERO DE PARES
Administración Central	Fibra óptica, Inalámbrico	2 (hilos)
Área Jurídica Social y Administrativas	Fibra óptica, Inalámbrico	2 (hilos)
Área Educativa Arte y Comunicación.	Fibra óptica, Inalámbrico	2 (hilos)
Área de la Salud Humana	Inalámbrico	---
Área Agropecuaria y Recursos Naturales Renovables	Fibra óptica, Inalámbrico	2 (hilos)
Área Energía, Industrias y Recursos Naturales No Renovables.	Fibra óptica, Inalámbrico	2 (hilos)

Para el caso de la fibra óptica se emplean conectores multimodo, para su conexión con el panel del rack del cuarto de comunicaciones (Jefatura de Informática), y transceptores ópticos (conversión de fibra óptica a UTP, o viceversa) para su posterior vínculo con el switch de la LAN interna del campus.

8.4.7.1.2. Cableado Horizontal

Los cinco Áreas de la UNL (AJSA, AEAC, ASH, AARNR, AEIRNNR,), presentan las mismas características en cuanto al cableado horizontal. Para la red de datos, se emplea cable UTP de 4 pares, categoría 5e, con conectores RJ 45 (RJ viene de *Registered Jack*). Según la norma ANSI/TIA/EIA 568 B, la distribución de pines del conector RJ 45 se presenta en la Figura 8.82

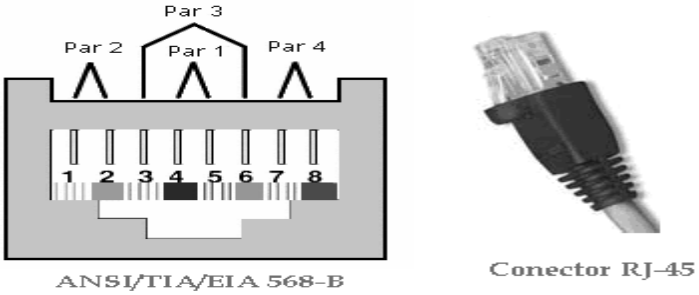


Figura 8.82 Distribución de pines del conector RJ45

8.4.7.2. ANÁLSIS COSTO-BENEFICIO DE LA SOLUCIÓN ALAMBRICA

Una vez desarrollado el diseño de la seguridad en la intranet de la UNL, se procederá a realizar un análisis sobre los elementos de la red activa procediendo a un estudio costo beneficio de la solución alambicas sobre los elementos de la red, en la que se analizará varias alternativas en base a aspectos técnicos y costos que representa cada elemento o equipo.

La selección de los equipos activos de datos será analizada de manera independiente, en función a los fabricantes de los mismos.

Para la red de datos se considerarán equipos perteneciente a dos fabricantes de networking: DLink y Cisco. DLink debido a la fuerte inclinación de la UNL por dichos equipos, y Cisco por su alta difusión en ambientes de networking, así como por la confiabilidad que ofrece.

- **DLINK**

Los switches DLINK manejan tarjetas de expansión que permite la escalabilidad de la red para cubrir potenciales crecimientos, por lo que se tiene que adicionar módulos con puertos adaptables en los diferentes modelos de switches que ofrece. Adicionalmente se utiliza transceivers (convertidores) GBIC con conectores LC y RJ45 para realizar las conexiónes Gigabit Ethernet con fibra óptica y cabe UTP.

En la siguiente Tabla se muestran los equipos DLINK que cumplen con los requerimientos establecidos, su modelo y características más importantes. La información presentada a continuación se obtuvo de la documentación técnica de los equipos provista por sus respectivos fabricantes.

Tabla 8.39 Características de los equipos DLINK

EQUIPO	CARACTERISTICA
Firewall *DFL-2500*	*Características:* protección firewall, filtrado de contenido, detección de intrusos, autenticación de usuarios, mensajes instantáneos, bloqueo P2P, protección de ataques de negación de servicio, soporte de VPNs, administración de ancho de banda. *Administración y configuración:* Basada en Web, interfaz de línea de comandos, reportes y monitoreo en tiempo real, SNMP v.1, SNMP v.2c. *Throughput:* 320Mbps. *8 puertos configurables.* *Balanceo de carga.* *Filtrado de contenido:* URL/Email, Java Script/Active X/Cookies, Programa IM/P2P.
Switch de acceso *DES-3550*	*Puertos:* 48 puertos 10/100Mbps RJ 45. 2 puertos Combo 10/100/1000Mbps cobre/SFP (fibra óptica). *Velocidad de conmutación:* 13,6 Gbps. *Fuente de Poder Redundante.* *Estándares:* 802.1p QoS, 802.1x (autenticación basada en puerto y MAC), 802.1q VLANs, listas de acceso L2/L3/L4, 802.1d/w Spanning tree. *Administración:* SNMP v.1, SNMP v.2c, SNMP v.3, RMON, BOOTP, TELNET *Puerto Uplink:* 802.3ad y soporte LACP. *Autenticación RADIUS.* *Switch capa 3.*
Transceiver mini-Gbic *DEM-311GT*	*Puerto 1000BASE-SX (estándar IEEE 802.3z) o 1000BASETX.* *Conector duplex LC o RJ 45.* *Operación Full duplex.* *Soporte de control de flujo 802.3x.* *Medio: fibra óptica* multimodo 50um o 62,5um sobre los 550 m,

	UTP cat 5e. L*ongitud de onda:* 850nm.
Switch de Distribución y Servidores *DGS-3312SR*	*Puertos:* 4 puertos Gigabit SFP. 2 slots abiertos para cobre/fibra (máximo 12 puertos). *Velocidad de conmutación:* 24 Gbps. *Fuente de Poder Redundante.* *Estándares:* IEEE 802.3u 100BASE-TX Fast Ethernet. IEEE 802.3ab 1000BASE-T Gigabit Ethernet. IEEE 802.1 p/q VLAN. IEEE 802.3x Full-duplex control de flujo. IEEE 802.3 Nway auto-negociación. IEEE 802.3z puertos SFP. IEEE 1394.b Stacking. IEEE 802.1d/w/s Spanning tree. IEEE 802.1p QoS. IEEE 802.1x control de acceso. Llistas de acceso L2/L3/L4. *Administración:* SNMP v.1, SNMP v.2c, SNMP v.3, RMON, BOOTP, TELNET, Web *Puerto Uplink:* 802.3ad y soporte LACP. *Autenticación RADIUS.* *Switch capa 4.*
Switch de Core *DXS-3326GSR*	*Puertos:* 24 puertos Gigabit SFP slots de fibra. 4 puertos Combo Gigabit de cobre. *Velocidad de conmutación:* 160 Gbps. *Fuente de Poder Redundante.* *Estádares:* IEEE 802.3u 100BASE-TX Fast Ethernet. IEEE 802.3ab 1000BASE-T Gigabit Ethernet. IEEE 802.1d/w/s Spanning Tree. IEEE 802.1 p/q VLAN. IEEE 802.1p colas de prioridad. IEEE 802.1x control de acceso basado en puerto y MAC. IEEE 802.3ad control uplink.

	IEEE 802.3x Full-duplex control de flujo. IEEE 802.3 Nway auto-negociación. Listas de acceso L2/L3/L4. *Puerto Uplink:* 802.3ad y soporte LACP. *Administración:* SNMP v.1, SNMP v.2c, SNMP v.3, RMON, BOOTP, TELNET, Web. *Autenticación RADIUS.* *Switch capa4.*

- **CISCO**

De manera similar a los equipos DLink, Cisco maneja tarjetas de expansión con módulos de puertos adaptables (GBIC) y transceivers (convertidores) GBIC. En la siguiente Tabla se presenta las características técnicas de los equipos activos Cisco para la red.

Tabla 8.40 Características de los equipos CISCO

EQUIPO	CARACTERÍSTICAS
Switch de Acceso *Catalyst 3560*	*Puertos:* 48 puertos Ethernet 10/100 Mbps (RJ 45). 4 puertos Gigabit Ethernet (SFP). *Estándares:* 802.1p QoS. 802.1x (autenticación basada en puerto y MAC). 802.1q VLANs. 802.1d Spanning tree. 802.3af. *Administración:* SNMP v.1, SNMP v.2c, SNMP v.3, RMON I y II. *Autenticación:* TACACS o RADIUS. *Capas OSI:* 2, 3 y 4.

Switch de Distribución, Core y Servidores *Catalyst 4500*	*Puertos: Distribución:* 6 Gigabit Ethernet (GBIC). *Core:* 6 Gigabit Ethernet (GBIC). *Servidores:* 18 Gigabit Ethernet (GBIC). *Velocidad de conmutación: 136* Gbps. *Estándares: Gigabit Ethernet:* IEEE 802.3z, IEEE 802.3x, IEEE 802.3ab. *1000BASE-X (GBIC):* 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX. *VLAN trunking:* IEEE 802.1q. *Spanning-Tree Protocol:* IEEE 802.1d. *Software:* Cisco IOS (Supervisor engine IV) 12.1 (12c) EW o superior. *Seguridad:* a*utenticación:* 802.1x. *Administración:* SNMP v.1 y v.2, VTP, CDP, MIB I y II, RMON I y II. *Autenticación:* passwords y TACACS. *Alimentación:* AC, fuente redundante (opcional). *Capas OSI:* 2, 3 y 4.

- **HIBRIDA**

Gracias a la compatibilidad de operabilidad que presentan los equipos Cisco y DLink, se ha optado por una tercera solución denominada "*híbrida"*. La solución "*híbrida"* combinará equipos Cisco y DLINK en la red.

Para la selección de los equipos de uno u otro fabricante se analizará el cumplimiento o no de las características descritas en los requerimientos de la red diseñada, como se presenta en la Tabla

Tabla 8.41 Cuadro comparativo entre equipos Dlink y Cisco

CARACTERISTICAS	**¿CUMPLE? SI/NO**	
	DLINK	**CISCO**
Switch de acceso		
48 puertos RJ 45 10/100 Mbps.	SI	SI
Puerto uplink Gigabit Ethernet para UTP cat 5e	SI	SI
Permitir manejo de VLANs (IEEE 802.1q).	SI	SI
Auto-negociación de la velocidad de puerto	SI	SI
Conmutación a nivel de capa 2.	SI	SI
Ser administrable.	SI	SI
Protocolos: IP, OSPF, RIP v2, BGP, DHCP, TELNET, SNMP v1, SNMP v2, SNMP v3 y RMON.	SI	SI
Manejo de listas de acceso de nivel 2	SI	SI
Spanning Tree Protocol (802.1 d).	SI	SI
Protocolo 802.1x (autenticación de dispositivos conectados a puertos LAN).	SI	SI
Switch de distribución		
5 puertos Gigabit Ethernet para UTP cat 5e	SI	SI
Puerto uplink Gigabit Ethernet para fibra óptica multimodo	SI	SI
Manejo y administración de VLANs (IEEE 802.1Q).	SI	SI
Auto-negociación de la velocidad de puerto	SI	SI
Conmutación a nivel de capa 2, 3 y 4.	SI	SI
Tipo administrable.	SI	SI
Protocolos: IP, OSPF, RIP v1, RIP v2, BGP, DHCP, TELNET, SNMP v1, SNMP v2, SNMP v3, RMON.	SI	SI
Manejo de listas de acceso de nivel 2, 3, 4	SI	SI
Configuración vía HTTP.	SI	SI
Protocolo 802.1x (autenticación de dispositivos conectados a puertos LAN).	SI	SI
Switch de core		
6 puertos Gigabit Ethernet para fibra óptica multimodo.	SI	SI

Puerto uplink Gigabit Ethernet para fibra óptica multimodo.	SI	SI
Manejo y administración de VLANs (IEEE 802.1q).	SI	SI
Auto-negociación de la velocidad de puerto.	SI	SI
Conmutación a nivel de capa 2, 3 y 4.	SI	SI
Tipo administrable.	SI	SI
Protocolos: IP, OSPF, RIP v1, RIP v2, BGP, DHCP, Telnet, SNMP v1, SNMP v2, SNMP v3, RMON.	SI	SI
Manejo de listas de acceso de nivel 2, 3 y 4. SI SI QoS de nivel 2, 3, v4 (802.1p, DiffServ, asignación de ancho de banda).	SI	SI
Enrutamiento: estático, dinámico RIP I y II, IPRouting.	NO	SI
Protocolo 802.1x (autenticación de dispositivos conectados a puertos LAN).	SI	SI
Spanning-Tree Protocol (802.1d).	SI	SI
Manejo de QoS para reconocer, priorizar y clasificar tráfico de VoIP.	NO	SI
Manejo de QoS para reconocer, priorizar y clasificar tráfico de Telefonía IP.	NO	SI
Switch de servidores		
5 puertos Gigabit Ethernet para fibra óptica multimodo	SI	SI
Puerto uplink Gigabit Ethernet para fibra óptica multimodo.	SI	SI
Manejo y administración de VLANs (IEEE 802.1Q).	SI	SI
Auto-negociación de la velocidad de puerto	SI	SI
Conmutación a nivel de capa 2, 3 y 4.	SI	SI
Tipo administrable.	SI	SI
Protocolos: IP, OSPF, RIP v1, RIP v2, BGP, DHCP, Telnet, SNMP v1, SNMP v2, SNMP v3, RMON.	SI	SI
Manejo de listas de acceso de nivel 2, 3 y 4	SI	SI
QoS de nivel 2, 3, v4 (802.1p, DiffServ, asignación de ancho de banda).	SI	SI
Enrutamiento: estático, dinámico RIP I y II, IpRouting.	NO	SI
Protocolo 802.1x (autenticación de dispositivos	SI	SI

conectados a puertos LAN).		
Spanning-Tree Protocol (802.1d).	SI	SI
Manejo de QoS para reconocer, priorizar y clasificar tráfico de VoIP.	NO	SI
Manejo de QoS para reconocer, priorizar y clasificar tráfico de Telefonía IP.	NO	SI

La selección de los equipos, que cumplen en su totalidad los requerimientos, se muestra en la siguiente Tabla, estos equipos serán seleccionados para su utilización en el esquema de seguridad.

Tabla 8.42 Selección de equipos

EQUIPOS DE RED DE DATOS	**MARCA**	**MODELO**
Switch de Acceso	DLINK	DES 3550
Switch de core	CISCO	Ws-x4515
Switch de servidores	CISCO	WS-X4516
Firewall	CISCO	Pix

Para el caso de la red de datos, de acuerdo a la información presentada en los puntos anteriores, la mayoría de los equipos recomendados por cada uno de los fabricantes cumplen con los requerimientos, por este motivo para la selección de la o las mejores alternativas se tomará en cuenta las características técnicas y el grado de confiabilidad que presentan los equipos. Se prevé que los puntos críticos de la red son la capa de core y la sección de la granja de servidores, debido a que si se presenta fallas en cualquiera de las dos secciones, la red dejaría de operar

La solución DLINK no cumple con los requerimientos técnicos en cuanto al grado de confiabilidad de las secciones críticas; por lo cual, se basará en este criterio para establece que la *alternativa DLink* no es recomendable de implementar. La solución Cisco está acorde con las exigencias técnicas y presenta un alto grado de confiabilidad, en conclusión es una alternativa óptima.

- La solución "híbrida" cuenta con los equipos de mejores características de las dos alternativas antes mencionadas. Así se tiene que, para las secciones críticas los dispositivos serán del fabricante Cisco (asegurando la confiabilidad); mientras que para el resto de niveles, se elegirá aquellos dispositivos que cumplan con los requerimientos establecidos y que involucren un menor costo (basándose en los bajos precios que involucra un equipo DLink frente a uno Cisco). **Por lo que la *solución "híbrida"* es recomendada.**

- Otra alternativa de seguridad en redes cableadas es el uso de un firewall en hardware, debido a que son dispositivos actualmente comercializados para realizar esta función específica.

La tarea de un firewall, es cumplir con las siguientes funciones:

a. Restringir el acceso desde el exterior hasta el interior.
b. Permitir un acceso limitado desde el exterior hasta la DMZ.
c. Permitir todo el acceso desde el interior hasta el exterior.
d. Permitir un acceso limitado desde el interior hasta la DMZ.

La zona desmilitarizada (DMZ), es una red aislada a la que pueden acceder los usuarios del exterior. La creación de una DMZ posibilita que un administrador ponga la información y los servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado. El firewall debe configurarse para que permita el acceso desde el exterior o el interior hasta la DMZ.

Los hosts o servidores que residen en la DMZ (hosts bastión), deben actualizarse con respecto a un sistema operativo y a sus modificaciones experimentales, lo que lo volverá menos vulnerable a los ataques. Un host bastión sólo ejecuta los servicios necesarios para realizar sus tareas de aplicación, en tanto que los servicios innecesarios son desactivados o eliminados, "cabe mencionar que la creación de la dmz depende del

precio de cómo se genere en su implementación en la UNL y la utilización de un firewall hardware (CISCO PIX) depende del ancho de banda que a la que se llegue"[55].

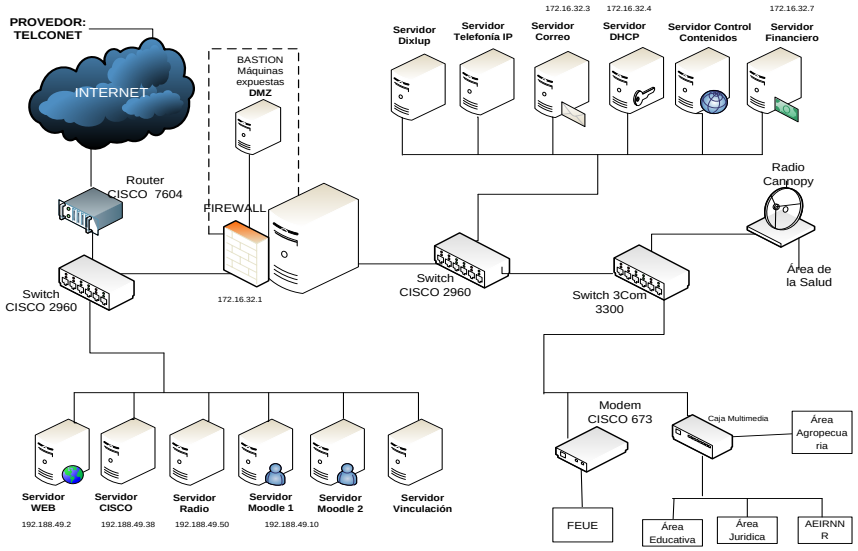


Figura 8.83 Esquema de la zona desmilitarizada

8.4.7.2.1. Configuración de switch cisco Catalyst 3560

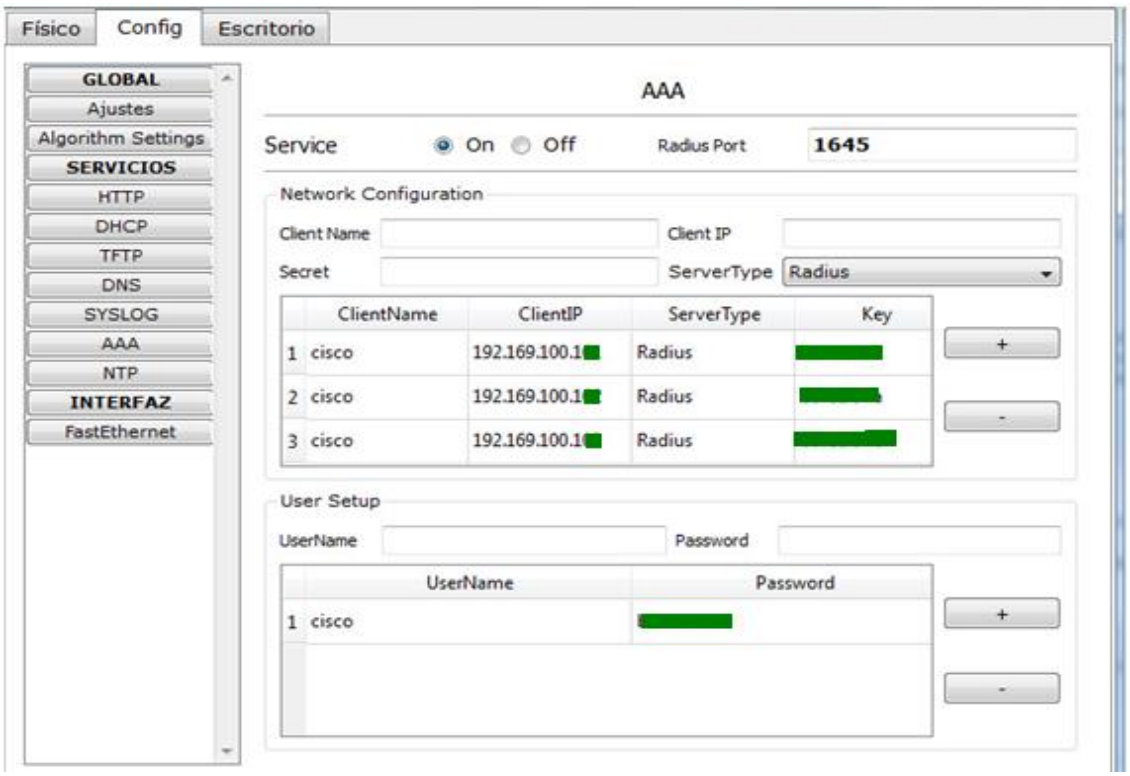


Figura 8.84 Configuración del switc cisco Catalyst 3560

[55] **Fuente:** Jefatura de Informática UNL

8.5.MANUAL DE POLITICAS DE SEGURIDAD DE REDES

8.5.1. Introducción

Este manual presenta un conjunto de mecanismos y políticas de seguridad para el uso adecuado de la red que la Universidad Nacional de Loja, particularmente en el Área de Energía, las Industrias y Recursos Naturales no Renovables, pone a disposición de sus trabajadores, profesores y estudiantes como herramientas que faciliten el desarrollo de sus funciones.

Luego de publicado a los miembros del Área, que hacen uso de estos recursos y servicios, este manual instituirá un basamento formal para dar cumplimiento a las normativas, lineamientos y políticas constituidas en él, en relación al uso y seguridad de la red.

Una vez obtenida la información contenida en este manual, cada miembro de la Comunidad Universitaria, será responsable del mismo y de su adecuada utilización.

Este manual es propiedad del Área de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja y puede ser ubicado en el web site de Internet: http://www.unl.edu.ec para su difusión a las diferentes áreas de la institución que así lo requieran.

La aplicación de las Políticas contenidas en este manual, son de obligatorio cumplimiento para todos los miembros del Área de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad y no podrán ser modificadas sin la

autorización del Unidad de Desarrollo Informático UDI[56] a quién deberá ser presentada cualquier propuesta de modificación.

La Unidad de Desarrollo Informático UDI deberá establecer los mecanismos que considere necesarios para verificar el cumplimiento de las políticas establecidas en este manual.

El presente manual representa una herramienta de trabajo que se considera perfectible y susceptible a correcciones, por lo que se agradece a todos los miembros de la Institución, cualquier recomendación que contribuya a su enriquecimiento, la cual debe ser dirigida al UDI.

8.5.2. Objetivo y Alcance

Objetivo

Establecer las Políticas Generales a contemplar en el uso del Internet, para asegurar la integridad y disponibilidad de la infraestructura tecnológica y la confidencialidad e integridad de la información que se manipula a través de ella.

Alcance

Las Políticas Generales establecidas en este manual regirán para todos los miembros del Área de la Energía, las Industrias y los Recursos Naturales no Renovables y deberán ser acatadas por todas aquellas personas que en el ejercicio de sus labores interactúen con los servicios y recursos del Internet tanto en forma directa (administrativos, docentes y estudiantes).

[56] Unidad de Desarrollo Informático

8.5.3. Riesgos de las Redes Inalámbricas

Aunque este trabajo vaya dirigido a los aspectos de seguridad de la red inalámbrica, no podemos pasar por alto los elementos que componen la red inalámbrica.

Existen 4 tipos de redes inalámbricas, la basada en tecnología BlueTooth, la IrDa (Infrared Data Association), la HomeRF y la WECA (Wi-Fi). La primera de ellas no permite la transmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizado por los dispositivos de ondas infrarrojas, debe permitir la visión directa entre los dos elementos comunicantes. Las tecnología HomeRF y Wi-Fi están basados en las especificaciones 802.11 (Ethernet Inalámbrica) y son las que utilizan actualmente las tarjetas de red inalámbricas.

La topología de estas redes consta de dos elementos clave, las estaciones cliente (STA) y los puntos de acceso (AP). La comunicación puede realizarse directamente entre estaciones cliente o a través del AP. El intercambio de datos sólo es posible cuando existe una autentificación entre el STA y el AP y se produce la asociación entre ellos (un STA pertenece a un AP). Por defecto, el AP transmite señales de gestión periódicas, el STA las recibe e inicia la autentificación mediante el envío de una trama de autentificación. Una vez realizada esta, la estación cliente envía una trama asociada y el AP responde con otra.

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. Varios son los riesgos derivables de este factor. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y una más que posible denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2’4GHz (frecuencia utilizada por las redes inalámbricas).

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si esta estación cliente ofrece servicios TCP/IP[57] o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC[58] de estaciones cliente legítimas.

Los puntos de acceso están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción en una red inalámbrica por parte de intrusos. A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros, como el protocolo WEP[59] fácilmente 'rompibles' por programas distribuidos gratuitamente por Internet.

8.5.4. Uso del manual

Para la correcta implementación de este Manual, se debe tomar en cuenta lo siguiente:

- El Manual deberá estar a disposición de todo el personal que forme parte del Área de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja.
- La Unidad de Desarrollo Informático UDI, debe difundir las políticas y lineamientos descritos en este Manual y velar por su cumplimiento.
- Cualquier cambio en las políticas de la Institución que afecte la estructura del Manual, generará también un cambio en su contenido con el fin de adaptarlo a

[57] TCP/IP, Protocolo de control de transmisión/Protocolo de Internet
[58] MAC (Media Access Control), Control de Acceso al medio
[59] WEP (Wired Equivalent Privacity), Privacidad Equivalente al Cableado

las nuevas políticas emitidas.

- Los Usuarios del Manual deberán notificar a la UDI las sugerencias, modificaciones o cambios que afecte el contenido del mismo, con el objeto de garantizar la vigencia de su contenido y con ello mejorar la base de conocimiento en el tiempo.

8.5.5. Mecanismos de seguridad

Para establecer mecanismos de seguridad basados en procesos de autenticación y cifrado, se definen diversos estándares de acuerdo las necesidades y al grado de confidencialidad de la información que manejan los clientes, se tiene estándares básicos que vienen incorporados en los equipos de la red y otros que proporcionan mayor seguridad que pueden ser instalados en los mismos o inclusive algunos que necesitan de dispositivos adicionales, teniendo un costo mucho mayor.

En el presente estudio se analizarán los estándares de contraseñas seguras, WPA[60], establecer permisos y VPN[61], que servirán como mecanismos de protección para la red y se describen a continuación.

8.5.5.1. Contraseñas seguras

Informar a los administrativos, docentes y alumnos de la importancia de las contraseñas es el primer paso para convertir las contraseñas en una valiosa herramienta de seguridad de la red, ya que dificultan la suplantación de su usuario. Es decir, no se debe dejar en cualquier parte ni se debe compartir.

[60] WPA (Wi-fi Protected Access)
[61] VPN (Virtual Private Network), tecnología de red que permite extender la red local sobre una red pública relativamente.

- **Características de una contraseña "segura":**

  - Una longitud de seis caracteres como mínimo; cuanto más larga, mejor.
  - Una combinación de letras mayúsculas y minúsculas, números y símbolos.
  - Se debe cambiar cada 90 días como mínimo y, al cambiarla, debe ser muy distinta de las contraseñas anteriores.
  - No utilice datos personales.

Es importante ser consciente de lo vital que resulta mantener una contraseña como una herramienta de seguridad. Por lo que se deben evitar las contraseñas inseguras, fáciles de descubrir y no deberán incluir:

- Un nombre real, nombre de usuario o nombre de la entidad.
- Una palabra común porque el riesgo ante "ataques de diccionario" aumenta.
- Contraseñas comunes, como "contraseña", "entrar" o "1,2,3,4".
- Sustituciones de letras conocidas, por símbolos similares.
- Una contraseña conocida por alguien.

8.5.5.2. Encriptación WPA

Surgió como alternativa segura y eficaz al WEP, se basa en el cifrado de la información mediante claves dinámicas, que se calculan a partir de una contraseña. WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance conjuntamente con la IEEE[62]. Este estándar busca corregir los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP[63] (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente

[62] IEEE (**Instituto de Ingenieros Electricistas y Electrónicos)**
[63] TKIP (**Temporal Key Integrity Protocol),** es un protocolo de seguridad utilizado en el estándar IEEE 802.11 para redes inalámbricas.

cada cierto tiempo, ampliando la longitud de la clave de 40 a 128 bits y pasa de ser única y estática a ser generada de forma dinámica para cada usuario, para cada sesión y por cada paquete enviado para evitar ataques que permitan revelar la clave. El vector de inicialización pasa de 24 a 48 bits, minimizando la reutilización de claves. TKIP utiliza además claves para tráfico de difusión y multidifusión.

De esta manera WPA mejora los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP. El mecanismo de autenticación usado en WPA emplea 802.1x y EAP. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

Modalidad de red doméstica, *o PSK*[64] *(Pre-Shared Key):* WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

8.5.5.3. Establecer permisos

Se pueden asignar distintos niveles de permisos a los usuarios según su función y responsabilidades en la organización. En vez de conceder a todos los usuarios el acceso "Administrador" (instituya una política de "práctica de menos privilegios”).

[64] PSK, La **modulación por desplazamiento de fase**

8.5.5.4. Implementación de un firewall

Un firewall o servidor de seguridad controla el acceso a la red. Puede impedir que los intrusos de Internet sondeen los datos de la red privada. Y puede controlar a los usuarios que tienen acceso fuera de la red.

Un firewall de hardware resulta más adecuado para una red ya que puede proteger todos los equipos de la misma. También ofrece un nivel adicional de defensa ya que puede "ocultar" de forma efectiva todos los equipos de red al exterior. Un firewall de software, sólo protege el equipo en el que se ejecuta, sin embargo proporciona una buena defensa de reserva a los servidores de seguridad de hardware.

8.5.5.5. Cerrar los puertos de red innecesarios

Los puertos de red permiten la comunicación entre los equipos cliente y los servidores. Para reforzar la seguridad de la red e impedir el acceso no autorizado, se debe cerrar los puertos de red que no se utilicen o sean innecesarios mediante servidores de seguridad dedicados, servidores de seguridad basados en host o filtros de seguridad de protocolo Internet.

8.5.6. Políticas de seguridad

8.5.6.1. Establecimiento de políticas de seguridad a ser implementadas

- Se definirá un grupo de políticas de seguridad para la implementación del cliente RADIUS, las mismas que brindarán protección a la información considerada confidencial, como son las claves de los usuarios que serán intercambiadas entre el usuario y el cliente RADIUS y posteriormente entre el cliente RADIUS y el servidor RADIUS.

- Se definirán políticas para la generación y utilización de las claves empleadas en los procesos de autenticación.
- Se definirán políticas de los requisitos mínimos que deben cumplir el sitio en el cual se instale el sistema de control de acceso.

8.5.6.2. Políticas de seguridad a ser implementadas

- El servicio de Internet provisto por la Universidad Nacional de Loja, a los miembros de su comunidad, a través de fibra óptica, deberá ser para el estricto uso en actividades propias o directamente relacionadas con las funciones de la Institución: Docencia, Investigación, Extensión y Gestión Universitaria. Se excluye todo uso de tipo personal o recreativo.
- Son usuarios de la red institucional los docentes de planta, administrativos, secretarias, alumnos, y toda aquella persona, que tenga contacto directo como empleado y utilice los servicios de la red institucional del Área de la Energía, Industrias y Recursos Naturales no Renovables de la Universidad Nacional de Loja.
- El uso del servicio de Internet a los miembros del AEIRNNR, para el desarrollo de las actividades inherentes a las funciones que desempeñan, estará sujeta a la aprobación de los encargados de la Unidad de Desarrollo Informático UDI o la(s) persona(s) que designen para tal fin.
- Se negará la utilización del servicio de Internet provisto por la Institución, a personal ajeno a la Comunidad Universitaria.
- Los usuarios del Internet, serán responsables del correcto uso de los mismos, el cual deberá ser racional, legal y ético, evitando su saturación o colapso por uso inadecuado o malicioso.
- Se debe respetar las restricciones de acceso a páginas Web que indiquen la Unidad de Desarrollo Informático UDI.
- En caso de requerir el acceso a alguna página bloqueada, deberá justificarlo y solicitar el desbloqueo a la Unidad de Desarrollo Informático UDI.
- Se asignará una cuenta de acceso a los sistemas de la intranet, a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o

permisos explícitos a los que este accederá, junto a la información personal del usuario

- Los alumnos, son usuarios limitados, estos tendrán acceso únicamente a los servicios de limitados de, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.
- El usuario es responsable exclusivo de mantener a salvo su contraseña.
- El sistema de autenticación solicitará que se ingresen un "nombre de usuario" y una "clave", a estos dos parámetros estará asociado un perfil que será asignado de acuerdo a los requerimientos o necesidades del usuario.
- El nombre de usuario será asignado por el administrador del sistema.
- Para la creación del nombre de usuario se considerará utilizar el número de cédula del usuario.
- Para garantizar que la clave de acceso de usuario sea segura, ésta deberá ser de al menos seis caracteres alfanuméricos.
- En el sistema se establecerán distintas categorías de usuarios en función de las actividades que el usuario realizará como Administrativos, Docentes y Alumnos.
- Para la creación de la cuenta y asignación de un "nombre de usuario" y "clave", el usuario deberá indicar la siguiente información que será empleada para la creación de la cuenta de usuario en el servidor

    - Primeramente la información general del usuario que se lista a continuación:

        a. Nombre de usuarios (Username)
        b. Clave (Password)
        c. Grupo (Group)

Por defecto si el usuario no se ha autenticado y desea acceder a una dirección web, se le mostrará una página de autenticación alojada en el cliente RADIUS, en esta página se le solicitará ingresar el "nombre de usuario" y la "clave" que le fuere **Usos prohibidos**

8.5.6.3. Queda prohibido:

- El uso simultáneo de una cuenta desde dos dispositivos diferentes.
- El uso para generar ganancias monetarias personales o propósitos comerciales que no estén directamente relacionados con asuntos que la propia Universidad autoriza.
- Descargar servicios como audio y video.
- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico (ej. antenas) más allá de los límites físicos del Área. El acceso a la red inalámbrica se restringe al campus universitario.
- El uso del servicio para molestar, acosar, intimidar, amenazar a otros o atente contra la integridad de los usuarios o para interferir con asuntos propios de las autoridades Universitarias.
- No deberá acceder a Páginas WEB relacionadas con Pornografía, Sexo, Violencia, Música, Videos, entre otros, que no tengan vinculación con sus obligaciones institucionales.
- Divulgar la clave de acceso de su cuenta personal, que le sea asignada para el uso del Internet.
- Acceder al Internet con cuentas asignadas a otros usuarios sin su previa autorización.
- Enviar mensajes con archivos anexos a través de la mensajería instantánea (Aplicación para Conversación o Chat, como Messenger)
- Asignar dinamicamente o estatica la ip, basada en dirección MAC del cliente, en capa 2.
- Controlar los puertos a nivel de firewall.

8.6. VALIDACIÓN DEL SERVIDOR

Luego de realizar las configuraciones correspondientes tanto en hardware como en software para la implementación del Servicio de autenticación Radius en la red inalámbrica del Área de Energía, Industrias y Recursos Naturales no Renovables de la Universidad Nacional de Loja, se planteó una encuesta acerca de dicho servicio a las siguientes personas: **(Para mayor detalle revisar anexo # 6 donde se encuentran las encuestas dirigidas a los usuarios de la red inalámbrica AEIRNNRSegWifi)**

- Estudiantes del AEIRNNR
- Docentes del AEIRNNR
- Personal administrativo del AEIRNNR

De las entrevistas realizadas se obtuvieron los siguientes resultados:

8.6.1. Resultados de la Encuesta Aplicada a los Usuarios del servicio de autenticación Radius en la red inalámbrica del Área de Energía, Industrias y Recursos Naturales no Renovables de la Universidad Nacional de Loja

1. **Pudo configurar satisfactoriamente la tarjeta de red inalámbrica.**

Tabla 8.43 Resultados Pregunta 1

ALTERNATIVAS	FRECUENCIA	%
Si	13	100
No	0	0
TOTAL	**13**	**100**

Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR

Elaboración: Los Autores

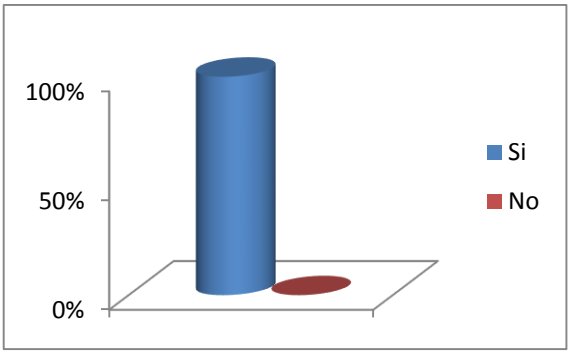


Figura 8.85 Resultado Pregunta 1
Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

El 100% de los encuestados describen que configuraron su tarjeta de red inalámbrica sin inconvenientes.

2. **Dados su usuario-contraseña pudo acceder a la red inalámbrica AEIRNNRSegWifi?**

Tabla 8.44 Resultados Pregunta 2

ALTERNATIVAS	**FRECUENCIA**	**%**
Si	13	100
No	0	0
TOTAL	**13**	**100**

Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

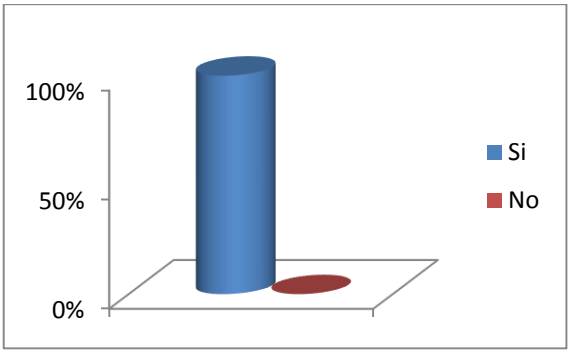


Figura 8.86 Resultado Pregunta 2
Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

El 100% de los encuestados refieren que dado su usuario-contraseña pudieron acceder a la red inalámbrica sin inconvenientes.

3. ¿Qué nivel de satisfacción tubo al conectarse a la red inalámbrica del AEIRNNRSegWifi?

Tabla 8.45 Resultados Pregunta 3

ALTERNATIVAS	FRECUENCIA	%
Bueno	11	84.61
Regular	2	15.34
Malo	0	0
TOTAL	**13**	**100**

Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

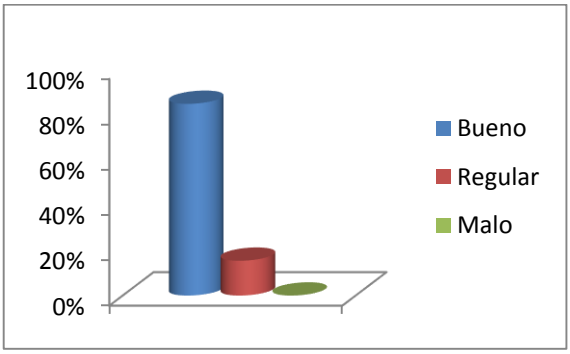


Figura 8.87 Resultado Pregunta 3
Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

De lo anterior concluimos que el 84.61% de los encuestados opinan que el nivel de satisfacción que tuvieron al conectarse a la red inalámbrica AEIRNNRSegWifi fue Bueno y el 15,34% restante manifiestan que el nivel de satisfacción que tuvieron al conectarse a la red inalámbrica AEIRNNRSegWifi fue Regular. Ninguno de los encuestados responde que el nivel de satisfacción que tuvieron al conectarse a la red inalámbrica AEIRNNRSegWifi fue Malo.

4. **¿Considera que el servicio de seguridad en redes inalámbricas es una prestación que se debería implementar en el AEIRNNR definitivamente?**

Tabla 8.46 Resultados Pregunta 4

ALTERNATIVAS	FRECUENCIA	%
Si	13	100
No	0	0
TOTAL	**13**	**100**

Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR

Elaboración: Los Autores

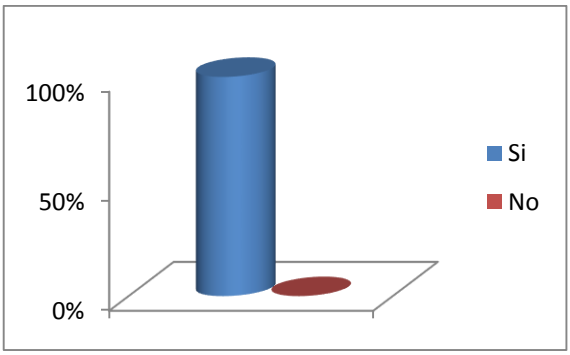


Figura 8.88 Resultado Pregunta 4
Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

El 100% de los encuestados consideran que el servicio de seguridad en redes inalámbricas es una prestación que si se debería implementar en el AEIRNNR definitivamente. Al explicar los encuestados el porqué, describen lo siguiente:

- Para poder controlar el acceso al Internet del Área y para que la red no se sature.
- Para poder tener un acceso seguro a la red inalámbrica.
- Para dar más facilidades a la conexión a Internet.
- Para poder evitar inconvenientes con los bloqueos de IP
- Para que exista una mayor seguridad en la red para los estudiantes pertenecientes al área

- Para que ninguno que pertenezca al Área pueda acceder a la red inalámbrica
- Porque es exclusividad de todos hacer uso de la red inalámbrica
- Para poder tener seguridad en actividades académicas y administrativas
- El Área debe contar con este tipo de seguridad inalámbrica permanentemente para que no se congestione la red y tener un mejor servicio.
- Siempre es necesario que todo proceso garantice su manipulación con medios seguros para el manejo de información.

5. **De las siguientes alternativas que Ud. conoce escoja, cual (es) cree que se debería implementar para mejorar la seguridad en las redes inalámbricas en el AEIRNNR.**

Tabla 8.47 Resultados Pregunta 5

ALTERNATIVAS	FRECUENCIA	%
WEP	3	23
WPA	1	7.69
RADIUS	9	69.23
TOTAL	**13**	**100**

Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR

Elaboración: Los Autores

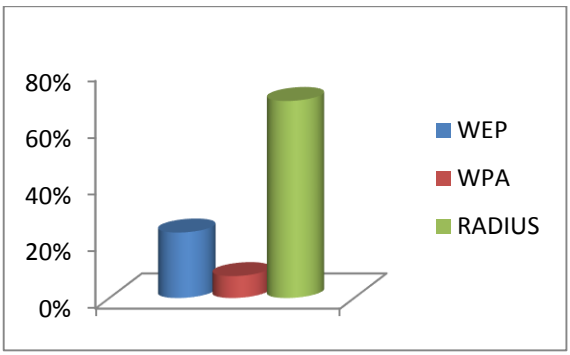


Figura 8.89 Resultado Pregunta 5
Fuente: Encuesta a los usuarios del servicio de autenticación Radius en la red inalámbrica del AEIRNNR
Elaboración: Los Autores

De lo anterior concluimos que el 69.23% de los encuestados opina que se debería implementar RADIUS para mejorar la seguridad en las redes inalámbricas en el

AEIRNNR, el 23% responde que se debería implementar WEP para mejorar la seguridad en las redes inalámbricas en el AEIRNNR, el 7.69% restante contesta que se debería implementar WPA para mejorar la seguridad en las redes inalámbricas en el AEIRNNR

9. VALORACION TECNICO - ECONOMICA

La valoración técnico-económica del presente proyecto se la realiza describiendo los recursos humanos, recursos técnicos, recursos materiales y recursos tecnológicos que se han intervenido, así como la aproximación del costo real del proyecto ya en ejecución.

La mayoría de las herramientas de desarrollo así como las aplicaciones utilizadas han sido de libre distribución, por lo que se facilita la obtención de estos recursos y de la información relacionada a su utilización con respecto a las seguridades de redes inalámbricas. Todo esto se encuentra a libre disposición en Internet lo que se facilita el acceso a estos recursos a cualquier persona que desee utilizarlos sin necesidad de pagar por alguna licencia.

Tabla 9.1 Aproximación del Costo Real del Proyecto

DESCRIPCIÓN	CANTIDAD	# HORAS	V/U	V/T
Recursos Humanos				
Investigadores	2	440	2.50	2200.00
Profesionales del campo de Redes (Jefatura Informática UNL)	2		0.00	0.00
Directora del Proyecto – Docente de la Carrera de Ingeniería en Sistemas	1		0.00	0.00
Recursos Técnicos				
Hardware				
Procesador Pentium IV 1.6 Mhz Disco Duro 80 GB Memoria 128 MB	1		1000.00	200.00
Procesador Pentium IV 1.6 Mhz Disco Duro 40 GB	1		0.00	0.00

Memoria 512 MB				
Memory Flash 1GB	2		30.00	60.00
Managed Ireless Access Point DWL-3200AP	1		0.00	0.00
Software				
Software Libre para la configuración del servidor de Freeradius (Linux-Debian)			0.00	0.00
Software Libre para la configuración del servidor de LDAP (Linux-Debian)			0.00	0.00
Office 2007			0.00	0.00
Recursos materiales				
Resmas 500 hojas de papel 75 g/m2 tamaño A4	2		3.20	6.40
Cartuchos de tinta para impresora.	3		2.50	7.00
Caja de CD's	1		10.00	10.00
Recursos Tecnológicos				
Internet.		112	0.8	89.60
Varios			315.00	315.00
COSTO REAL DEL PROYECTO				2888.00

10. CONCLUSIONES

Sobre el presente trabajo se obtuvieron varias conclusiones sobre la gestión de seguridad en una red inalámbrica, basadas en la investigación teórica del problema y en el desarrollo de la solución. A continuación se mencionarán cada una de ellas.

- La realidad en la que se encuentra La Universidad Nacional de Loja, permitió identificar falencias como: no contar con la utilización de un servidor de autenticación, la comunicación entre el Access Point y el Cliente no es cifrada, no está integrado a otros componentes de gestión de la red, y está sujeto a ataques del tipo snniffing.

- La red Inalámbrica de la Universidad Nacional de Loja en un 80% no es segura, debido a que las políticas de seguridad en un 40% no se encuentran bien definidas, estando vulnerables a agresiones desde el exterior.

- El personal de los centros de cómputo no son profesionales de la rama de Computación, por lo que se obtuvieron inconvenientes en el momento de la recolección de información, puesto que ellos poseían una información empírica de este campo.

- El D'link DWL3200ap en las redes inalámbricas posee protocolo RADIUS. Encontrándose inconvenientes en los Switch Capa 2 del AEIRNNR los cuales no soportan tal protocolo.

- La distribución que se empleo para el servidor Freeradius es Debían 5, dando problemas en las distribuciones Ubuntu y Fedora por la incompatibilidad de librerías con el servidor Freeradius.

- La versión apt de Freeradius desde los repositorios de Debían, no traía el módulo eap+ttls para Openssl, por lo que se opto por instalar desde los códigos fuentes.

- Debido a políticas internas de la Universidad Nacional de Loja no se logró hacer la conexión con la base de datos del SGA, por lo que se tuvo que levantar una base de datos paralela de todos los alumnos, profesores y administrativos del AEIRNNR .

- En escenarios donde se requiera el uso de una red acceso publico, la solución con cliente suplicante (Secure W2), resulta una alternativa ya que ofrece autenticación de una forma transparente, algo con lo que cuenta un cliente móvil.

- La implantación de este esquema es una prestación que se debería optar en su totalidad. Lo que se plantea aquí es garantizar un medio de acceso seguro entre el cliente móvil y el punto de acceso a la red (AP).

11. RECOMENDACIONES

Sobre la base de los resultados obtenidos en la presente tesis, se considera plantear las siguientes recomendaciones:

- La adquisición de un Switch Wireless que permita la gestión, mantenimiento y seguridad de la red inalámbrica en el espacio radioeléctrico, que se integre con la tecnología existente es decir un controlador inalámbrico de la marca Cisco que permita la escalabilidad de la red.

- La adopción de Políticas y mejoras practicas, de manera que se vean involucrados usuarios y administradores con el fin de brindar un servicio con altos niveles de calidad y seguridad.

- Los servidores FreeRADIUS, OpenLDAP, Mysql se deberían ubicar en máquinas distintas; es decir, en distinto hardware; ya que estos servidores (sobretodo el Freeradius y el Mysql) se encontrarán en constante actividad solicitando y registrando datos.

- Los cambios de configuraciones, habilitación o eliminación de servicios que se realice, deben hacerse primero en un ambiente de pruebas, y luego del análisis de los resultados, incorporarlo al ambiente real.

- Realizar auditorías a la gestión de seguridad, para validar si cumple con los requerimientos de seguridad que necesita la Universidad.

- Se hace necesario contar con una Infraestructura de clave pública que permita la gestión de certificados para servidores y clientes, lo que incrementará el nivel de seguridad en los procesos de cifrado y control de acceso a servicios de la red.

- Implementación del esquema para la Asignación dinámica de VLANs para los clientes de la red cableada, lo que garantizará a sus usuarios acceder a los servicios de la red basados en su perfil de usuario en cualquier equipo de la red

ingresando sus credenciales. A sí mismo el administrador de la red se evitará de realizar cambios en los equipos de red.

- Establecer listas de control de acceso por direcciones físicas o de MAC (Media Access Control) de los dispositivos que acceden a la red, combinando mecanismos de autenticación a la red y cifrado de datos

12. BIBLIOGRAFIA

SITIOS WEB:

- GREEN, W.B. 1993 Protocolo AAA en redes inalmbricas [//74.125.77.132/search?q=cache:7493CxM-n5UJ:www.imaginar.org/digitalizacion/manuales/manual_digitalizacion.pdf+digitalizacion+de+documentos&hl=es&ct=clnk&cd=3&gl=ec&client=firefox-a]Sevilla [Consulta: 06 Julio 2009]
- 80211-planet.com
- commsdesign.com
- drizzle.com/~aboba/IEEE/
- ebcvg.com
- [es.kioskea.net/contents/wireless/wlintro.php3],[Consulta, 12 de Agosto 2009]
- [es.wikipedia.org/wiki/IEEE_802.11.html] Argentina [Consulta 15 Mayo 2009]
- [es.wikipedia.org/wiki/Red_inal%C3%A1mbrica],[Consulta, 12 de Agosto 2009]
- [es.wikipedia.org/wiki/Wi-Fi.html] España [Consulta 15 MAyo 2009]
- hispasec.com
- madridwireless.net
- OCHOA, Beatriz 1996 Procesos de Autenticación y Autorización [monografias.com/trabajos11/metods.html]Colombia [Consulta: 06 Julio 2009]
- MACKAY, Patrick, 2004 seguridad SSL[msmvps.com/blogs/pmackay/archive/2004/11/27/easim1.aspx] Argentina[Consulta: 04 Junio 2009]
- neworder.box.sk
- personaltelco.net
- NAVARRO , X, 2000 ¿Seguridad en una intranet? [poliedric.com/docs/certdigital.php]Barcelona [Consulta: 04 Junio 2009]
- securitywireless.info

- FARIAS, Mariela , 2003 seguridad en redes [en linea] Argentina [seguridadwireless.net/] [Consulta 16 Mayo 2009]
- standards.ieee.org/getieee802/802.11.html
- valenciawireless.org

13. ANEXOS

ANEXO 1: PROYECTO DE TESIS DE GRADO

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

INGENIERÍA EN SISTEMAS

PROYECTO DE TESIS DE GRADO

TEMA:

"DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACION EN EL AREA DE ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, UTILIZANDO HERRAMIENTAS OPEN SOURCE."

AUTORES:

GILVER STALIN AGUILAR PUCHAICELA

JANNETH ELIZABETH MONCAYO ROMERO

LOJA – ECUADOR

2010

1. TITULO:

“DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACION EN EL AREA DE ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, UTILIZANDO HERRAMIENTAS OPEN SOURCE.”

2. PROBLEMÁTICA

2.1. SITUACIÓN PROBLÉMICA

La Universidad Nacional de Loja posee varios medios de comunicación (telefónicas, redes de datos), que le permiten mantener una relación constante entre las cinco Áreas Académicas Administrativas que la conforman, las Unidades de Desarrollo y los diferentes organismos, así como también el mundo exterior.

Nuestro centro de estudios superiores no puede quedar exento de estar a la par de la tecnología. Es por eso que se ha creído conveniente presentar una alternativa que permita la comunicación rápida y económica, utilizando la red de datos existente en el campus universitario.

La solución está basada en la seguridad en los datos de la intranet, la misma que está siendo usada en instituciones educativas, empresas e industrias a nivel mundial; pero debido a que nos encontramos en un mundo donde las grandes empresas de telecomunicaciones han tenido a lo largo de la historia hegemonía, también está tratando de apoderarse de esta nueva tecnología, brindando soluciones empresariales a costos muy elevados. No obstante, existe la posibilidad de usar software libre, para poder migrar a lo que se refiere seguridad, donde los costos bajan considerablemente a nivel de hardware y software para la implementación y ejecución de esta tecnología.

Seguridad en una intranet, es la tecnología que permite la transmisión de fragmentos de datos a través de Internet. Mientras la transmisión de datos e información ha sido primordial en la aplicación en sistemas de información, ha generado grandes expectativas por el ahorro de recursos que ésta representa.

Algunas de las ventajas de usar seguridad en los datos de manera breve tenemos: integración sobre una intranet un servicio más de la red, tal como otros servicios informáticos, las redes IP son la red estándar universal para la Internet, Intranets y

Extranets, estándares efectivos (H.323 y SIP), uso de las redes de datos existentes, entre otras.

La Universidad Nacional de Loja tiene implementado el backbone de fibra óptica con el respectivo cableado en cada uno de los edificios, permitiendo que la mayoría del personal de la universidad tenga acceso a los diversos servicios y facilidades que soporta la red.

El campus de la UNL cubre un área geográfica bastante grande y no es posible realizar cableado estructurado en cada rincón de la Universidad porque los costos de implementación, mantenimiento y administración son muy altos; para esto, una solución confiable y que ofrece gran flexibilidad es el uso de la tecnología inalámbrica por las ventajas antes expuestas.

El uso de la tecnología inalámbrica en el campus de la Universidad, permite por un lado que el personal que por razones laborales está en constante desplazamiento, desempeñe mejor las tareas que estén afines con el uso de los servicios que soporta la red LAN, y, que se pueda extender los servicios a los lugares de difícil acceso. Por otra parte el acceso a los servicios de red se ha expandido para permitir que los estudiantes puedan acceder desde las aulas, biblioteca, laboratorios y en general en los lugares de cobertura inalámbricos, lo que permite que el aprendizaje y sus métodos tengan una nueva herramienta para su mejor desempeño.

Sin embargo, junto con su funcionalidad y demás ventajas, este tipo de implementaciones trae consigo importantes riesgos de seguridad que afrontar, muchos de ellos asociados a la inexistencia de delimitación física de forma clara, y otros más importantes asociados a la carencia de mecanismos de seguridad suficientemente fuertes que protejan el acceso a los recursos tecnológicos y a la información.

Con la aparición de nuevas tecnologías , estándares y protocolos de comunicación que se especializan en ofrecer soluciones el presente trabajo se ha encaminado al **DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACION EN EL AREA DE ENERGIA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, UTILIZANDO HERRAMIENTAS OPEN SOURCE,** donde el usuario podrá acceder a la red pública para Internet , en forma controlada cumpliendo así con dos normas de validación por dirección física (MAC) y por usuario y contraseña, adicionalmente se incluye la seguridad, para evitar el acceso de usuarios a la red de datos privadas existentes, cumpliendo así con algunos estándares de los proveedores de Internet.

2.2. PROBLEMA GENERAL DE LA INVESTIGACIÓN

El análisis de esta problemática nos permite configurar el siguiente problema de investigación: **"Las redes de datos públicas y privadas de la Universidad Nacional de Loja no cuentan con un esquema de seguridad".**

2.3. DELIMITACIÓN.

A través de este proyecto pretendemos realizar un estudio que nos permita a través del uso de la intranet de la Universidad, realizar el diseño y la implementación del esquema de seguridad para los usuarios que hacen uso de la intranet. El diseño se lo va a desarrollar evaluando la situación actual de la red de datos, aplicabilidad y uso y las falencias existentes. La implementación se la realizará buscando mecanismos de seguridad que se acople a sistemas AAA (Autentificación, Autorización, Administración), luego dar apertura a la autenticación por MAC[65], posteriormente se incorpora un HotSpot con portal-cautivo para validación de usuario-contraseña, además se realizará la configuración de un servidor usando software libre.

2.3.1. PROBLEMAS ESPECÍFICOS DE INVESTIGACIÓN

- Las falencias del sistema actual de la Universidad han provocado que se desaprovechen los recursos de red de datos.
- No existe un conocimiento claro de los protocolos que se requiere para la implementación del esquema de seguridad en redes de datos, así como también, se desconoce las ventajas de cada uno de ellos.
- No existe un documento en el que contenga políticas de seguridad en redes de datos

[65] Es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red.

- No se conoce las estrategias de implementación de seguridad en la red de datos de la Universidad Nacional de Loja.
- No contar con medios para realizar pruebas la que determinen la eficiencia del mismo.
- No existe la disposición del personal administrativo para la ejecución del mismo.

2.3.2. ESPACIO

Luego de la implementación del servidor el servicio quedará listo para ser empleado por todos los usuarios de la red de datos, pero por razones de costos los investigadores utilizaran herramientas Open Source y configuraran solo los servidores del Área de Energía, las Industrias y los Recursos Naturales no Renovables.

2.3.3. TIEMPO

En cuanto al tiempo que hemos planificado para poder desarrollar nuestro proyecto, se tiene un estimado de seis meses aproximadamente, empezando en el mes de abril para concluir en el mes de octubre, con 153 días labrables.

2.3.4. UNIDADES DE OBSERVACION

- Realidad actual de la red interna de la Universidad Nacional de Loja
- Redes de Datos
- Hardware y Software para la implementación del esquema de seguridad en el Área de Energía, las Industrias y Recursos Naturales no Renovables.
- Seguridad Física.

3. JUSTIFICACIÓN

3.1. JUSTIFICACIÓN

El proyecto **"Diseño del esquema de seguridad para la intranet de la Universidad Nacional de Loja e implementación en el Área de Energía, las Industrias y los Recursos Naturales no Renovables, utilizando herramientas Open Source."**, se justifica plenamente por los siguientes considerandos.

- ✓ **JUSTIFICACION ACADEMICA**

La Universidad Nacional de Loja, es el centro de estudios superiores más reconocido en el sur del Ecuador, y ha sido pionero en brindar a los estudiantes medios a través de los cuales puedan desenvolverse en su vida profesional, como la Investigación, que es el eje fundamental del Sistema Académico Modular por Objetos de Transformación (SAMOT). El presente proyecto de Tesis permite crear espacios de investigación para futuros proyectos así como permitirá al Área de Energía, Industria y Recursos Naturales no Renovables tener en su campus un servicio ya muy utilizado en empresas e instituciones educativas en diversas partes del mundo, además de contar con políticas de seguridad para el uso del mismo. Los conocimientos recibidos en el transcurso de nuestros estudios superiores, nos dan la confianza que se podrá llevar adelante este proyecto.

- ✓ **JUSTIFICACION TECNICA**

En la actualidad la Universidad cuenta con una Red Interna, la misma que le permite la intercomunicación entre sus cinco Áreas Académico – Administrativas. Esto brinda desde ya, una gran ventaja para el diseño del esquema de seguridad en la Universidad Nacional de Loja. En el mundo existen programas que son acogidos por empresas realizados con lenguajes de programación libre de pagos, debido a ello acogeremos el

software libre que nos permita realizar la implementación del servicio en el Área de Energía, Industria y Recursos Naturales no Renovables.

- ✓ **JUSTIFICACION OPERATIVA**

El proyecto se realizará con la ayuda y experiencia que nos brinden desde la UDI (Unidad de Desarrollo Informático) ya que es ahí donde se controla todas las redes de datos del Área de Energía, Industria y Recursos Naturales no Renovables. Además sabemos del nivel académico de los funcionarios que laboran en el departamento ya que constantemente están actualizando sus conocimiento. También requerimos el apoyo de los docentes de la Carrera de Ingeniería en Sistemas que con la experiencia demostrada en nuestra formación académica nos brindarán la asesoría necesaria para sacar adelante este proyecto.

La ejecución del mismo permitirá establecer seguridades a las distintas redes de datos, ya que se establece independencia en las redes de acceso públicas y las redes privadas e incluso admitirá que empresas locales puedan obtener las prestaciones del presente proyecto.

- ✓ **JUSTIFICACION ECONOMICA**

El presente proyecto se justifica económicamente ya que los recursos que serán utilizados para este propósito están plenamente identificados, permitiendo de esta manera limitar el gasto económico ya que se cuenta con la posibilidad de obtener financiamiento propio para el desarrollo del proyecto. Siendo un estudio e implementación con software libre, los costos del presente proyecto no serán elevados.

3.2. VIABILIDAD.

El propósito fundamental para llevar a cabo este proyecto, será el proponer un Esquema de Seguridad que se adapte a los requerimientos y servicios de la Universidad, para lo cual se partirá de un estudio completo y objetivo de las principales tecnologías en redes

de datos utilizadas actualmente en la UNL, destacando que la implementación se realizara manejando los equipos existentes en la institución, dando así la comodidad de que los usuarios puedan contar con una seguridad en sus redes de datos, tanto privadas como públicas.

4. OBJETIVO

4.1. OBJETIVO GENERAL:

Diseñar el esquema de seguridad para la intranet de la Universidad Nacional de Loja e implementarlo en el Área de Energía, las Industrias y los Recursos Naturales no Renovables, que contemple Sistemas AAA (Autenticación, Autorización y Administración).

4.2. OBJETIVOS ESPECÍFICOS:

- ✓ Evaluar la situación actual de la red: aplicabilidad y uso, tecnología, equipamiento, topología.
- ✓ Analizar los mecanismos de seguridad que incorporen sistemas de autenticación, autorización y Administración (AAA) para redes de datos que puedan ser implementados en la Universidad Nacional de Loja.
- ✓ Seleccionar la mejor alternativa en cuanto a mecanismos de seguridad, en base a los requerimientos y prestaciones del Área de Energía las Industrias y Recursos Naturales no Renovables.
- ✓ Generar el manual de políticas de seguridad.
- ✓ Implementar el esquema de seguridad planteado, en el Área de Energía las Industrias y Recursos Naturales no Renovables como plan piloto.
- ✓ Evaluar el esquema de seguridad a implementar.

5. MARCO TEORICO

CAPITULO I

1. REDES DE DATOS

Se entiende por red al conjunto interconectado de computadoras autónomas. Es decir es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información. La red permite comunicarse con otros usuarios y compartir archivos y periféricos.

La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación.

1.1. ALAMBRICAS O CABLEADAS.

Se comunica a través de cables de datos (generalmente basada en Ethernet. Los cables de datos, conocidos como cables de red de Ethernet o cables con hilos conductores (CAT5), conectan computadoras y otros dispositivos que forman las redes. Las redes alámbricas son mejores cuando usted necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional.

1.1.1. **Medios de Trasmisión de redes cableadas**.

Por medio de transmisión, la aceptación amplia de la palabra, se entiende el material físico cuyas propiedades de tipo electrónico, mecánico, óptico, o de cualquier otro tipo se emplea para facilitar el transporte de información entre terminales distante geográficamente.

El medio de transmisión consiste en el elemento q conecta físicamente las estaciones de trabajo al servidor y los recursos de la red. Entre los diferentes medios utilizados en las LANs se puede mencionar:

1.1.1.1. **Cable de par trenzado:**

El cable de par trenzado es una forma de conexión en la que dos conductores son entrelazados para cancelar las interferencias electromagnéticas (IEM) de fuentes externas y la diafonía de los cables adyacentes.

El entrelazado de los cables disminuye la interferencia debido a que el área de bucle entre los cables, el cual determina el acoplamiento magnético en la señal, es reducida. En la operación de balanceado de pares, los dos cables suelen llevar señales iguales y opuestas (modo diferencial), las cuales son combinadas mediante sustracción en el destino. El ruido de los dos cables se cancela mutuamente en esta sustracción debido a que ambos cables están expuestos a IEM similares.

Este tipo de cable, está formado por el conductor interno el cual está aislado por una capa de polietileno coloreado. Debajo de este aislante existe otra capa de aislante de polietileno la cual evita la corrosión del cable debido a que tiene una sustancia antioxidante.

Normalmente este cable se utiliza por pares o grupos de pares, no por unidades, conocido como cable multipar. Para mejorar la resistencia del grupo se trenzan los cables del multipar.

Los colores del aislante están estandarizados, y son los siguientes: Naranja/ Blanco-Naranja, Verde/ Blanco-Verde, Azul/ Blanco-Azul, Marrón/Blanco-Marrón.
Cuando ya están fabricados los cables unitariamente y aislados, se trenzan según el color que tenga cada uno. Los pares que se van formando se unen y forman subgrupos,

estos se unen en grupos, los grupos dan lugar a superunidades, y la unión de superunidades forma el cable.

1.1.1.2. Cable coaxial

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor, en la Figura 2.1 se indica sus componentes. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales.

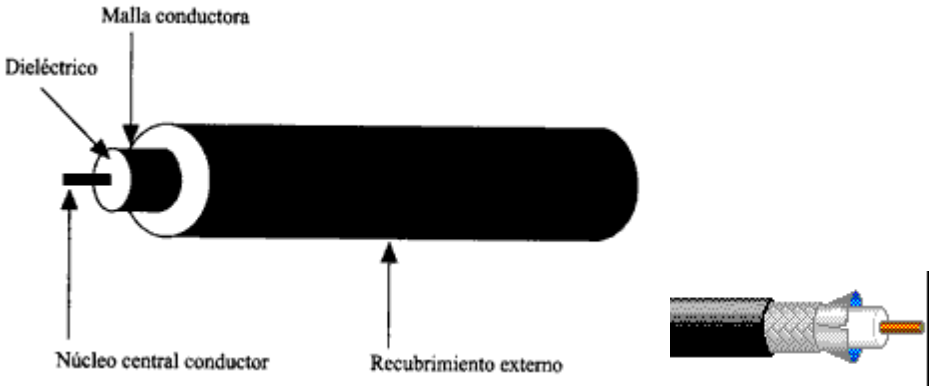


Figura 1.1 Cable Coaxial

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro. Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso.

Es capaz de llegar a anchos de banda comprendidos entre los 80 Mhz y los 400 Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica seríamos capaces de tener, como mínimo del orden de 10.000 circuitos de voz.

1.1.1.3. **Fibra Óptica**

La fibra óptica permite la transmisión de señales luminosas y es insensible a interferencias electromagnéticas externas. Cuando la señal supera frecuencias de 10^{10} Hz hablamos de frecuencias ópticas. Los medios conductores metálicos son incapaces de soportar estas frecuencias tan elevadas y son necesarios medios de transmisión ópticos.

Por otra parte, la luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente para ser utilizada en la transmisión de datos. Son necesarias fuentes especializadas: Fuentes láser. A partir de la década de los sesenta se descubre el láser, una fuente luminosa de alta coherencia, es decir, que produce luz de una única frecuencia y toda la emisión se produce en fase.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

1. Fibra monomodo. Permite la transmisión de señales con ancho de banda hasta 2 GHz.
2. Fibra multimodo de índice gradual. Permite transmisiones de hasta 500 MHz.
3. Fibra multimodo de índice escalonado. Permite transmisiones de hasta 35 MHz.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda.

Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales Ver Figura 2.2. Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas.

Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad.

Figura 1.2 Fibra óptica**.**

1.1.2. Topologías.

1.1.2.1. Topología Lineal o bus.

Una Red en forma de Bus o Canal de difusión es un camino de comunicación bidireccional con puntos de terminación bien definidos. Cuando una estación trasmite, la señal se propaga a ambos lados del emisor hacia todas las estaciones conectadas al Bus hasta llegar a las terminaciones del mismo. Así, cuando una estación trasmite su mensaje alcanza a todas las estaciones, por esto el Bus recibe el nombre de canal de difusión.

Figura 1.3 Topología bus.

1.1.2.2. Topología Anillo (Token Ring).

La topología en anillo se caracteriza por un camino unidireccional cerrado que conecta todos los nodos. Dependiendo del control de acceso al medio, se dan nombres distintos a esta topología: Bucle; se utiliza para designar aquellos anillos en los que el control de acceso está centralizado (una de las estaciones se encarga de controlar el acceso a la red). Anillo; se utiliza cuando el control de acceso está distribuido por toda la red. Como las características de uno y otro tipo de la red son prácticamente las mismas, utilizamos el término anillo para las dos. En cuanto a fiabilidad, presenta características similares al Bus: la avería de una estación puede aislarse fácilmente, pero una avería en el cable inutiliza la red. Sin embargo, un problema de este tipo es más fácil de localizar, ya que el cable se encuentra físicamente dividido por las estaciones. Las redes de éste tipo, a menudo, se conectan formando topologías físicas distintas al anillo, pero conservando la estructura lógica (camino lógico unidireccional) de éste.

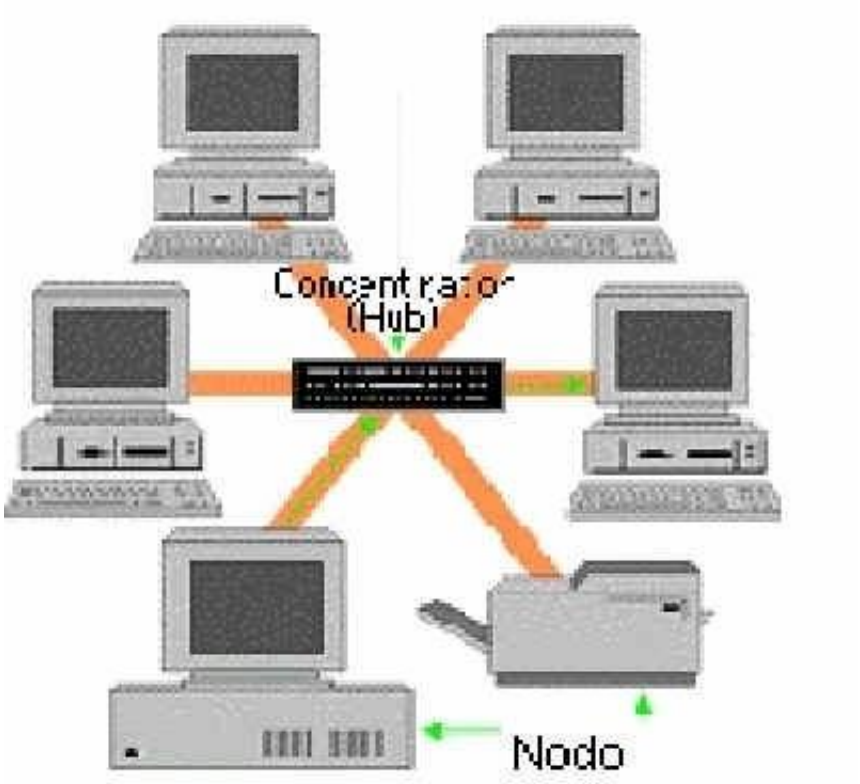


Figura 1.4 Topología anillo.

1.1.2.3. Topología Estrella.

En este esquema todas las estaciones están conectadas a un concentrador o HUB con cable por computadora.

Para futuras ampliaciones pueden colocarse otros HUBs en cascada dando lugar a la estrella jerárquica.

Por ejemplo en la estructura CLIENTE-SERVIDOR: el servidor está conectado al HUB activo, de este a los pasivos y finalmente a las estaciones de trabajo.

Ventajas:

- La ausencia de colisiones en la transmisión y dialogo directo de cada estación con el servidor.
- La caída de una estación no anula la red.

Desventajas:

Baja transmisión de datos, se puede observar esta topología en la Figura 2.5.

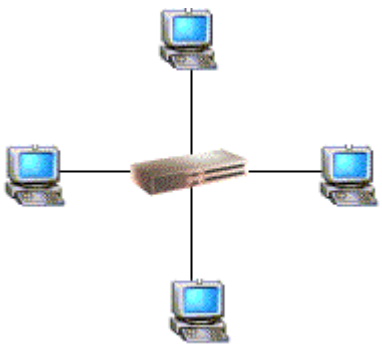


Figura 1.5 Topología estrella.

1.1.2.4. Topología tipo Malla.

Se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

1.1.3. Tipos de Redes.

Se clasifican según su Extensión y Topología. Según su Extensión tenemos redes LAN, MAN y WAN.

1.1.3.1. LAN (Redes de Área Local):

Son redes de propiedad privada dentro de un solo edificio de hasta unos cuantos kilómetros de extensión.

LAN es un sistema de comunicación entre computadoras, con la característica de que la distancia entre las computadoras debe ser pequeña.

Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir los recursos (impresoras, etc.) e intercambiar información.

Las LAN se distinguen de otro tipo de redes por las siguientes tres características: tamaño, tecnología de transmisión y topología.

Las LAN están restringidas en tamaño, las computadoras se distribuyen dentro de la LAN para obtener mayor velocidad en las comunicaciones dentro de un edificio o un conjunto de edificios, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano.

Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos y también simplifica la administración de la red.

Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas.

Las LAN tradicionales operan a velocidades de 10 a 12 GBPS, tienen bajo retardo (décimas de microsegundos) y experimentan muy pocos errores.

Las LAN pueden tener diversas topologías. La topología o la forma de conexión de la red, depende de algunos aspectos como la distancia entre las computadoras y el medio de comunicación entre ellas ya que este determina la velocidad del sistema.

Básicamente existen tres topologías de red: estrella (Star), canal (Bus) y anillo (Ring)

1.1.3.2. WAN (Redes de Área Amplia)

Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas máquinas se llaman Hosts.

Los Hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un Host a otro.

La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (Hosts), simplifica enormemente el diseño total de la red. En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos o canales) mueven los bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. Como término genérico para las computadoras de conmutación, les llamaremos enrutadores. La velocidad normal lleva un rango de los 56 KBPS a los 155 MBPS. Los retardos para una WAN pueden variar de unos cuantos milisegundos a unas decenas de segundos.

1.1.3.3. MAN (Redes de Área Metropolitana):

Una MAN es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar una serie de oficinas cercanas o en una ciudad, puede ser pública o privada Una MAN puede manejar datos y voz, e incluso podría estar relacionada con una red de televisión por cable local.

Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales.

Como no tiene que conmutar, el diseño se simplifica.

La principal razón para distinguir las MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este se llama DQDB (bus dual de cola distribuida).

El DQDB consiste en dos buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras.

Cada bus tiene una cabeza terminal (head-end), un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior, el tráfico hacia la izquierda usa el bus inferior. Un aspecto clave de las MAN es que hay un medio de difusión al cuál se conectan todas las computadoras.

Esto simplifica mucho el diseño comparado con otros tipos de redes.

1.2. INALAMBRICAS

1.2.1. IEEE 802.11

Es un estándar de IEEE desarrollado en 1997, que en su versión original ofrecía un ancho de banda de 2 Mbps, velocidad bastante reducida para dar cobertura a un número elevado de clientes. Con el tiempo han ido surgiendo variantes de este primer estándar que han dado solución a diversos problemas de las redes inalámbricas.

Tabla 1.1 Estándares IEEE 802.11

ESTÁNDAR	DESCRIPCIÓN
802.11	• Estándar WLAN original.

	• Soporta de 1 a 2 Mbps.
802.11ª	• Estándar WLAN de alta velocidad en la banda de los 5 GHz. • Soporta hasta 54 Mbps.
802.11b	• Estándar WLAN para la banda de 2.4 GHz. • Soporta 11 Mbps
802.11e	• Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	• Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	• Establece una técnica de modulación adicional para la banda de los 2.4 GHz. • Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	• Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	• Está dirigido a superar la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado). Es un estándar que aún está en proceso de desarrollo, pero parece que el futuro de las WLAN pasa por IEEE 802.11i

En la Tabla 1.1, se muestran los diferentes estándares existentes dentro del complejo IEEE 802.11. La especificación 802.11g fue ratificada por el IEEE en junio de 2003, y opera en un ancho de banda que abarca las frecuencias dentro del rango de 2.4 a 2.497 GHz del espectro de radio. IEEE 802.11g permiten una velocidad máxima de 54 Mbps.

Las redes de área local inalámbricas utilizan esta especificación de una manera mayoritaria.

1.2.2. REDES DE ÁREA LOCAL INALÁMBRICAS

Las redes inalámbricas están definidas en el estándar 802.11 [IEEE80211] de la *IEEE*[66]. El estándar 802.11 es un miembro de la familia 802 [IEEE802], y consiste en una serie de especificaciones para las tecnologías de redes de área local (*LAN*). Dichas especificaciones están enfocadas en las dos capas inferiores del modelo *OSI* debido a que incorporan elementos tanto de la capa física (*PHY*[67]) como de la capa de enlace.

Todas la redes del tipo 802 poseen ambas capas, la capa de enlace tiene por objeto determinar cómo se accede al medio de transmisión para enviar o recibir los datos, pero los detalles de cómo esos datos son transmitidos o recibidos es el objeto de la capa.

Las especificaciones individuales en la serie 802 se identifican por segundo número. Por ejemplo, 802.3 [IEEE8023], es la especificación para las redes denominados genéricamente *Ethernet CSMA/CD*[68]. 802.5 es la especificación para *Token Ring.* 802.2 especifica una capa de enlace común, la *LLC*[69] que puede ser utilizada por cualquier tecnología de *LAN* de una capa inferior. En la especificaciones 802.1 , en la Figura 2.6 se muestra la familia del Protocolo IEEE 802

66 I*nstitute of Electronics and Electrical Engineers*, Instituto de Ingenieros en Electrónica y Electricidad.
67 Abreviatura del inglés de la palabra *Physical*, física.
68 del inglés *Carrier Sense Multiple Access with Collision Detection*, sensado de portadora con acceso múltiple y detección de colisiones.
69 del inglés *Logical Link Control,* control del enlace lógico.

,se definen las características de administración como 802.1D (*Bridging*[70]) o 802.1Q (*VLANs*[71]).

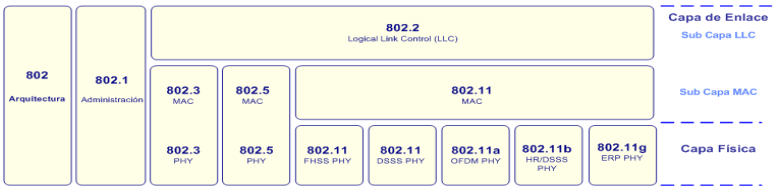


Figura 1.6 Familia del Protocolo IEEE 802

1.2.3. REDES INALAMBRICAS

Las redes inalámbricas son aquellas en las cuales se realiza un intercambio de datos por medio de la propagación de ondas electromagnéticas las cuales llevan la información, estas se encuentran comunicándose entre si como un conjunto de ordenadores que en especifico no son mas que los diferentes computadores de los usuarios que se encuentren dentro del rango de irradiación y le sea permitido el ingreso a la red.

Algunas computadoras vienen equipadas para el servicio inalámbrico. Los ordenadores más nuevos vienen adaptados para Wi-Fi. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

Las características principales de las redes inalámbricas por onda de radio es que las fuentes de interferencia existen en mayor cantidad que las fuentes para las redes cableadas. Al utilizar el aire como medio de transmisión para las ondas de radio, estas se encuentras expuestas a interferencias generadas por el mismo ambiente (humedad, tormentas eléctricas, etc.), el campo magnético de la tierra, otras ondas de radio como las antenas de radiodifusión; y la cobertura que ofrecen es directamente proporcional a

[70] del inglés *Bridge*, especifica las conexiones de puente.
[71] del inglés *Virtual LANs*, redes virtuales.

la potencia de la antena, aunque los estándares de transmisión juegan un papel de regulación en las potencias y frecuencias a ser utilizadas para la transmisión.

Las redes inalámbricas empezaron a cobrar fuerza desde que los costos de los equipos que permiten la conectividad empezaron a bajar, y esto permitió la incursión de la tecnología inalámbrica en diferentes aspectos de la vida diaria. Muchos lugares como aeropuertos, escuelas, oficinas, restaurantes, hoteles etc. empezaron a instalar WLANs para que sus clientes o usuarios, que contaran con un dispositivo móvil de cómputo, lograran acceder a la red del lugar y hacer uso de Internet principalmente. Este tipo de redes cobró mucho auge en la mayor parte del mundo y generó ganancias que fortalecieron el uso de las redes inalámbricas en muchos más lugares.

Las redes inalámbricas no solo se han enfocado a lugares de área pequeña como lo son las casa y oficinas, inclusive edificios; en comparación con lo que son manzanas y ciudades enteras. Las redes con certificación WiMAX[72] están siendo implementadas para cubrir estos espacios geográficos tan grandes con resultados similares que ofrecen las redes Wi-Fi: independencia de los cables pero con el manejo de gran ancho de banda. Las velocidades de transferencia son más grandes que las redes Wi-Fi con lo que se garantiza gran movilidad dentro de una ciudad manteniendo la disponibilidad de los servicios.

1.2.4. ELEMENTOS DE LA INFRAESTRUCTURA DE LA RED

Los elementos que componen la infraestructura de una red inalámbrica son cuatro:

- **Estaciones:** Las estaciones son dispositivos computacionales que poseen una interfaz de red inalámbrica. Típicamente estos dispositivos son *Notebooks, PDA*, etc. pero pueden ser computadoras normales en lugares en que se ha optado no realizar un cableado de red y utilizar tecnologías inalámbricas solamente. Adicionalmente varios

[72] WiMAX, Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas

fabricantes de dispositivos electrónicos están utilizando 802.11 para comunicar dispositivos no computacionales.

- **Access Points o Puntos de Acceso (AP)*:*** *Los AP* fundamentalmente cumplen la función de *bridge* entre una red inalámbrica y una red cableada, transformando los marcos 802.11 a otro tipos de marcos para poder enviarlos al resto de la red. Esta no es la única función que cumplen los *AP*, pero es la más importante.

- **Medio de Transmisión Inalámbrico:** Es el medio de transmisión utilizado por las estaciones para enviar y recibir marcos. Si bien 802.11 define varias capas físicas diferentes, las capas basadas en *RF* han sido mucho más populares que las capas basadas en transmisión Infrarroja (*IR*). El hecho de que las señale no están circunscriptas a un medio físico, como por ejemplo un cable, tiene como consecuencia que los límites geográficos de la red son difusos.

- **Sistema de Distribución*:*** El sistema de distribución es el componente lógico de 802.11 que se utiliza para reenviar los marcos a su destino. Si bien 802.11 no especifica ninguna tecnología en particular para implementar el sistema de distribución, generalmente solo se denomina *Red de Backbone*, y está formado por las conexiones *Ethernet* que unen los distintos *AP*, en la Figura 2.7 se muestra el Sistema de Distribución.

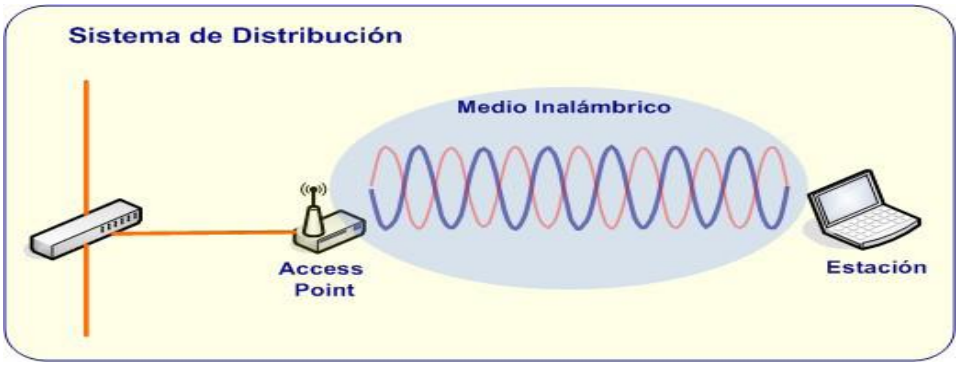


Figura 1.7 Sistema de Distribución

1.2.5. TOPOLOGÍAS DE RED

Existen dos topologías de red diferentes:

1.2.5.1 RED AD-HOC

Una red ad hoc (peer to peer) es una red de área local independiente que no está conectada a una infraestructura cableada y donde todas las estaciones se encuentran conectadas directamente unas con otras. La configuración de una red de área local inalámbrica en modo ad hoc, se utiliza para establecer una red donde no existe la infraestructura inalámbrica o donde no se requieran servicios avanzados de valor añadido.

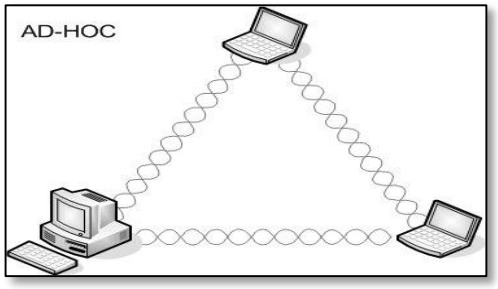


Figura 1.8 Red Ad Hoc

1.2.5.2. RED DE INFRAESTRUCTURA

En una red de infraestructura, los clientes WLAN se conectan a una red corporativa a través de un punto de acceso inalámbrico. La mayoría de las redes de área local inalámbricas corporativas opera en modo de infraestructura. El sistema desarrollado para el campus de la universidad utiliza una topología de red de este tipo.

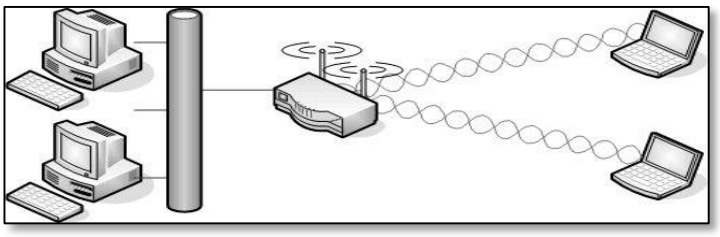


Figura 1.9 Topología en modo Infraestructura

CAPITO II

HARDWARE Y SOFTWARE PARA LA IMPLEMENTACION DEL ESQUEMA DE SEGURIDAD EN EL ÁREA DE ENERGÍA, LAS INDUSTRIAS Y RECURSOS NATURALES NO RENOVABLES.

2.1. Introducción.

En la actualidad empresas e instituciones han optado por la seguridad en sus redes de datos, con el propósito de obtener seguridad en sus comunicaciones de datos, para estos fines es necesario contar con hardware y software apropiado que permita la implementación de esta tecnología.

En el presente capítulo se abordará las características de software de seguridad, hardware necesario, refiriéndonos a particularidades del servidor, puntos de acceso de comunicación.

2.2.Software seleccionado para la configuración e implementación del servidor.

2.2.1. Arquitectura RADIUS.

Los servidores de autentificación remota de usuarios por dial-in (RADIUS) permiten la autentificación de usuarios cuando estos intentan acceder al servidor. Utilizan el protocolo AAA (autentificación, autorización y manejo de cuentas) lo cual permite un manejo adecuado de todos los clientes que hacen uso del servidor. Cuando el usuario intenta acceder a la red misma, necesita identificarse por medio de un nombre de usuario y una contraseña. Esta información es recibida por el servidor RADIUS el cual valida una petición de autentificación contra la información almacenada en su base de datos. Si la petición fue aceptada, el servidor se encargará de asignar una dirección IP y

los demás parámetros necesarios para la conexión y manejo de la cuenta. Los mecanismos de autentificación pueden ser diversos como PAP, CHAP o EAP, según lo soporte el servidor.

Al iniciar una sesión con un servidor RADIUS se puede tener un registro sobre el inicio y el final de la sesión, lo que es útil en sistemas que necesitan llevar un control estadístico sobre el tipo de usuario, tiempo de uso y propósito de uso de la red por parte de los usuarios. RADIUS es usado principalmente por proveedores de servicio de Internet (ISP) o por cualquier red que tenga la necesidad de utilizar cuentas de usuarios para sus estaciones de trabajo. RADIUS fue creado originalmente por Livingston Enterprise y en 1997, se convirtió en un estándar. Algunos estándares se encuentran descritos en: RFC2865, RFC2866, RFC3580.

RADIUS es un protocolo usado ampliamente en ambientes de red. Se aplica usualmente con dispositivos de red incrustados como ruteadores, servidores, y switches. Algunas razones de su uso son (9):

• Los sistemas incrustados generalmente no pueden manejar información de autentificación de los usuarios cuando el número de estos es muy grande. Dicho proceso requiere mayor espacio de almacenamiento que el que los sistemas incrustados poseen.

• RADIUS facilita una administración centralizada. Esto representa una ventaja cuando los usuarios son agregados y retirados durante el día, y la información de autentificación cambia constantemente.

• Se provee cierto nivel de protección contra ataques activos de escucha de la red o sniffing.

La seguridad ofrecida por el esquema nombre de usuario y contraseña, puede o no comprometer la seguridad del sistema, dependiendo de sí toda la responsabilidad recae sobre este esquema. Si se aplican un esquema de autentificación PAP, la seguridad se ve totalmente comprometida pues este mecanismo es desprotegido. Si se aplica un esquema de desafío CHAP, la seguridad recaerá en el proceso de autentificación. El proceso de manejo de cuentas de RADIUS no transporta información que debe ser mantenida como confidencial, la Figura 3.1 muestra la Arquitectura RADIUS..

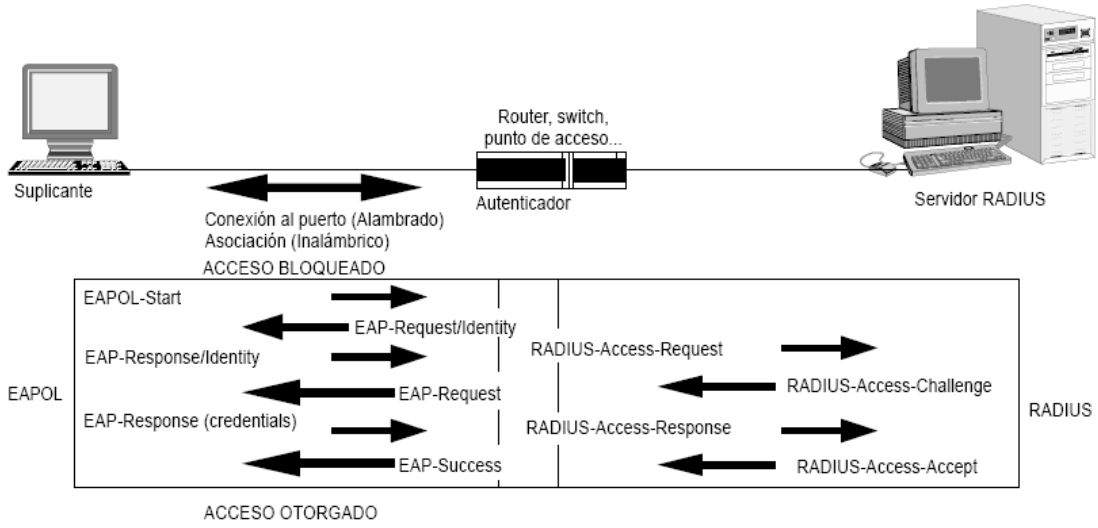


Figura 2.1 Arquitectura RADIUS.

2.2.2. Sintaxis de archivos de configuración.

Configuración en el Switch o Access Point

Username cisco privilege 15 password cisco

aaa new-model

aaa authentication login default group radius local

radius-server host 172.16.31.161 auth-port 1645 acct-port 1646 key testing123

Configuración en el Servidor Radius archivo “clients.conf”

```
client 172.16.1.18/16 {
        secret = clavesecreta
        shortname = NAS1
        nastype = cisco
}
```

Configuración en el Servidor Radius archivo “users”

```
cisco1          Service-Type = NAS-Prompt-User,
                 cisco-avpair = "shell:priv-lvl=15"
```

2.3.Hardware seleccionado para la implementación del esquema de seguridad.

2.3.1. Puntos de Acceso

Los puntos de acceso (AP) son dispositivos que permiten la conexión inalámbrica de un equipo móvil de cómputo 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, routers y switchs. 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 funciones como de administración de redes contemplando tareas como la configuración de la función de ruteo, re 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/g tiene un radio de 100 m aproximadamente.

CAPITULO III

SEGURIDAD FISICA.

3.1.Ubicación del servidor y acceso físico a él.

Los dos aspectos más importantes son: el lugar en que se encuentra ubicado el servidor y las personas que tienen acceso físico al mismo. Los especialistas en seguridad llevan mucho tiempo sosteniendo que si usuarios malintencionados tienen acceso físico, los controles de seguridad son inútiles y dicha afirmación es totalmente cierta. Salvo raras excepciones, casi todos los sistemas de computación son vulnerables a ataques *in situ.*

Desde luego, ataque puede significar muchas cosas en este contexto. Por ejemplo, hay que imaginarse que han dejado a algún usuario malintencionado solo con sus servidores durante 10 segundos, es muy probable que éstos sufran daños importantes en ese intervalo de tiempo. El usuario podría realizar un rudimentario ataque de denegación de servicio[73] desconectando cables, desconectando hardware de red o reiniciando los servidores.

Pero estos actos casi nunca se dan en oficinas. Su mayor preocupación deberían ser los usuarios locales autorizados, aquéllos que tienen al menos autorización limitada para acceder al sistema. Se ha estimado que el 80% de las intrusiones provienen del personal interno. El motivo es que este personal tiene acceso a información que los agresores remotos a menudo no pueden obtener.

Pero ésta no es la única ventaja que tiene el personal interno. La confianza es otra más. En muchas empresas, los empleados de confianza deambulan libremente sin temor a que les hagan preguntas. Después de todo, se supone que éstan en su sitio y a nadie se le ocurre cuestionar su presencia, a menos que entren en área restringida. Así que, ¿cómo se puede proteger un sistema frente a los enemigos internos?

[73] La denegación se servicio es un estado que se produce cuando un usuario deja inoperativo un servidor de forma malintencionada haciendo que deniegue el servicio a usuarios legítimos.

3.2.Estación de trabajo y seguridad.

Cuando se aseguran estaciones de trabajo, hay que preocuparse principalmente del acceso físico y del robo. Entre las herramientas de prevención típicas que se utilizan se incluyen:

- Contraseñas de BIOS y consola.
- Controles de acceso biométrico
- Dispositivos antirrobos
- Números únicos, marcados y otras técnicas.

3.2.1. Contraseña de BIOS y consola.

La mayoría de las arquitecturas (como X86, PPC o Sparc) utilizan contraseñas de BIOS-PROM, contraseñas de consola o de ambos tipos. Los fabricantes de hardware incluyen estos sistemas de contraseñas como una capa externa de seguridad, un obstáculo para disuadir a los usuarios esporádicos de fisgonear.

Las contraseñas de la BIOS o de la PROM evitan que los usuarios malintencionados accedan a la configuración del sistema, mientras que las contraseñas de consola suelen proteger los perfiles de usuario de la estación de trabajo. En cualquier caso, estos sistemas de contraseñas son, al menos, parcialmente efectivos y es conveniente usarlos siempre que le sea posible.

Sin embargo, no hay que olvidarse de establecer la contraseña de configuración y de usuario, ya que si no lo hace, podría acabar lamentándolo. Actualmente, las teclas y contraseñas predeterminadas de configuración de la BIOS de casi tidis los fabricantes son muy conocidas.

3.2.2. Controles de acceso biométrico

La seguridad física del hardware consiste en el uso de dispositivos de acceso biométrico. Estas herramientas autentican a los usuarios en base a características biológicas suyas, entre las que se incluyen:

- Olor corporal.
- Estructura facial.
- Huellas dactilares.
- Patrones de retina o de iris.
- Trazado de las Venas.
- Voz.

3.2.3. Dispositivos antirrobos

Otra amenaza es el robo, tanto del sistema entero como de componentes individuales. No es necesario que roben el servidor. Pueden llevarse los dispositivos de disco duro, memoria o tarjetas de expansión.

- Laptop Lockup evita el robo de equipos portátiles utilizando cables de acero resistente al sabotaje y un candado de cobre que se asegura al portátil a la mesa. Administra una gran variedad de portátiles.
- FlexLock-50 asegura las estaciones de trabajo con cable de media pulgada resistente a cizallas, cortaalambres y sierras para metal. Pioneer ofrece también sistemas de base metálica que aseguran las estaciones de trabajo a las mesas.
- Computer Guardian.- es un sistema antirrobo para PC independiente de la plataforma. Consta de una tarjeta de expansión y software en un disquete externo. Cuando se mueve el PC o alguien trata de forzar sus componentes, el sistema hace sonar una sirena para asustar al ladrón y avisar a los demás.
- Phazer.- es un dispositivo de seguridad de fibra óptica que detecta intentos de forzado físico. Este sistema de monitorización descansa sobre un bucle cerrado de fibra óptica. Si el bucle se abre, se genera una alarma. PHAZER es magníficos para laboratorios de computación de Universidades u otras redes grandes.

3.3.Números únicos, marcados y otras técnicas.

Algunas medidas de seguridad habituales que pueden servir como refuerzo legal son las siguientes:

- Llevar un registro meticuloso de todo el hadware, incluyendo los números de modelo serie, ya que son necesarios si se llama a la policía. A menudo no son suficiente con que se pueda reconocer una maquina por sus sonidos, chasquidos y desconchones. La policía suele exigir algo más sustancial, como numero de serie, facturas de compra, etc.
- Marque de forma permante los componentes con un número único de identificación utilizando tinta indeleble pintura fluorescente o pintura tinta ultravioleta, que es visible con luz negra. En particular, marque la placa madre, las tarjetas de expansión, las unidades de disco, el interior y el exterior de la caja de la unidad y el monitor.

6. METODOLOGIA

En la presente sección se describe la aplicación de las metodologías planteadas en el anteproyecto. La metodología nos da una visión de cómo se ha desarrollado el proceso investigativo.

Nuestra investigación estuvo planificada mediante tareas que nos han permitido encontrar los mecanismos correctos para llegar a cumplir los objetivos.

Las tareas, métodos, instrumentos que se utilizó para el desarrollo del proyecto investigativo son:

Tabla 1 Métodos e instrumentos utilizados

TAREA REALIZADA	METODOLOGÍA
Investigación bibliográfica en libros sobre seguridad en redes de datos. Investigación sobre software que contenga sistemas AAA Investigación sobre FREERADIUS Investigación acerca de la arquitectura de FREERADIUS Entrevistas con personas relacionadas al campo de Redes. Investigar sobre configuración de archivos 3Com Analizar la información recogida.	**El método sintético** (Consiste en la reunión racional de varios elementos dispersos en una nueva totalidad donde El investigador sintetiza las superaciones en la imaginación para establecer una explicación tentativa que se someterá a prueba). Este método nos permitió en primera instancia buscar en bibliografía especializada (libros, Internet), y en entrevistas con personas relacionadas y así acumular gran cantidad de información. Pero no toda la información recolectada puede ser utilizada debido a que no es verídica o porque está fuera del ámbito de la investigación planteada. Es así que se realizó un análisis de la documentación para poder tener como resultado datos verídicos que nos permitieron conocer como es

	el funcionamiento real de mecanismos de seguridad en redes. Métodos e instrumentos utilizados en estas tareas: ***Observación Directa.-*** Es aquella en la cual el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar ***Observación Indirecta.-*** Cuando el investigador entra en el conocimiento del hecho o fenómeno observado a través de las observaciones realizadas anteriormente por otra persona. ***Entrevista.-*** Consiste en el diálogo entre dos personas: el entrevistador (el investigador) y el entrevistado; se realiza con el fin de obtener información por parte de una persona entendida en la materia de la investigación. ***Mapa Conceptual.-*** Esquema gráfico que refleja un conjunto de conceptos sobre una temática específica y las relaciones que existen entre ellos. ***Lectura comprensiva.-*** Tiene por objeto el conocimiento ordenado y sistemático de un aspecto de la realidad o de los acontecimientos, hechos o ideas relacionadas con un tema específico.
Investigar cómo se encuentra distribuida la red de datos de la Universidad Nacional de Loja. Análisis de la tecnología existente (hardware, software).	Para tener una idea clara de cómo se encuentra distribuida la red de la Universidad y su situación actual, utilizamos método descriptivo que consiste en la recolección de datos directamente por los investigadores con el

Análisis de los esquemas de red (alámbrica, e, inalámbrica) actuales. Análisis de los esquemas de seguridad existentes. Definir las falencias del sistema actual y sus proyecciones de uso y crecimiento.	adicional de interpretar los mismos de una manera racional. Este método nos permitió describir la red de datos de las Área Académicas - Administrativas y Departamentos de la Universidad y realizar un análisis de la situación actual, además detallamos los equipos principales con los que cuenta la Universidad para brindar los diferentes servicios que brinda a los usuarios de la red. Métodos e instrumentos utilizados en estas tareas: Observación Directa Observación Indirecta
Obtener requerimientos funcionales y requerimientos de seguridad. Análisis de los requerimientos obtenidos. Establecer políticas de seguridad necesarias para acceder a cada recurso.	**Mapa conceptual o Mapa de conceptos,** tipo de esquema gráfico que refleja un conjunto de conceptos sobre una temática específica y las relaciones que existen entre ellos. Su finalidad es sintetizar o resumir de forma gráfica lo más significativo de un tema determinado que se refleja en un texto. Los mapas de conceptos son muy empleados en las disciplinas sociales. Es una técnica muy útil para hacer evidentes los conceptos clave, para separar la información significativa de la trivial y para establecer conexiones entre conocimientos.
Obtener el software requerido para instalar FREERADIUS. Investigación sobre configuración de archivos para FREERADIUS Instalación del software requerido para FREERADIUS	**El método científico experimental** (la aplicación más completa de la investigación científica porque permite establecer con toda claridad el principio de relación causa – efecto. Consiste en provocar voluntariamente una situación que se quiere estudiar) nos ha

Pruebas del servicio	permitido desarrollar algunas tareas planificadas. Este método nos permitió a través de software y hardware vinculado a seguridad en redes realizar pruebas que nos llevaron a definir con exactitud los mecanismos con los cuales lograremos la configuración final de: Servidor RADIUS. Seguridad en redes inalámbricas. Seguridad en redes alámbricas. Métodos e instrumentos utilizados en estas tareas: Observación Directa Observación Indirecta

6.1. MATRIZ DE CONSISTENCIA GENERAL

PROBLEMÁTICA: "Las redes de datos públicas y privadas de la Universidad Nacional de Loja no cuentan con un esquema de seguridad".				
TEMA	**PROBLEMA**	**OBJETO DE INVESTIGACION**	**OBJETIVO DE LA INVESTIGACION**	**HIPOTESIS DE INVESTIGACION**
"DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACIÓN EN EL ÁREA DE ENERGÍA LAS INDUSTRIAS Y RECURSOS NATURALES NO RENOVABLES, UTILIZANDO HERRAMIENTAS OPEN SOURCE"	La falta de un esquema de seguridad en la intranet de la Universidad Nacional de Loja, ha provocado que se desaprovechen los recursos de red de datos.	El Sistema AAA (Autorización, Autentificación, Administración) en la intranet de la Universidad Nacional de Loja.	Diseñar el esquema de seguridad para la intranet de la Universidad Nacional de Loja e implementarlo en el Área de Energía, las Industrias y Recursos, que contemple sistema AAA	Permitir que los recursos de la Universidad Nacional de Loja sean administrados de forma correcta, para que a través de el se pueda contar con un esquema de seguridad en sus datos.

6.2. MATERIALES, MÉTODOS Y TÉCNICAS DE TRABAJO

6.2.1. MATERIALES.

Los materiales que se utilizaron para el presente proyecto son los siguientes:

- Una resmas 500 hojas de papel 75 g/m2 tamaño A4
- Tres Cartuchos de tinta para impresora.
- Una caja de CD's
- Un Computador Core 2 Duo, 1 Gb RAM, disco duro 160 GB
- Una Memory flash
- Seis WRT-Radauth marcas WRT54GLA
- Seis Acces Point de marcas D-Link 'Dwl-g700 Ag'
- Software Libre para la configuración del servidor RADIUS
- Software Libre adicional para la configuración del servidor RADIUS
- Office 2007
- Sistema Operativo Linux.
- Sistema Operativo Windows.
- Internet.

6.2.2. MÉTODOS.

Los métodos de investigación escogidos para el presente proyecto son los siguientes:

- **El método sintético** (Consiste en la reunión racional de varios elementos dispersos en una nueva totalidad donde El investigador sintetiza las superaciones en la imaginación para establecer una explicación tentativa que se someterá a prueba). Este método nos permitió en primera instancia buscar en bibliografía

especializada (libros, Internet), y en entrevistas con personas relacionadas y así acumular gran cantidad de información. Pero no toda la información recolectada puede ser utilizada debido a que no es verídica o porque está fuera del ámbito de la investigación planteada. Es así que se realizó un análisis de la documentación para poder tener como resultado datos verídicos que nos permitieron conocer como es el funcionamiento real de mecanismos de seguridad en redes.

- **El método científico experimental** (la aplicación más completa de la investigación científica porque permite establecer con toda claridad el principio de relación causa – efecto. Consiste en provocar voluntariamente una situación que se quiere estudiar) nos ha permitido desarrollar algunas tareas planificadas

6.2.3. TÉCNICAS.

Algunas de las técnicas para obtener información son las siguientes.

- ✓ **Observación.**

Es una técnica que consiste en observar atentamente el fenómeno, hecho, tomar información y registrarla para su posterior análisis.

La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Entre las clases de observación tenemos:

- **Observación Directa:** Es aquella en la cual el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar.
- **Observación Indirecta:** Cuando el investigador entra en el conocimiento del hecho o fenómeno observado a través de las observaciones realizadas anteriormente por otra persona. (Libros, revistas, etc.)

Dentro del proyecto adoptaremos la observación en los siguientes casos:

- Investigar cómo se encuentra distribuida la red alámbrica e inalámbrica de la Universidad Nacional de Loja y en especial del Área de Energía, Industria y Recursos Naturales no Renovables.
- Configuración de equipos (3Com) para el servicio
- Instalación del software requerido para RADIUS.

✓ **Entrevista**

Es una técnica para obtener datos, que consiste en el diálogo entre dos personas: el entrevistador (el investigador) y el entrevistado; se realiza con el fin de obtener información por parte de una persona entendida en la materia de la investigación. De hecho la entrevista constituye una técnica indispensable porque permite conseguir datos que de otro modo sería muy difícil conseguir.

La entrevista será utilizada en la siguiente situación:

- Buscar la ayuda de personal capacitado, para poder tener una entrevista personal.

✓ **Mapa Conceptual**

Un mapa conceptual es una herramienta para la organización y representación del conocimiento, mapa conceptual es una secuencia ordenada de pasos y procesos, cuya finalidad es sintetizar o resumir de forma gráfica lo más significativo de un tema determinado que se refleja en un texto. Los mapas de conceptos son muy empleados en las disciplinas sociales.

Es una técnica muy útil para hacer evidentes los conceptos clave, para separar la información significativa de la trivial y para establecer conexiones entre conocimientos.

Esta técnica utilizaremos en las siguientes tareas:

- Investigación Bibliográfica en libros sobre seguridad en redes de datos
- Investigación en Internet sobre seguridad en redes de datos
- Analizar la información recogida.
- Investigación en Internet sobre seguridad en redes de datos

✓ **Lectura Comprensiva**

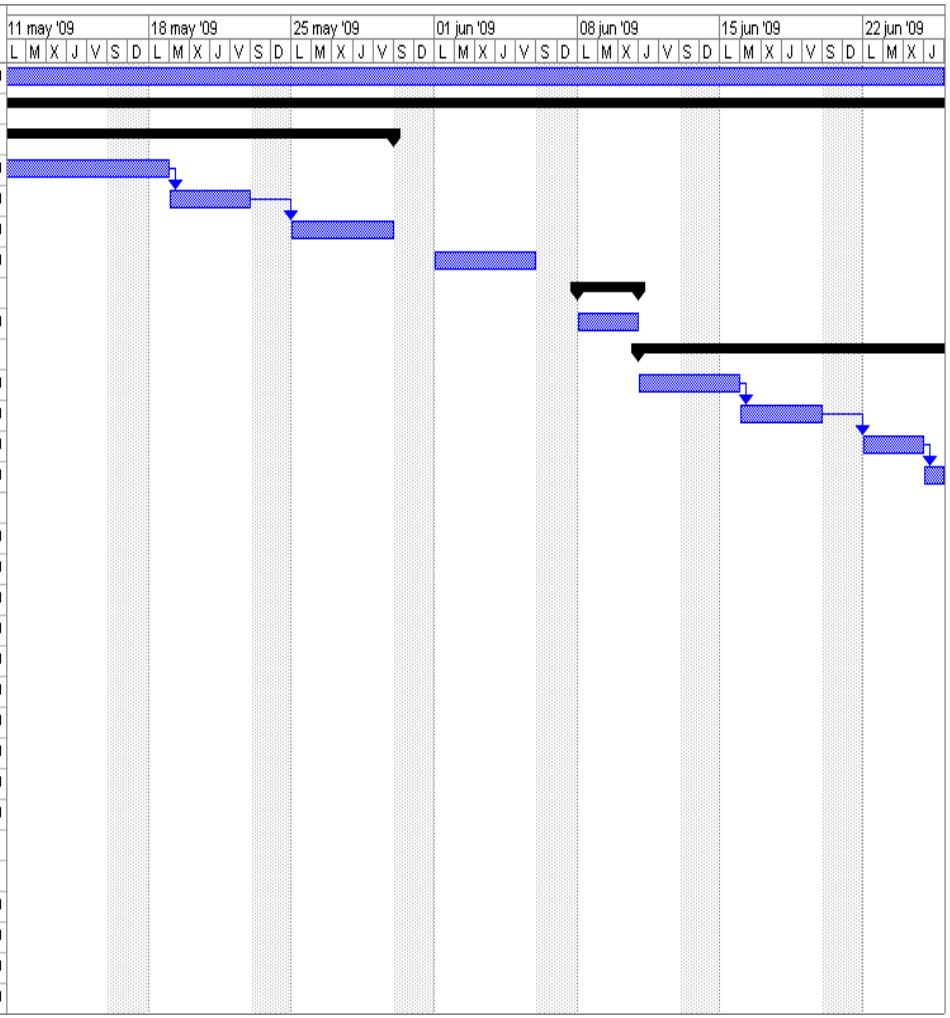
La lectura comprensiva tiene por objeto la interpretación y comprensión critica del texto, es decir en ella el lector no es un ente pasivo, sino activo en el proceso de la lectura, es decir que descodifica el mensaje, lo interroga, lo analiza, lo critica, etc.
Esta lectura requiere una estrategia especial. Debe hacerse lentamente sin prisas, con material especial, esto es, notas, apuntes, esquemas, mapas, gráficas, posibilidad de cotejar varios textos.

La lectura la utilizamos en las siguientes situaciones:

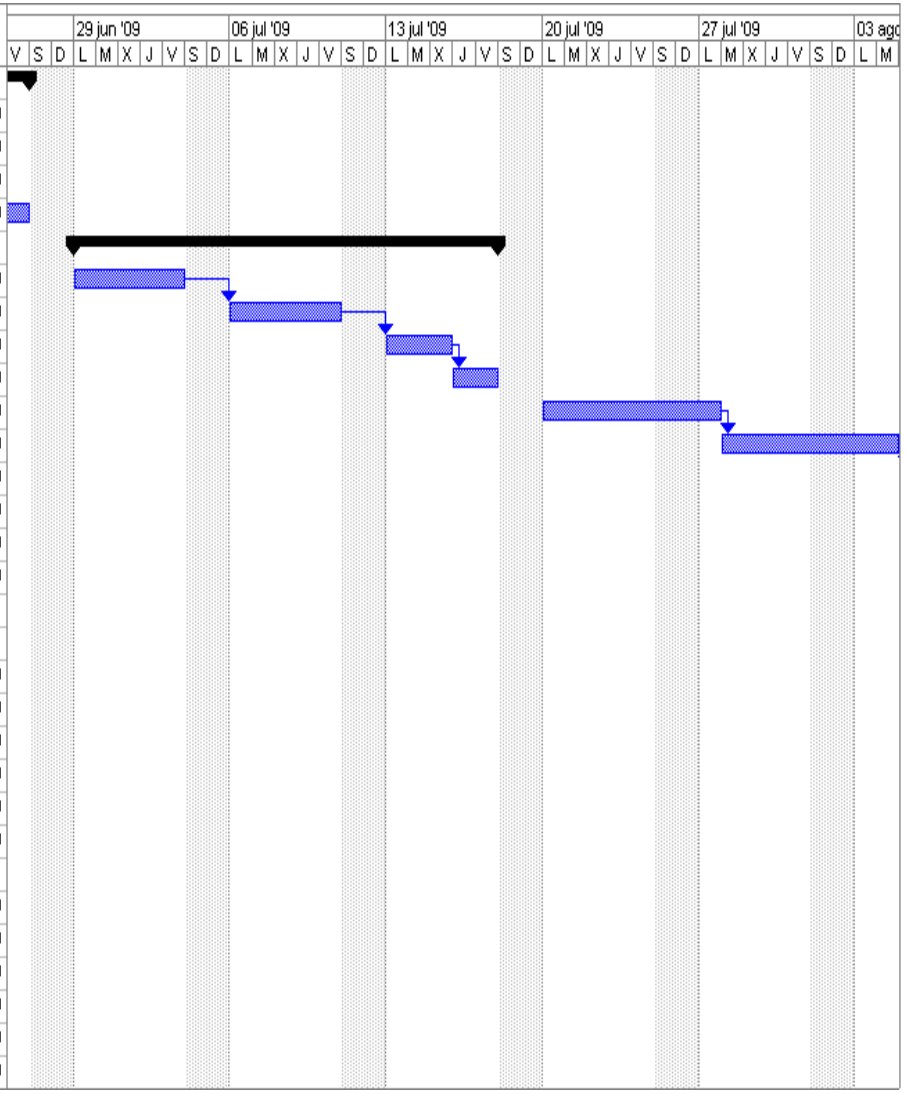
- Investigación Bibliográfica en libros sobre seguridad en redes de datos
- Investigación en Internet sobre seguridad en redes de datos
- Analizar la información recogida.
- Investigación en Internet sobre seguridad en redes de datos
- Investigación en Internet sobre configuración de archivos para RADIUS

7. CRONOGRAMA

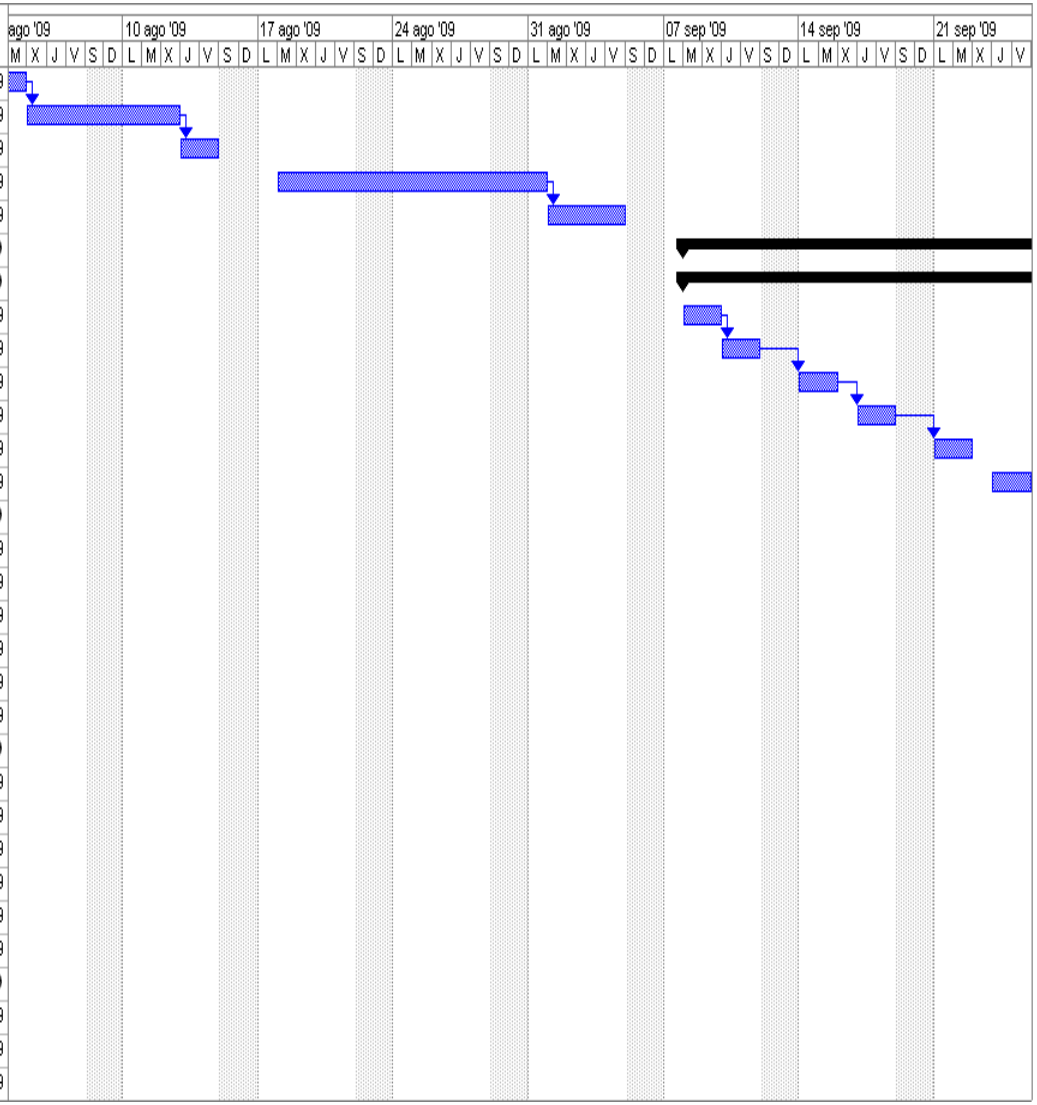
Nombre de tarea	Duración	Comienzo	Fin
DISEÑO DEL ESQUEMA DE SEGURIDAD PARA LA INTRANET DE LA UNIVERSID/	268 días	lun 11/05/09	mié 19/05/10
ESTUDIO DE LA RED DE DATOS (ALÁMBRICA E INALÁMBRICA) Y SEGURIDAD	**85 días?**	**lun 11/05/09**	**vie 04/09/09**
Investigar acerca de la red de datos	**15 días?**	**lun 11/05/09**	**vie 29/05/09**
Investigar acerca de la red de datos Alámbrica e Inalámbrica	6 días?	lun 11/05/09	lun 18/05/09
Investigar Medios de Trasmición	4 días?	mar 19/05/09	vie 22/05/09
Investigar Topologías	5 días?	lun 25/05/09	vie 29/05/09
Investigar acerca de Hadware y Software para la Implementación del esquer	5 días?	lun 01/06/09	vie 05/06/09
Investigar acerca Seguridad Física.	**3 días?**	**lun 08/06/09**	**mié 10/06/09**
Investigar acerca de la ubicación de los servidores	3 días?	lun 08/06/09	mié 10/06/09
Investigar acerca de la seguridad en redes de datos.	**12 días?**	**jue 11/06/09**	**vie 26/06/09**
Investigar acerca de la seguridad de la información	3 días?	jue 11/06/09	lun 15/06/09
Investigar los factores que intervienen en la seguridad.	4 días?	mar 16/06/09	vie 19/06/09
Investigar los tipos de ataques	3 días?	lun 22/06/09	mié 24/06/09
Investigar las técnicas de ataques	2 días?	jue 25/06/09	vie 26/06/09
Investigar acerca de las políticas de seguridad existentes.	**15 días?**	**lun 29/06/09**	**vie 17/07/09**
Investigar políticas de seguridad en redes de datos	5 días?	lun 29/06/09	vie 03/07/09
Investigar políticas de acceso a servicios de red	5 días?	lun 06/07/09	vie 10/07/09
Investigar políticas de diseño de Firewall	3 días?	lun 13/07/09	mié 15/07/09
Investigar políticas específicas del sistema	2 días?	jue 16/07/09	vie 17/07/09
Investigar sobre software que contengan sistemas AAA.	6 días?	lun 20/07/09	lun 27/07/09
Investigación sobre FREERADIUS.	6 días?	mar 28/07/09	mar 04/08/09
Investigación acerca de la arquitectura de FREERADIUS.	6 días?	mié 05/08/09	mié 12/08/09
Obtener el software requerido para instalar FREERADIUS.	2 días?	jue 13/08/09	vie 14/08/09
Investigación sobre configuración de archivos FREERADIUS.	10 días?	mar 18/08/09	lun 31/08/09
Realizar un documento técnico con la información obtenida.	4 días?	mar 01/09/09	vie 04/09/09
SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA	**57 días?**	**mar 08/09/09**	**mié 25/11/09**
Entrevista con el personal a cargo de la red de datos en la U.N.L	**14 días?**	**mar 08/09/09**	**vie 25/09/09**
Entrevista con el personal a cargo de la red de datos en Administración (	2 días	mar 08/09/09	mié 09/09/09
Entrevista con el personal encargado del centro de cómputo del Área de	2 días?	jue 10/09/09	vie 11/09/09
Entrevista con el personal encargada del centro de cómputo del Área Jur	2 días	lun 14/09/09	mar 15/09/09
Entrevista con el personal encargado del centro de cómputo del Área de	2 días?	jue 17/09/09	vie 18/09/09



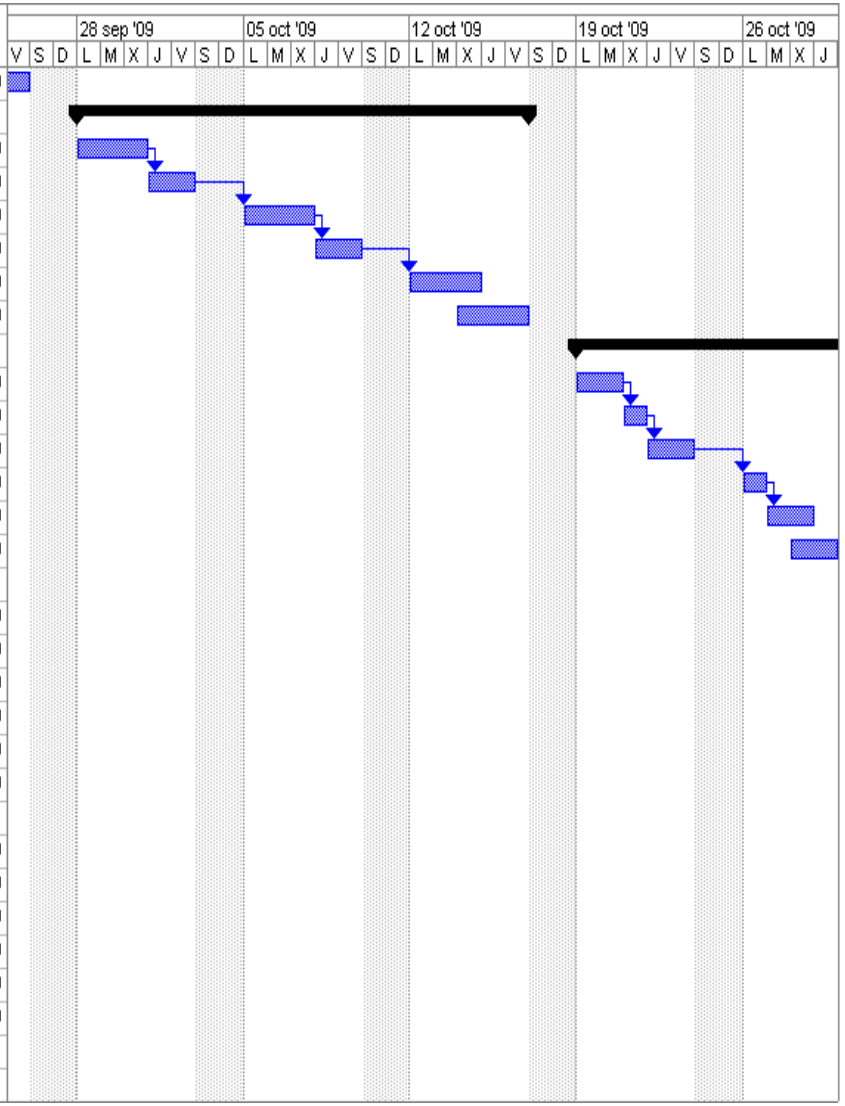
Nombre de tarea	Duración	Comienzo	Fin
Investigar acerca de la seguridad en redes de datos.	**12 días?**	**jue 11/06/09**	**vie 26/06/09**
Investigar acerca de la seguridad de la información	3 días?	jue 11/06/09	lun 15/06/09
Investigar los factores que intervienen en la seguridad.	4 días?	mar 16/06/09	vie 19/06/09
Investigar los tipos de ataques	3 días?	lun 22/06/09	mié 24/06/09
Investigar las técnicas de ataques	2 días?	jue 25/06/09	vie 26/06/09
Investigar acerca de las políticas de seguridad existentes.	**15 días?**	**lun 29/06/09**	**vie 17/07/09**
Investigar políticas de seguridad en redes de datos	5 días?	lun 29/06/09	vie 03/07/09
Investigar políticas de acceso a servicios de red	5 días?	lun 06/07/09	vie 10/07/09
Investigar políticas de diseño de Firewall	3 días?	lun 13/07/09	mié 15/07/09
Investigar políticas específicas del sistema	2 días?	jue 16/07/09	vie 17/07/09
Investigar sobre software que contengan sistemas AAA.	6 días?	lun 20/07/09	lun 27/07/09
Investigación sobre FREERADIUS.	6 días?	mar 28/07/09	mar 04/08/09
Investigación acerca de la arquitectura de FREERADIUS.	6 días?	mié 05/08/09	mié 12/08/09
Obtener el software requerido para instalar FREERADIUS.	2 días?	jue 13/08/09	vie 14/08/09
Investigación sobre configuración de archivos FREERADIUS.	10 días?	mar 18/08/09	lun 31/08/09
Realizar un documento técnico con la información obtenida.	4 días?	mar 01/09/09	vie 04/09/09
SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA	**57 días?**	**mar 08/09/09**	**mié 25/11/09**
Entrevista con el personal a cargo de la red de datos en la U.N.L	**14 días?**	**mar 08/09/09**	**vie 25/09/09**
Entrevista con el personal a cargo de la red de datos en Administración (	2 días	mar 08/09/09	mié 09/09/09
Entrevista con el personal encargado del centro de cómputo del Área de	2 días?	jue 10/09/09	vie 11/09/09
Entrevista con el personal encargada del centro de cómputo del Área Ju	2 días	lun 14/09/09	mar 15/09/09
Entrevista con el personal encargado del centro de cómputo del Área de	2 días?	jue 17/09/09	vie 18/09/09
Entrevista con el personal encargado del centro de computo del Área de	2 días	lun 21/09/09	mar 22/09/09
Entrevista con el personal encargado del centro de computo del Área de	2 días	jue 24/09/09	vie 25/09/09
Encuesta con el personal a cargo de la red de datos en la U.N.L,	**15 días**	**lun 28/09/09**	**vie 16/10/09**
Encuesta con el personal a cargo de la red de datos en Administración C	3 días	lun 28/09/09	mié 30/09/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 01/10/09	vie 02/10/09
Encuesta con el personal encargada del centro de cómputo del Área Jur	3 días	lun 05/10/09	mié 07/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 08/10/09	vie 09/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	lun 12/10/09	mié 14/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	mié 14/10/09	vie 16/10/09



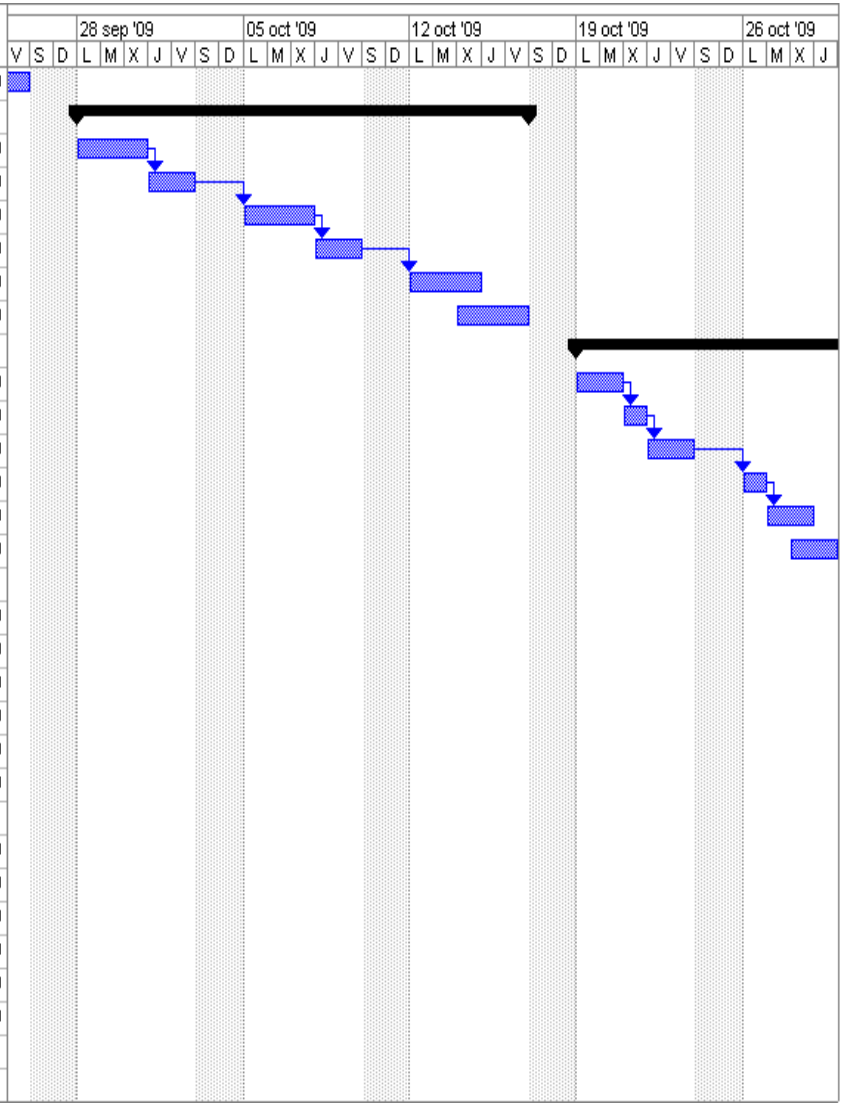
Nombre de tarea	Duración	Comienzo	Fin
Investigación sobre FREERADIUS.	6 días?	mar 28/07/09	mar 04/08/09
Investigación acerca de la arquitectura de FREERADIUS.	6 días?	mié 05/08/09	mié 12/08/09
Obtener el software requerido para instalar FREERADIUS.	2 días?	jue 13/08/09	vie 14/08/09
Investigación sobre configuración de archivos FREERADIUS.	10 días?	mar 18/08/09	lun 31/08/09
Realizar un documento técnico con la información obtenida.	4 días?	mar 01/09/09	vie 04/09/09
SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA	**57 días?**	**mar 08/09/09**	**mié 25/11/09**
Entrevista con el personal a cargo de la red de datos en la U.N.L.	**14 días?**	**mar 08/09/09**	**vie 25/09/09**
Entrevista con el personal a cargo de la red de datos en Administración (	2 días	mar 08/09/09	mié 09/09/09
Entrevista con el personal encargado del centro de cómputo del Área de	2 días?	jue 10/09/09	vie 11/09/09
Entrevista con el personal encargada del centro de cómputo del Área Ju	2 días	lun 14/09/09	mar 15/09/09
Entrevista con el personal encargado del centro de cómputo del Área de	2 días?	jue 17/09/09	vie 18/09/09
Entrevista con el personal encargado del centro de computo del Área de	2 días	lun 21/09/09	mar 22/09/09
Entrevista con el personal encargado del centro de computo del Área de	2 días	jue 24/09/09	vie 25/09/09
Encuesta con el personal a cargo de la red de datos en la U.N.L.,	**15 días**	**lun 28/09/09**	**vie 16/10/09**
Encuesta con el personal a cargo de la red de datos en Administración C	3 días	lun 28/09/09	mié 30/09/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 01/10/09	vie 02/10/09
Encuesta con el personal encargada del centro de cómputo del Área Jur	3 días	lun 05/10/09	mié 07/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 08/10/09	vie 09/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	lun 12/10/09	mié 14/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	mié 14/10/09	vie 16/10/09
Análisis de la tecnología existente (Hardware y Software) en la Unive	**9 días**	**lun 19/10/09**	**jue 29/10/09**
Análisis de la tecnología existente en Administración Central (Jefatura Int	2 días	lun 19/10/09	mar 20/10/09
Análisis de la tecnología en el Área de Educación, Arte y Comunicación	1 día	mié 21/10/09	mié 21/10/09
Análisis de la tecnología en el Área Jurídica Social y Administrativa.	2 días	jue 22/10/09	vie 23/10/09
Análisis de la tecnología en el Área de Salud Humana.	1 día	lun 26/10/09	lun 26/10/09
Análisis de la tecnología en el Área de Agropecuaria y de Recursos Natu	2 días	mar 27/10/09	mié 28/10/09
Análisis de la tecnología en el Área de Energía, Industrias y Recursos Na	2 días	mié 28/10/09	jue 29/10/09
Análisis de los esquemas de red (topología)	**12 días**	**vie 30/10/09**	**lun 16/11/09**
Análisis del esquema de red en Administración Central.	2 días	vie 30/10/09	lun 02/11/09
Análisis del esquema de red en el Área de Educación, Arte y Comunicac	3 días	mar 03/11/09	jue 05/11/09
Análisis del esquema de red en el Área Jurídica Social y Administrativa.	2 días	vie 06/11/09	lun 09/11/09



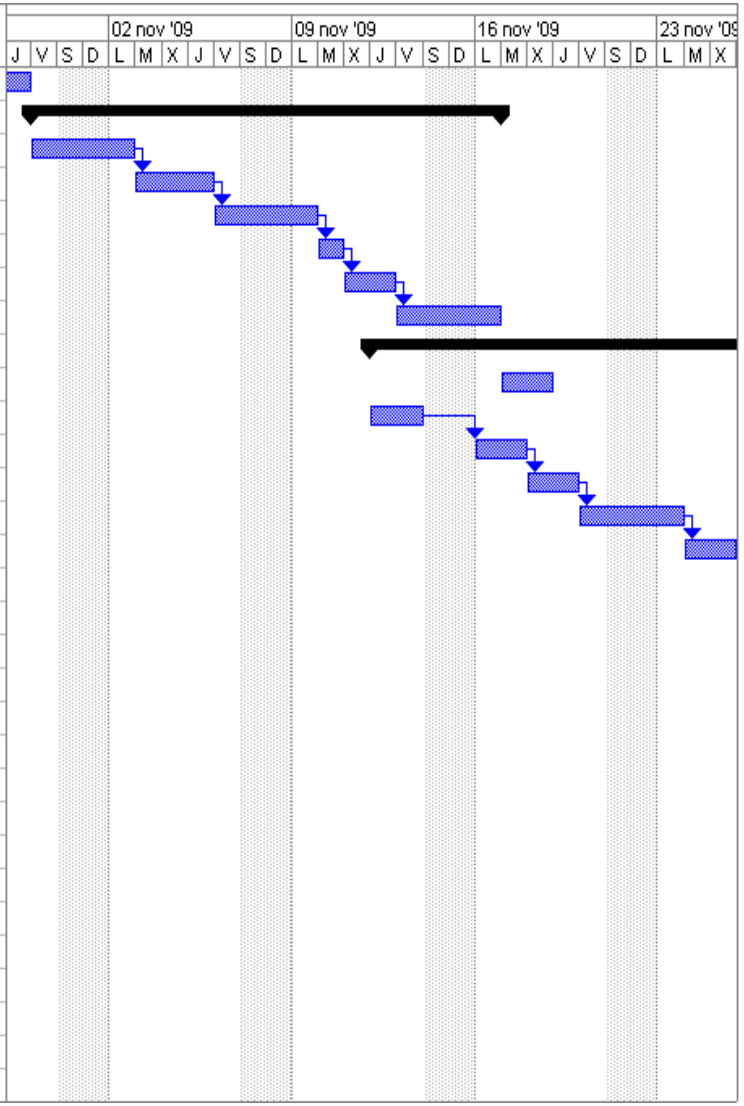
Nombre de tarea	Duración	Comienzo	Fin
Entrevista con el personal encargado del centro de computo del Área de	2 días	jue 24/09/09	vie 25/09/09
Encuesta con el personal a cargo de la red de datos en la U.N.L.,	**15 días**	**lun 28/09/09**	**vie 16/10/09**
Encuesta con el personal a cargo de la red de datos en Administración C	3 días	lun 28/09/09	mié 30/09/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 01/10/09	vie 02/10/09
Encuesta con el personal encargada del centro de cómputo del Área Jur	3 días	lun 05/10/09	mié 07/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 08/10/09	vie 09/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	lun 12/10/09	mié 14/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	mié 14/10/09	vie 16/10/09
Análisis de la tecnología existente (Hardware y Software) en la Unive	**9 días**	**lun 19/10/09**	**jue 29/10/09**
Análisis de la tecnología existente en Administración Central (Jefatura Int	2 días	lun 19/10/09	mar 20/10/09
Análisis de la tecnología en el Área de Educación, Arte y Comunicación	1 día	mié 21/10/09	mié 21/10/09
Análisis de la tecnología en el Área Jurídica Social y Administrativa.	2 días	jue 22/10/09	vie 23/10/09
Análisis de la tecnología en el Área de Salud Humana.	1 día	lun 26/10/09	lun 26/10/09
Análisis de la tecnología en el Área de Agropecuaria y de Recursos Natu	2 días	mar 27/10/09	mié 28/10/09
Análisis de la tecnología en el Área de Energía, Industrias y Recursos Na	2 días	mié 28/10/09	jue 29/10/09
Análisis de los esquemas de red (topología)	**12 días**	**vie 30/10/09**	**lun 16/11/09**
Análisis del esquema de red en Administración Central.	2 días	vie 30/10/09	lun 02/11/09
Análisis del esquema de red en el Área de Educación, Arte y Comunicac	3 días	mar 03/11/09	jue 05/11/09
Análisis del esquema de red en el Área Jurídica Social y Administrativa.	2 días	vie 06/11/09	lun 09/11/09
Análisis del esquema de red en el Área de Salud Humana.	1 día	mar 10/11/09	mar 10/11/09
Análisis del esquema de red en el Área de Agropecuaria y de Recursos	2 días	mié 11/11/09	jue 12/11/09
Análisis del esquema de red en el Área de Energía, Industrias y Recurso	2 días	vie 13/11/09	lun 16/11/09
Análisis de las políticas de seguridad en la Universidad Nacional de l	**10 días**	**jue 12/11/09**	**mié 25/11/09**
Análisis de políticas de seguridad en Administración Central.	2 días	mar 17/11/09	mié 18/11/09
Análisis de políticas de seguridad en el Área de Educación, Arte y Comu	2 días	jue 12/11/09	vie 13/11/09
Análisis de políticas de seguridad en el Área Jurídica Social y Administra	2 días	lun 16/11/09	mar 17/11/09
Análisis de políticas de seguridad en el Área de Salud Humana,	2 días	mié 18/11/09	jue 19/11/09
Análisis de políticas de seguridad en el Área de Agropecuaria y de Recu	2 días	vie 20/11/09	lun 23/11/09
Análisis de políticas de seguridad en el Área de Energía, Industrias y Rec	2 días	mar 24/11/09	mié 25/11/09
SELECCIÓN DE LAS MEJORES ALTERNATIVAS EN BASE A LOS REQUERIMIEN	**49 días?**	**jue 26/11/09**	**mar 02/02/10**
Obtención de Requerimientos de seguridad para redes clableadas e	**6 días?**	**jue 26/11/09**	**jue 03/12/09**



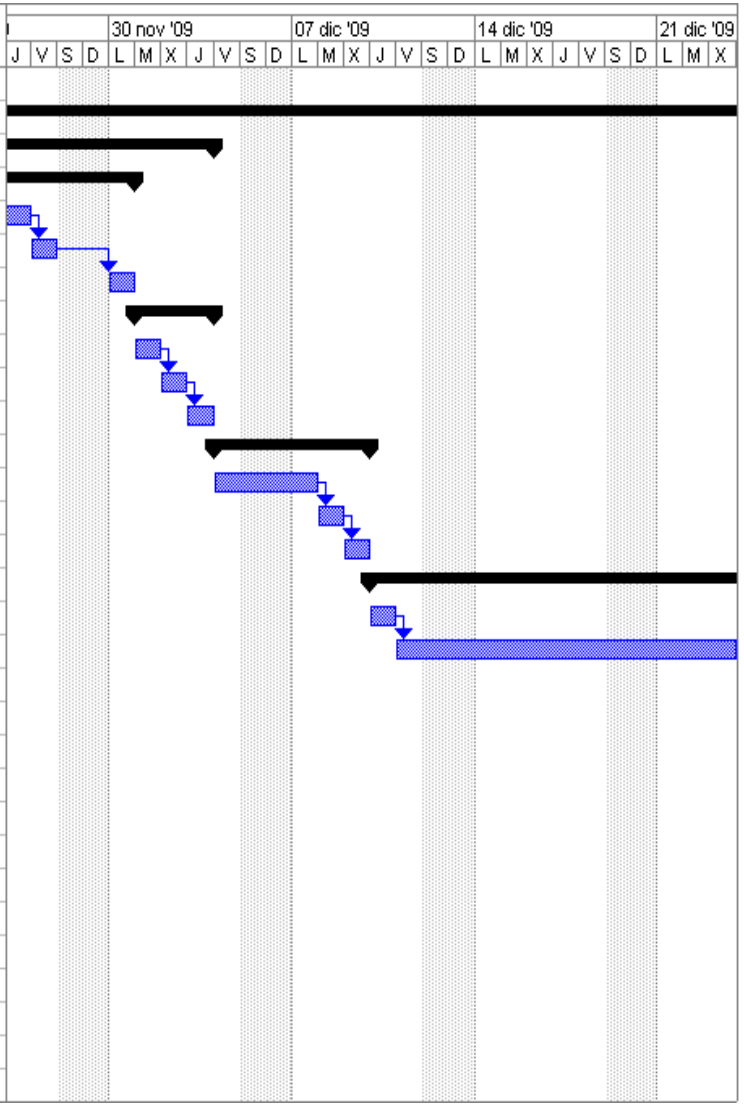
Nombre de tarea	Duración	Comienzo	Fin
Entrevista con el personal encargado del centro de computo del Área de	2 días	jue 24/09/09	vie 25/09/09
Encuesta con el personal a cargo de la red de datos en la U.N.L,	**15 días**	**lun 28/09/09**	**vie 16/10/09**
Encuesta con el personal a cargo de la red de datos en Administración C	3 días	lun 28/09/09	mié 30/09/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 01/10/09	vie 02/10/09
Encuesta con el personal encargada del centro de cómputo del Área Jur	3 días	lun 05/10/09	mié 07/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	2 días	jue 08/10/09	vie 09/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	lun 12/10/09	mié 14/10/09
Encuesta con el personal encargado del centro de cómputo del Área de	3 días	mié 14/10/09	vie 16/10/09
Análisis de la tecnología existente (Hardware y Software) en la Unive	**9 días**	**lun 19/10/09**	**jue 29/10/09**
Análisis de la tecnología existente en Administración Central (Jefatura Int	2 días	lun 19/10/09	mar 20/10/09
Análisis de la tecnología en el Área de Educación, Arte y Comunicación	1 día	mié 21/10/09	mié 21/10/09
Análisis de la tecnología en el Área Jurídica Social y Administrativa.	2 días	jue 22/10/09	vie 23/10/09
Análisis de la tecnología en el Área de Salud Humana.	1 día	lun 26/10/09	lun 26/10/09
Análisis de la tecnología en el Área de Agropecuaria y de Recursos Natu	2 días	mar 27/10/09	mié 28/10/09
Análisis de la tecnología en el Área de Energía, Industrias y Recursos Na	2 días	mié 28/10/09	jue 29/10/09
Análisis de los esquemas de red (topología)	**12 días**	**vie 30/10/09**	**lun 16/11/09**
Análisis del esquema de red en Administración Central.	2 días	vie 30/10/09	lun 02/11/09
Análisis del esquema de red en el Área de Educación, Arte y Comunicac	3 días	mar 03/11/09	jue 05/11/09
Análisis del esquema de red en el Área Jurídica Social y Administrativa.	2 días	vie 06/11/09	lun 09/11/09
Análisis del esquema de red en el Área de Salud Humana.	1 día	mar 10/11/09	mar 10/11/09
Análisis del esquema de red en el Área de Agropecuaria y de Recursos	2 días	mié 11/11/09	jue 12/11/09
Análisis del esquema de red en el Área de Energía, Industrias y Recurso	2 días	vie 13/11/09	lun 16/11/09
Análisis de las políticas de seguridad en la Universidad Nacional de l	**10 días**	**jue 12/11/09**	**mié 25/11/09**
Análisis de políticas de seguridad en Administración Central.	2 días	mar 17/11/09	mié 18/11/09
Análisis de políticas de seguridad en el Área de Educación, Arte y Comu	2 días	jue 12/11/09	vie 13/11/09
Análisis de políticas de seguridad en el Área Jurídica Social y Administra	2 días	lun 16/11/09	mar 17/11/09
Análisis de políticas de seguridad en el Área de Salud Humana,	2 días	mié 18/11/09	jue 19/11/09
Análisis de políticas de seguridad en el Área de Agropecuaria y de Recu	2 días	vie 20/11/09	lun 23/11/09
Análisis de políticas de seguridad en el Área de Energía, Industrias y Rec	2 días	mar 24/11/09	mié 25/11/09
SELECCIÓN DE LAS MEJORES ALTERNATIVAS EN BASE A LOS REQUERIMIEN	**49 días?**	**jue 26/11/09**	**mar 02/02/10**
Obtención de Requerimientos de seguridad para redes clableadas e	**6 días?**	**jue 26/11/09**	**jue 03/12/09**



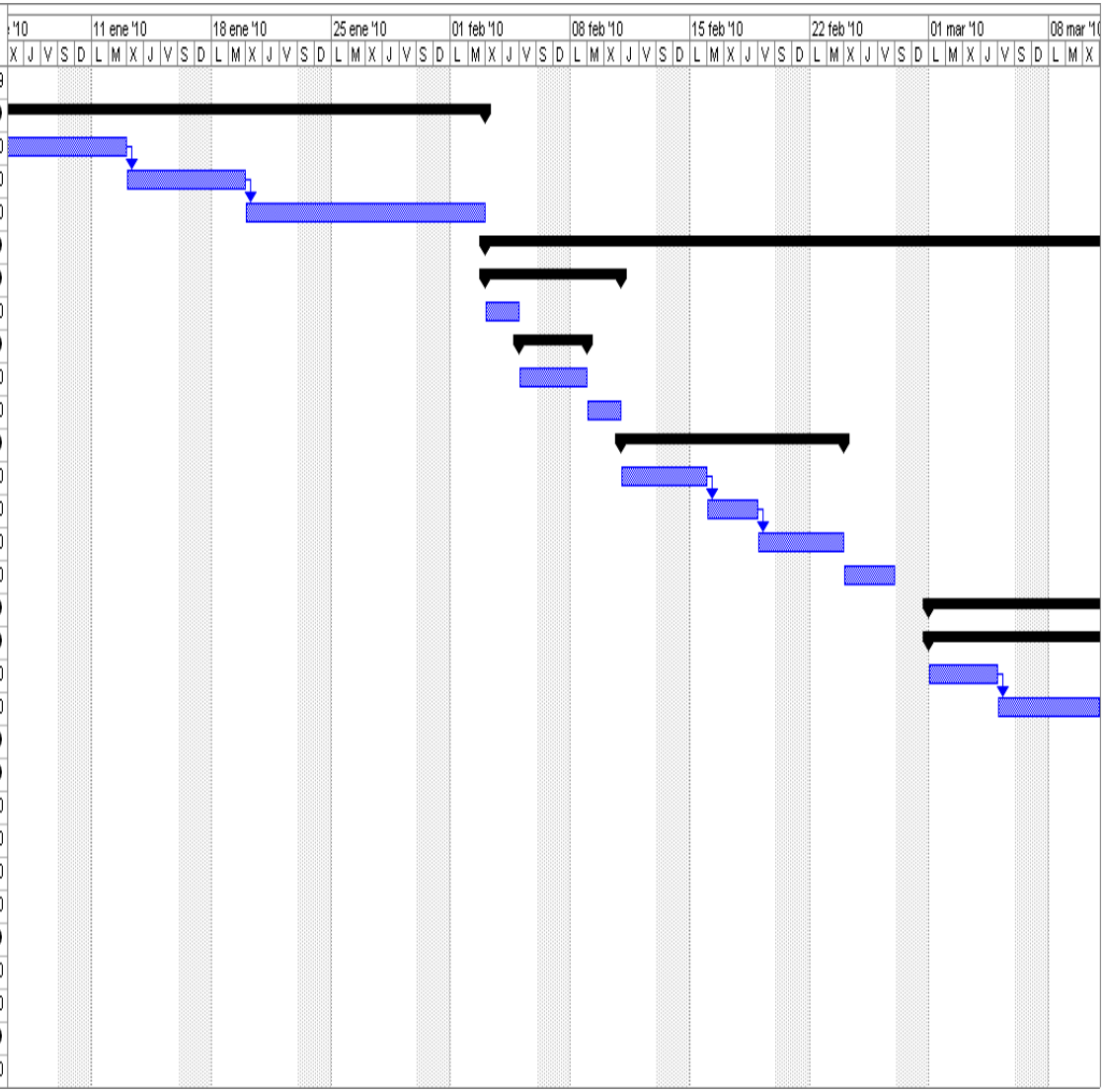
Nombre de tarea	Duración	Comienzo	Fin
Análisis de la tecnología en el Área de Energía, Industrias y Recursos Na	2 días	mié 28/10/09	jue 29/10/09
Análisis de los esquemas de red (topología)	**12 días**	**vie 30/10/09**	**lun 16/11/09**
Análisis del esquema de red en Administración Central.	2 días	vie 30/10/09	lun 02/11/09
Análisis del esquema de red en el Área de Educación, Arte y Comunicac	3 días	mar 03/11/09	jue 05/11/09
Análisis del esquema de red en el Área Jurídica Social y Administrativa.	2 días	vie 06/11/09	lun 09/11/09
Análisis del esquema de red en el Área de Salud Humana.	1 día	mar 10/11/09	mar 10/11/09
Análisis del esquema de red en el Área de Agropecuaria y de Recursos	2 días	mié 11/11/09	jue 12/11/09
Análisis del esquema de red en el Área de Energía, Industrias y Recurso	2 días	vie 13/11/09	lun 16/11/09
Análisis de las políticas de seguridad en la Universidad Nacional de l	**10 días**	**jue 12/11/09**	**mié 25/11/09**
Análisis de políticas de seguridad en Administración Central.	2 días	mar 17/11/09	mié 18/11/09
Análisis de políticas de seguridad en el Área de Educación, Arte y Comu	2 días	jue 12/11/09	vie 13/11/09
Análisis de políticas de seguridad en el Área Jurídica Social y Administra	2 días	lun 16/11/09	mar 17/11/09
Análisis de políticas de seguridad en el Área de Salud Humana,	2 días	mié 18/11/09	jue 19/11/09
Análisis de políticas de seguridad en el Área de Agropecuaria y de Recu	2 días	vie 20/11/09	lun 23/11/09
Análisis de políticas de seguridad en el Área de Energía, Industrias y Rec	2 días	mar 24/11/09	mié 25/11/09
SELECCIÓN DE LAS MEJORES ALTERNATIVAS EN BASE A LOS REQUERIMIEN	**49 días?**	**jue 26/11/09**	**mar 02/02/10**
Obtención de Requerimientos de seguridad para redes clableadas e	**6 días?**	**jue 26/11/09**	**jue 03/12/09**
Inalámbricas	**3 días?**	**jue 26/11/09**	**lun 30/11/09**
Virtual Private Network (VPN).	1 día	jue 26/11/09	jue 26/11/09
Proxy-Web	1 día	vie 27/11/09	vie 27/11/09
IEEE 802.11i	1 día?	lun 30/11/09	lun 30/11/09
Clableadas	**3 días?**	**mar 01/12/09**	**jue 03/12/09**
Criptografía.	1 día?	mar 01/12/09	mar 01/12/09
Firewall	1 día?	mié 02/12/09	mié 02/12/09
IEEE 802.1	1 día?	jue 03/12/09	jue 03/12/09
Obtención de requerimientos funcionales.	**4 días**	**vie 04/12/09**	**mié 09/12/09**
Brindar el acceso a algunos servicios para estudiantes, profesores y ad	2 días	vie 04/12/09	lun 07/12/09
Ofrecer servicios de acceso a la red pública (Internet).	1 día	mar 08/12/09	mar 08/12/09
Permitir la movilidad de los usuarios a través de las diferentes áreas de s	1 día	mié 09/12/09	mié 09/12/09
Desarrollo de la alternativa de solución en el Área de Energía, Indust	**10 días**	**jue 10/12/09**	**mié 23/12/09**
Ubicación del servidor RADIUS en el Área de Energía, Industrias y Recur	1 día	jue 10/12/09	jue 10/12/09



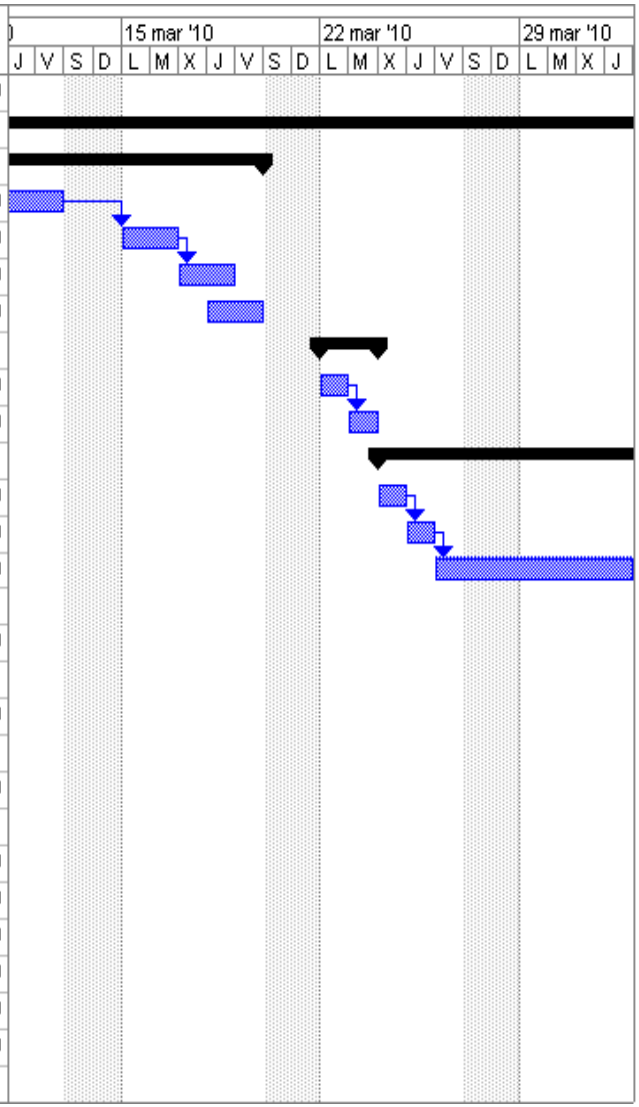
Nombre de tarea	Duración	Comienzo	Fin
Análisis de políticas de seguridad en el Área de Energía, Industrias y Rec	2 días	mar 24/11/09	mié 25/11/09
SELECCIÓN DE LAS MEJORES ALTERNATIVAS EN BASE A LOS REQUERIMIEN	**49 días?**	**jue 26/11/09**	**mar 02/02/10**
Obtención de Requerimientos de seguridad para redes clableadas e	**6 días?**	**jue 26/11/09**	**jue 03/12/09**
Inalámbricas	**3 días?**	**jue 26/11/09**	**lun 30/11/09**
Virtual Private Network (VPN).	1 día	jue 26/11/09	jue 26/11/09
Proxy-Web	1 día	vie 27/11/09	vie 27/11/09
IEEE 802.11i	1 día?	lun 30/11/09	lun 30/11/09
Clableadas	**3 días?**	**mar 01/12/09**	**jue 03/12/09**
Criptografía.	1 día?	mar 01/12/09	mar 01/12/09
Firewall	1 día?	mié 02/12/09	mié 02/12/09
IEEE 802.1	1 día?	jue 03/12/09	jue 03/12/09
Obtención de requerimientos funcionales.	**4 días**	**vie 04/12/09**	**mié 09/12/09**
Brindar el acceso a algunos servicios para estudiantes, profesores y ad	2 días	vie 04/12/09	lun 07/12/09
Ofrecer servicios de acceso a la red pública (Internet).	1 día	mar 08/12/09	mar 08/12/09
Permitir la movilidad de los usuarios a través de las diferentes áreas de s	1 día	mié 09/12/09	mié 09/12/09
Desarrollo de la alternativa de solución en el Área de Energía, Indust	**10 días**	**jue 10/12/09**	**mié 23/12/09**
Ubicación del servidor RADIUS en el Área de Energía, Industrias y Recur	1 día	jue 10/12/09	jue 10/12/09
Configuración del Servidor.	9 días	vie 11/12/09	mié 23/12/09
Optimización de los equipos existentes en el Área de Energía, Indu	**20 días**	**mié 06/01/10**	**mar 02/02/10**
Comprobar si los equipos son óptimos o permitan realizar la implementac	5 días	mié 06/01/10	mar 12/01/10
Configuración de loa Access Point	5 días	mié 13/01/10	mar 19/01/10
Configuración de los Switch.	10 días	mié 20/01/10	mar 02/02/10
VALIDACION DEL ESQUEMA DE SEGURIDAD	**26 días**	**mié 03/02/10**	**mié 10/03/10**
Selección De La Mejor Alternativa De Seguridad Para Redes Cablead	**6 días**	**mié 03/02/10**	**mié 10/02/10**
Selección del mecanismo de seguridad	2 días	mié 03/02/10	jue 04/02/10
Análisis del estándar IEEE 802.1x para redes cableadas	**2 días**	**vie 05/02/10**	**lun 08/02/10**
Protocolo EAP-EAPOL	2 días	vie 05/02/10	lun 08/02/10
Análisis de Autenticación basada en 802.1x para redes WIFI	2 días	mar 09/02/10	mié 10/02/10
Requerimientos técnicos de la solución	**9 días**	**jue 11/02/10**	**mar 23/02/10**
En los usuarios	3 días	jue 11/02/10	lun 15/02/10
En los Acces Point y Switchs	3 días	mar 16/02/10	jue 18/02/10



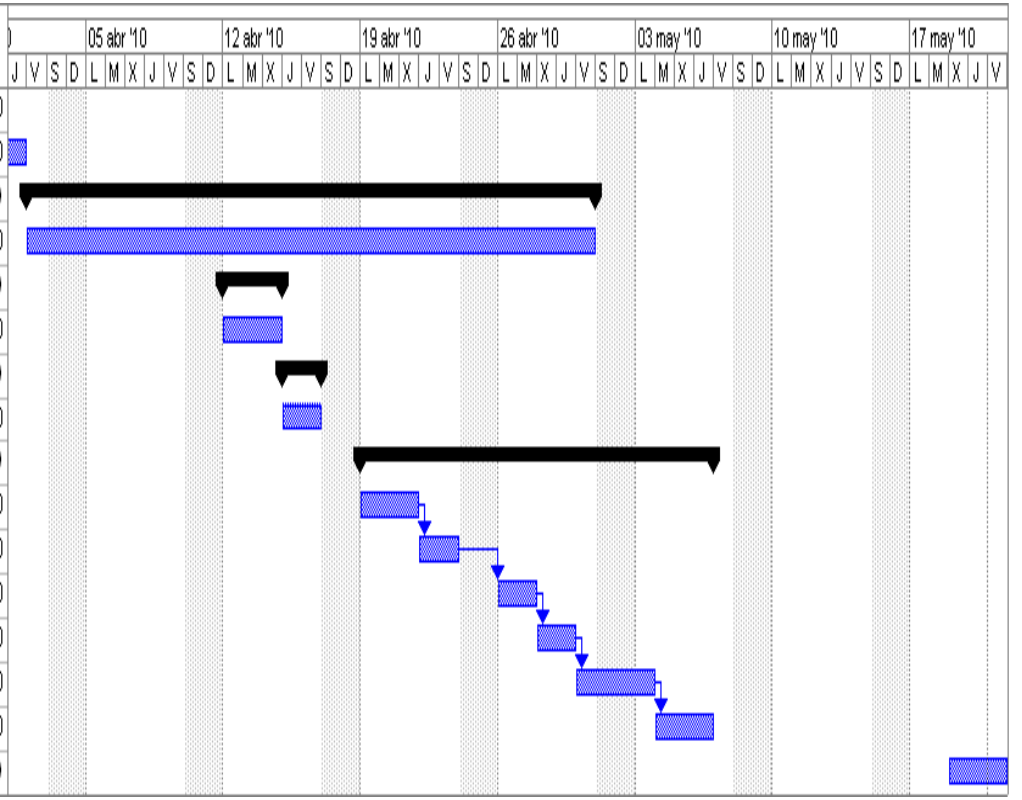
Nombre de tarea	Duración	Comienzo	Fin
Configuración del Servidor.	9 días	vie 11/12/09	mié 23/12/09
Optimización de los equipos existentes en el Área de Energía, Indu	**20 días**	**mié 06/01/10**	**mar 02/02/10**
Comprobar si los equipos son óptimos o permitan realizar la implementac	5 días	mié 06/01/10	mar 12/01/10
Configuración de loa Access Point	5 días	mié 13/01/10	mar 19/01/10
Configuración de los Switch.	10 días	mié 20/01/10	mar 02/02/10
VALIDACION DEL ESQUEMA DE SEGURIDAD	**26 días**	**mié 03/02/10**	**mié 10/03/10**
Selección De La Mejor Alternativa De Seguridad Para Redes Cablead	**6 días**	**mié 03/02/10**	**mié 10/02/10**
Selección del mecanismo de seguridad	2 días	mié 03/02/10	jue 04/02/10
Análisis del estándar IEEE 802.1x para redes cableadas	**2 días**	**vie 05/02/10**	**lun 08/02/10**
Protocolo EAP-EAPOL	2 días	vie 05/02/10	lun 08/02/10
Análisis de Autenticación basada en 802.1x para redes WIFI	2 días	mar 09/02/10	mié 10/02/10
Requerimientos técnicos de la solución	**9 días**	**jue 11/02/10**	**mar 23/02/10**
En los usuarios	3 días	jue 11/02/10	lun 15/02/10
En los Acces Point y Switchs	3 días	mar 16/02/10	jue 18/02/10
En el servidor de autenticación	3 días	vie 19/02/10	mar 23/02/10
Selección del Servidor	3 días	mié 24/02/10	vie 26/02/10
Autenticaciones	**8 días**	**lun 01/03/10**	**mié 10/03/10**
Selección del mecanismo de autenticación	**8 días**	**lun 01/03/10**	**mié 10/03/10**
Validación por dirección física del dispositivo de red (MAC)	4 días	lun 01/03/10	jue 04/03/10
Validación por usuario – contraseña	4 días	vie 05/03/10	mié 10/03/10
IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PLANTEADO EN EL AREA D	**37 días?**	**jue 11/03/10**	**vie 30/04/10**
Instalación del servidor	**7 días?**	**jue 11/03/10**	**vie 19/03/10**
Implementación del servidor FREERADIUS	2 días	jue 11/03/10	vie 12/03/10
Implementación del servidor OPENLDAP	2 días	lun 15/03/10	mar 16/03/10
Implementación del servidor MYSQL	2 días	mié 17/03/10	jue 18/03/10
Implementación del servidor de gestión WEB	2 días?	jue 18/03/10	vie 19/03/10
Instalación de OPENSSL y generación de certificados	**2 días?**	**lun 22/03/10**	**mar 23/03/10**
Generación de Certificados	1 día?	lun 22/03/10	lun 22/03/10
Scripts Generación de Certificados	1 día?	mar 23/03/10	mar 23/03/10
Configuración de OpenLDAP como base de datos de usuario	**7 días?**	**mié 24/03/10**	**jue 01/04/10**
Configuración de LDAP	1 día?	mié 24/03/10	mié 24/03/10



Nombre de tarea	Duración	Comienzo	Fin
Validación por usuario – contraseña	4 días	vie 05/03/10	mié 10/03/10
IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PLANTEADO EN EL AREA D	**37 días?**	**jue 11/03/10**	**vie 30/04/10**
Instalación del servidor	**7 días?**	**jue 11/03/10**	**vie 19/03/10**
Implementación del servidor FREERADIUS	2 días	jue 11/03/10	vie 12/03/10
Implementación del servidor OPENLDAP	2 días	lun 15/03/10	mar 16/03/10
Implementación del servidor MYSQL	2 días	mié 17/03/10	jue 18/03/10
Implementación del servidor de gestión WEB	2 días?	jue 18/03/10	vie 19/03/10
Instalación de OPENSSL y generación de certificados	**2 días?**	**lun 22/03/10**	**mar 23/03/10**
Generación de Certificados	1 día?	lun 22/03/10	lun 22/03/10
Scripts Generación de Certificados	1 día?	mar 23/03/10	mar 23/03/10
Configuración de OpenLDAP como base de datos de usuario	**7 días?**	**mié 24/03/10**	**jue 01/04/10**
Configuración de LDAP	1 día?	mié 24/03/10	mié 24/03/10
Construcción del Árbol Ldap	1 día?	jue 25/03/10	jue 25/03/10
Ingreso de datos en la base de datos LDAP	5 días	vie 26/03/10	jue 01/04/10
Instalación de MYSQL	**21 días**	**vie 02/04/10**	**vie 30/04/10**
Ingreso de datos en la base de datos MYSQL	21 días	vie 02/04/10	vie 30/04/10
Instalación de FRERADIUS como servidor AAA	**3 días**	**lun 12/04/10**	**mié 14/04/10**
Configuración	3 días	lun 12/04/10	mié 14/04/10
Configuración de los Acces Point d-link 3200ap con protocolo 802.1x	**2 días**	**jue 15/04/10**	**vie 16/04/10**
Menú de Configuración	2 días	jue 15/04/10	vie 16/04/10
MANUAL DE POLITICAS DE SEGURIDAD DE REDES	**14 días**	**lun 19/04/10**	**jue 06/05/10**
Riesgos de las Redes Inalámbricas	3 días	lun 19/04/10	mié 21/04/10
Uso del manual	2 días	jue 22/04/10	vie 23/04/10
Mecanismos de seguridad	2 días	lun 26/04/10	mar 27/04/10
Contraseñas seguras	2 días	mié 28/04/10	jue 29/04/10
Establecimiento de políticas de seguridad a ser implementadas	2 días	vie 30/04/10	lun 03/05/10
Políticas de seguridad a ser implementadas	3 días	mar 04/05/10	jue 06/05/10
Pruebas	**3 días**	**mié 19/05/10**	**vie 21/05/10**



Nombre de tarea	Duración	Comienzo	Fin
Construcción del Árbol Ldap	1 día?	jue 25/03/10	jue 25/03/10
Ingreso de datos en la base de datos LDAP	5 días	vie 26/03/10	jue 01/04/10
Instalación de MYSQL	**21 días**	**vie 02/04/10**	**vie 30/04/10**
Ingreso de datos en la base de datos MYSQL	21 días	vie 02/04/10	vie 30/04/10
Instalación de FRERADIUS como servidor AAA	**3 días**	**lun 12/04/10**	**mié 14/04/10**
Configuración	3 días	lun 12/04/10	mié 14/04/10
Configuración de los Acces Point d-link 3200ap con protocolo 802.1x	**2 días**	**jue 15/04/10**	**vie 16/04/10**
Menú de Configuración	2 días	jue 15/04/10	vie 16/04/10
MANUAL DE POLITICAS DE SEGURIDAD DE REDES	**14 días**	**lun 19/04/10**	**jue 06/05/10**
Riesgos de las Redes Inalámbricas	3 días	lun 19/04/10	mié 21/04/10
Uso del manual	2 días	jue 22/04/10	vie 23/04/10
Mecanismos de seguridad	2 días	lun 26/04/10	mar 27/04/10
Contraseñas seguras	2 días	mié 28/04/10	jue 29/04/10
Establecimiento de políticas de seguridad a ser implementadas	2 días	vie 30/04/10	lun 03/05/10
Políticas de seguridad a ser implementadas	3 días	mar 04/05/10	jue 06/05/10
Pruebas	**3 días**	**mié 19/05/10**	**vie 21/05/10**



8. PRESUPUESTO Y FINANCIAMIENTO

DESCRIPCIÓN	CANTIDAD	# HORAS	V/U	V/T
Recursos Humanos				
Investigadores	2	440	2.50	2200.00
Profesionales del campo de Redes (Jefatura Informática UNL)	2		0.00	0.00
Directora del Proyecto – Docente de la Carrera de Ingeniería en Sistemas	1		0.00	0.00
Recursos Técnicos				
Hardware				
Procesador Pentium III 1001.780Mhz Disco Duro 40 GB Memoria 256 MB	1		1000.00	1000.00
Memory Flash 1GB	2		30.00	60.00
Wrt-Radauth WRT54GLA	1		---	---
Access Point D-Link Dwl-g700 Ap.	4		---	---
Software				
Software Libre para la configuración del servidor de seguridad. (RADIUS)			0.00	0.00
Software Libre para la			0.00	0.00

configuración del servicio de Autenticación.				
Sistema Operativo del Servidor de seguridad (Linux – Estrella Roja 2.0.2)			0.00	0.00
Office 2007			0.00	0.00
Recursos materiales				
Resmas 500 hojas de papel 75 g/m2 tamaño A4	2		3.20	6.40
Cartuchos de tinta para impresora.	3		2.50	7.00
Caja de CD's	1		10.00	10.00
Recursos Tecnológicos				
Internet.		112	0.8	89.60
Varios			315.00	315.00
COSTO REAL DEL PROYECTO				**3688.00**

9. BIBLIOGRAFIA

SITIOS WEB:

- GREEN, W.B. 1993 Protocolo AAA en redes inalmbricas [//74.125.77.132/search?q=cache:7493CxM-n5UJ:www.imaginar.org/digitalizacion/manuales/manual_digitalizacion.pdf+digitalizacion+de+documentos&hl=es&ct=clnk&cd=3&gl=ec&client=firefox-a]Sevilla [Consulta: 06 Febrero 2009]
- LABORERO, Diego, 2008 S [cxo-community.com.ar/index.php?option=com_content&task=view&id=1281&Itemid=1&utm_source=emBlue_Boletin$16&utm_medium=Oferta:617407]Sevilla [Consulta: 07 Febrero 2009]
- SAVOLAINEN, Martti, 2004 Métodos de Encriptación [en.wikipedia.org/wiki/Wireless_security] Colombia [Consulta 16 de Enero 2009]
- LLULL, Eduard. 2001 IEEE – Seguridad en LAN [es.wikipedia.org/wiki/IEEE_802.11.html] Argentina [Consulta 15 Enero 2009]
- SANTOS, Sergio. Seguridad – Firma digital [en línea] [es.wikipedia.org/wiki/Wi-Fi.html] España [Consulta 15 Enero 2009]
- OCHOA, Beatriz 1996 Procesos de Autenticación y Autorización [monografias.com/trabajos11/metods.html]Colombia [Consulta: 06 Febrero 2009]
- MACKAY, Patrick, 2004 seguridad SSL[msmvps.com/blogs/pmackay/archive/2004/11/27/easim1.aspx] Argentina[Consulta: 04 Febrero 2009]
- NAVARRO, X, 2000 ¿Seguridad en una intranet? [poliedric.com/docs/certdigital.php]Barcelona [Consulta: 04 Febrero 2009]
- FARIAS, Mariela , 2003 seguridad en redes [en linea] Argentina [seguridadwireless.net/] [Consulta 16 Enero 2009]

ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA ESPECÍFICA

OBJETIVO ESPECÍFICO 1: "Evaluar la situación actual de la red: aplicabilidad y uso, tecnología, topología, esquema de seguridad".			
PROBLEMA ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**HIPOTESIS**	**SISTEMA CATEGORIAL**
Determinar que desventajas posee la situación actual con respecto a la seguridad en redes inalámbricas.	Realizar un análisis de la tecnología existente, esquemas de seguridad, el cual permita comprender la situación actual que posee la red de datos de la Universidad Nacional de Loja al implementar el esquema de seguridad a las redes Alámbricas e inalámbricas.	Las falencias del sistema actual de la Universidad han provocado que se desaprovechen los recursos de red de datos.	**R**ealidad Actual de la red de datos de la Universidad Nacional de Loja.

OBJETIVO ESPECÍFICO 2: "Analizar los mecanismos de seguridad que incorporen sistemas de Autenticación, Autorización, Administración (AAA) para redes de datos que puedan ser implementados en la Universidad Nacional de Loja."			
PROBLEMA ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**HIPOTESIS**	**SISTEMA CATEGORIAL**
No contar con un esquema de seguridad que salvaguarde los datos de la intranet de la Universidad Nacional de Loja lo que permite la exposición a diferentes ataques desde el exterior como interiormente.	Documentar las especificaciones técnicas de cada uno de los protocolos existentes para seguridad en redes de datos, lo cual permitirá a los directivos de la Universidad, tener una visión más clara de la factibilidad del cambio de tecnología.	No existe un conocimiento claro de los protocolos que se requiere para la implementación del esquema de seguridad en redes de datos, así como también, se desconoce las ventajas de cada uno de ellos	Redes. Seguridad en redes de datos. Seguridades físicas.

OBJETIVO ESPECÍFICO 3: "Seleccionar la mejor alternativa en cuanto a mecanismos de seguridad, en base a los requerimientos y prestaciones del Área de energía Las Industrias y Recursos Naturales No Renovables"			
PROBLEMA ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**HIPOTESIS**	**SISTEMA CATEGORIAL**
No Contar con requerimientos del Área de Energía las Industrias y Recursos Naturales no Renovables que permita determinar cuales son sus puntos débiles en cuanto a seguridad.	Mediante un análisis técnico se podrá implementar adecuadamente seguridad en redes haciendo uso de la herramienta Open Source.	No se conoce las estrategias de implementación de seguridad en la red de datos del Área de Energía las Industrias y Recursos Naturales no Renovables.	RADIUS Autenticación. Autorización.

OBJETIVO ESPECÍFICO 4: "Generar el manual de políticas de seguridad."			
PROBLEMA ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**HIPOTESIS**	**SISTEMA CATEGORIAL**
La Universidad Nacional de Loja en su actualidad no posee un manual de políticas de seguridad en la que permita manejar con certeza el uso de los recursos.	Desarrollar un manual de políticas en base a los requerimientos de la Universidad y de sus usuarios.	No existe un documento en el que contenga políticas de seguridad en redes de datos.	Políticas de Seguridad.

OBJETIVO ESPECÍFICO 5: "Implementar el esquema de seguridad planteado en el Área de Energía las Industrias y Recursos Naturales no Renovables como plan piloto."			
PROBLEMA ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**HIPOTESIS**	**SISTEMA CATEGORIAL**
No contar con la colaboración de las personas encargadas en los centros de computo,	Motivar a los directivos del Área de Energía, las Industrias y Recursos Naturales No Renovables las ventajas que consisten en la implementación.	No existe la disposición del personal administrativo para la ejecución del mismo.	Hardware y software para la implementación del esquema de seguridad en el Área de Energía, las Industrias y Recursos Naturales No Renovables.

OBJETIVO ESPECÍFICO 5: "Evaluar el esquema de seguridad a implementar."			
PROBLEMA ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**HIPOTESIS**	**SISTEMA CATEGORIAL**
No contar con los medios o el equipamiento necesario para poder implementar el esquema de seguridad, lo que atrasaría la implementación del mismo.	Prestar los medios necesarios para realizar una correcta evaluación.	No contar con medios para realizar pruebas la que determinen la eficiencia del mismo.	Hardware y software para la implementación del esquema de seguridad en el Área de Energía, las Industrias y Recursos Naturales No Renovables.

ANEXO 2: MATRIZ DE OPERATIVIDAD DE OBJETIVOS

OBJETIVO ESPECIFICO 1: EVALUAR LA SITUACIÓN ACTUAL DE LA RED: APLICABILIDAD Y USO, TECNOLOGÍA, EQUIPAMIENTO, TOPOLOGÍA.						
ACTIVIDAD O TAREA	**METODOLOGIA**	**FECHA**		**RESPONSABLES**	**PRESUPUESTO**	**RESULTADOS ESPERADOS**
		INICIO	**FINAL**			
Análisis de la tecnología existente (Hardware, Software)	Recolectar datos para interpretarlos de una manera racional	01/04/09	16/04/09	Stalin Aguilar Janneth Moncayo	$ 10.00	Presentar un Documento acerca de los equipos que existen en la Universidad.
Análisis de los esquemas de red (alámbrica, e, inalámbrica)	Recolectar datos para interpretarlos de una manera racional	17/04/09	04/05/09	Stalin Aguilar Janneth Moncayo	$ 10.00	Presentar esquemas de red que existen dentro de la Universidad.
Análisis de los esquemas de seguridad existentes	Recolectar datos para interpretarlos de una manera racional	05/05/09	25/05/09	Stalin Aguilar Janneth Moncayo	$ 10.00	Indicar a través de un documento como están desarrollados los

						esquemas de seguridad de la Universidad
Definir las falencias del sistema actual y sus proyecciones de uso y crecimiento.	Recolectar datos para interpretarlos de una manera racional	26/05/09	10/06/09	Stalin Aguilar Janneth Moncayo	$ 30.00	Documentar un informe de las falencias detectadas que se encuentren dentro de la red de la Universidad
Investigar como se encuentra distribuida la red de datos de la Universidad Nacional de Loja.	Recolectar datos para interpretarlos de una manera racional	11/06/09	17/06/09	Stalin Aguilar Janneth Moncayo	$ 30.00	Detallar por medio de un informe como está distribuida la red de datos de la Universidad Nacional de Loja
Entrevistas con personas relacionadas al campo de Redes.	Buscar la ayuda de personal capacitado, para poder tener una entrevista personal	18/06/09	24/06/09	Stalin Aguilar Janneth Moncayo	$ 60.00	presentación de un documento de las experiencias de redes alámbricas e inalámbricas en la personas entrevistadas a través de modelos de encuestas o cuestionarios..

OBJETIVO ESPECIFICO 2: ANALIZAR LOS MECANISMOS DE SEGURIDAD QUE INCORPOREN SISTEMAS DE AUTENTICACIÓN, AUTORIZACIÓN Y ADMINISTRACIÓN (AAA) PARA REDES DE DATOS QUE PUEDAN SER IMPLEMENTADOS EN LA UNIVERSIDAD NACIONAL DE LOJA

ACTIVIDAD O TAREA	METODOLOGIA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Investigación sobre software que contengan sistemas AAA	Visitar sitios web que posean información verídica sobre software para seguridad en redes.	25/06/09	29/06/09	Janneth Moncayo Stalin Aguilar	$ 8.00	Documentar los diversos software que existen para la implementación de seguridad en redes Escoger la mejor alternativa en base a los diversos software

						que existen.
Investigación sobre FREERADIUS	Visitar sitios web que posean información verídica sobre FREERADIUS	30/06/09	02/07/09	Janneth Moncayo Stalin Aguilar	$ 8.00	Obtener una documentación sobre RADIUS
Investigación acerca de la Arquitectura de FREERADIUS.	Visitar sitios web que posean información sobre arquitectura de RADIUS	03/07/09	08/07/09	Janneth Moncayo Stalin Aguilar	$ 8.00	Entender y documentar la arquitectura RADIUS
Obtener el software requerido para instalar FREERADIUS,	Visitar sitios web que posean información verídica sobre RADIUS	09/07/09	13/07/09	Janneth Moncayo Stalin Aguilar	$ 16.00	Instalar RADIUS en el servidor de seguridad.
Investigación sobre configuración de archivos de FREERADIUS	Seguir el procedimiento que indican el manual de instalación.	14/07/09	15/07/09	Janneth Moncayo Stalin Aguilar	$ 20.0	Servidor RADIUS instalados dentro de Intranet del AEIRNNR

OBJETIVO ESPECIFICO 3: SELECCIONAR LA MEJOR ALTERNATIVA EN CUANTO A MECANISMOS DE SEGURIDAD, EN BASE A LOS REQUERIMIENTOS Y PRESTACIONES DEL AREA DE ENERGIA LAS INDUSTRIA Y RECURSOS NATURALES NO RENOVABLES.

ACTIVIDAD O TAREA	METODOLOGIA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Obtener requerimientos funcionales y requerimientos de seguridad.	Buscar la ayuda del personal capacitado, para poder tener una idea clara del esquema.	03/08/09	07/08/09	Janneth Moncayo Stalin Aguilar	$ 75.00	Saber de experiencias de seguridad en redes en nuestra ciudad.
Análisis de los requerimientos obtenidos	Lectura comprensiva, cuadros sinópticos, mapas conceptúales	10/08/09	13/08/09	Janneth Moncayo Stalin Aguilar	$ 10.00	Armar un marco teórico que sea la base para el desarrollo de la investigación,

						para tener claro el funcionamiento del esquema a implantar en el AEIRNNR.
Ordenar los requerimientos según la prioridad establecida.	Lectura comprensiva, cuadros sinópticos.	14/08/09	17/08/09	Janneth Moncayo Stalin Aguilar	$ 8.00	Conocer la estructura de los requerimientos, los mismos que determinaran la funcionalidad del mismo.

OBJETIVO ESPECÍFICO 4: GENERAR EL MANUAL DE POLITICAS DE SEGURIDAD.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSA-BLES	PRESU-PUESTO $	RESULTADOS ESPERADOS
		INICIO	FINAL			
Construir un documento que resuma las políticas que se implementen en el esquema de seguridad.	Crear un documento que resuma las políticas que van a ser aplicadas en el proyecto.	16/07/09	17/07/09	Janneth Moncayo Stalin Aguilar	$ 8.00	Obtener un documento en que se detalle las políticas necesarias a implementar.
Establecer políticas de seguridad necesarias para acceder a cada recurso.	De acuerdo a las necesidades de la Universidad establecer las políticas.	20/07/09	30/07/09	Janneth Moncayo Stalin Aguilar	$ 8.00	Determinar las políticas a seguir en el proyecto.

OBJETIVO ESPECIFICO 5: IMPLEMENTAR DEL ESQUEMA DE SEGURIDAD PLANTEADO, EN EL ÁREA DE ENERGÍA LAS INDUSTRIAS Y RECURSOS NATURALES NO RENOVABLES COMO PLAN PILOTO.

ACTIVIDAD O TAREA	METODOLOGIA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Optimizar la utilización de la tecnología existente.	Visitar el área de la energía, industrias y recursos naturales no renovables para poder determinar el tipo de Hardware que ésta posee.	02/09/09	10/09/09	Stalin Aguilar Janneth Moncayo	$ 10.00	Utilizar de manera eficiente todos los equipos que se encuentren en el área de la energía las industrias y los recursos naturales no renovables
Investigar sobre la configuración de archivos en 3Com.	Visitar sitios web que posean información verídica sobre la configuración de archivos en 3Com	11/09/09	17/09/09	Stalin Aguilar Janneth Moncayo	$ 10.00	Encontrar Documentación sobre la configuración de archivos en 3Com
Configurar los swicht capa 2	Seguir el procedimiento que	18/09/09	01/10/09	Stalin Aguilar	$ 10.00	Swicht capa 2

administrables (3Com).	indican los manuales de configuración de los swicht capa 2 administrables			Janneth Moncayo		administrables configurados dentro del Área de la Energía, Industrias y Recursos Naturales no Renovables
Implantar el esquema de seguridad.	Emplear la información recogida de internet acerca de los esquemas de seguridad	05/10/09	09/10/09	Stalin Aguilar Janneth Moncayo	$ 30.00	Esquema de seguridad funciona y se ejecuta en el servidor
Validar su correcto funcionamiento.	Realizar diversas pruebas entre los usuarios que tengan acceso al servicio	12/10/09	13/10/09	Stalin Aguilar Janneth Moncayo	$ 30.00	Obtener el criterio de los usuarios que tengan acceso al servicio

OBJETIVO ESPECÍFICO 6: EVALUAR EL ESQUEMA DE SEGURIDAD A IMPLEMENTAR.						
ACTIVIDAD O TAREA	**METODOLOGÍA**	**FECHA**		**RESPONSABLES**	**PRESUPUESTO $**	**RESULTADOS ESPERADOS**
		INICIO	FINAL			
Análisis de las ventajas y desventajas que trae la implantación de seguridad en redes de datos.	Determinar las ventajas que produce implantando el esquema de seguridad.	24-09-07	26-09-07	Janneth Moncayo Stalin Aguilar	$ 10.00	Verificar las ventajas que se ajustan al sistema de seguridad de la intranet de la Universidad.

ANEXO 3: MATRIZ DE CONTROL DE RESULTADOS

NUMERO	RESULTADOS	FECHA	FIRMA DIRECTOR DE TESIS
1	Presentar un Documento acerca de los equipos que existen en la Universidad.	16/04/09	
2	Presentar esquemas de red que existen dentro de la Universidad.	04/05/09	
3	Indicar a través de un documento como están desarrollados los esquemas de seguridad de la Universidad	25/05/09	
4	Documentar un informe de las falencias detectadas que se encuentren dentro de la red de la Universidad	10/06/09	

5	Detallar por medio de un informe como está distribuida la red de datos de la Universidad Nacional de Loja	17/06/09	
6	Presentación de un documento de las experiencias de redes alámbricas e inalámbricas en la personas entrevistadas a través de modelos de encuestas o cuestionarios..	24/06/09	
7	Documentar los diversos software que existen para la implementación de seguridad en redes	29/06/09	
8	Escoger la mejor alternativa en base a los diversos software que existen.	29/06/09	
9	Obtener una documentación sobre RADIUS	02/07/09	

10	Entender y documentar la arquitectura RADIUS	08/07/09	
11	Instalar RADIUS en el servidor de seguridad.	13/07/09	
12	Servidor RADIUS instalados dentro de Intranet del AEIRNNR	15/07/09	
13	Obtener un documento en que se detalle las políticas necesarias a implementar.	17/07/09	

14	Determinar las políticas a seguir en el proyecto	30/07/09	
15	Saber de experiencias de seguridad en redes en nuestra ciudad.	07/08/09	
16	Armar un marco teórico que sea la base para el desarrollo de la investigación, para tener claro el funcionamiento del esquema a implantar en el AEIRNNR.	13/08/09	
17	Conocer la estructura de los requerimientos, los mismos que determinaran la funcionalidad del mismo.	17/08/09	
18	Verificar las ventajas que se ajustan al sistema de seguridad de la intranet de la Universidad.	26-09-07	

19	Utilizar de manera eficiente todos los equipos que se encuentren en el área de la energía las industrias y los recursos naturales no renovables	10/09/09	
20	Encontrar Documentación sobre la configuración de archivos en 3Com	17/09/09	
21	Swicht capa 2 administrables configurados dentro del Área de la Energía, Industrias y Recursos Naturales no Renovables	01/10/09	
22	Esquema de seguridad funciona y se ejecuta en el servidor	09/10/09	
23	Obtener el criterio de los usuarios que tengan acceso al servicio	13/10/09	

ANEXO 2: ENCUESTAS DIRIGIDAS A ENCARGADOS DE LOS CENTROS DE COMPUTOS

UNIVERSIDAD NACIONAL DE LOJA

Área De Energía, Industrias Y Recursos Naturales No Renovables

CARRERA DE INGENIERIA EN SISTEMAS

ENCUESTA

Como Egresados de la Carrera de Ingeniería en Sistemas le solicitamos de la manera mas comedida que se digne colaborar en la contestación de la siguiente entrevista, cuyos datos nos servirán de apoyo en el desarrollo de nuestra tesis, acerca de la "SEGURIDAD EN LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA"

Nombre: _____
Área: _____
Cargo: _____
Fecha: _____

1. **¿De quién depende la responsabilidad de la seguridad informática en la Institución?**
   - Auditoria Interna. ( )
   - Jefatura de Informática. ( )
   - Departamento de Finanzas. ( )
   - No se tiene específico formalmente. ( )

2. **El presupuesto de la Institución incluye aspectos de seguridad informática.**
   Si ( ) No ( )

3. **¿En qué se centra la seguridad informática en la Institución? (Elija todas las que se apliquen).**
   - Protección de la red. ( )
   - Proteger los datos críticos de la Institución. ( )
   - Proteger el almacenamiento de los datos de los estudiantes. ( )
   - Desarrollo y afinamiento de seguridad de las aplicaciones. ( )
   - Otras: ( )
     ¿Cuáles?
     ……
     ……

4. **¿Qué casos de violación de seguridad tuvieron lugar en la Institución? (Elija todas las respuestas aplicables).**
   - Manipulación de aplicaciones de Software. ( )
   - Accesos no Autorizados. ( )
   - Virus. ( )

- Robo de datos. ( )
- Monitoreo no Autorizado del tráfico. ( )
- Negación del Servicio. ( )
- Pérdida de Integridad. ( )
- Pérdida de Información. ( )
- Ninguno. ( )
- Otros. ( )
  ¿Cuáles?
  .....
  .....

5. ¿Cuántas intrusiones o incidentes de seguridad identifico en promedio durante el periodo anterior?

- Ninguna ( )
- Entre 1-3 ( )
- Entre 4-7 ( )
- Mas de 7 ( )
- No sabe ( )
- No responde ( )

6. Una vez que ocurre la violación de seguridad esta se notifica a:

- Asesor legal ( )
- Autoridades Locales ( )
- Departamento de Informática ( )
- Ninguna No se denuncia ( )
- Otro ( )
  ¿Cuál?
  .....
  .....

7. ¿Cuántas pruebas de seguridad realiza la Institución para valorar el estado de seguridad informática?

- Una al Año ( )
- Entre 2 y 4 al año ( )
- Más de 4 al año ( )
- Ninguna ( )

8. ¿Cuál de los siguientes mecanismos utiliza actualmente la Institución para proteger sus Sistemas de Información? (Elija todas las aplicables).

- Smart Cards ( )
- Biometría (huella, digital) ( )
- Antivirus ( )
- Autenticación Autorización (AA) ( )
- Filtro de paquetes ( )
- Firewalls Hardware ( )
- Firewalls Software ( )
- Firmas digitales/certificados digitales ( )

- VPN (Redes privadas virtuales) ( )
- Proxies ( )
- Sistemas de detección de intrusos ( )
- Monitoreo ( )
- Ninguno ( )
- Otros ( )

  ¿Cuáles?

  ……
  ……

9. ¿La Institución cuenta con políticas de seguridad de redes?

- No se tiene políticas de seguridad definidas ( )
- Actualmente se encuentra en desarrollo ( )
- Existe políticas formales, escritas documentadas e informada a todos ( )

10. ¿Cuáles de los siguientes es obstáculo principal para lograr una adecuada seguridad informática en la Institución?

- Inexistencias de políticas de seguridad ( )
- Falta de tiempo ( )
- Falta de formación Técnica ( )
- Falta de apoyo de directivos ( )
- Falta de colaboración entre Aéreas ( )
- Complejidad Tecnológica ( )
- Poco entendimiento de seguridad informática ( )
- Falta de recursos ( )
- Falta de personal ( )
- Ninguno ( )

11. ¿De las siguientes actividades de seguridad cuáles son realizadas en la Institución y cuáles son realizadas por personal externo?

	Institución	**Personal Externo**
- Integración y pruebas de los planes de recuperación de información	( )	( )
- Divulgación de aspectos relacionados con la seguridad	( )	( )
- Manejo de incidentes de seguridad y análisis de vulnerabilidades	( )	( )
- Evaluación de Seguridad	( )	( )
- Seguimiento y Monitoreo de actividades	( )	( )
- Administración de Seguridad	( )	( )
- Configuraciones técnicas	( )	( )

12. ¿Con que frecuencias se hacen las revisiones de seguridad de activos de información?

- Anual ( )
- Semestral ( )
- Eventual ( )
- Nunca ( )

13. Dentro de la Institución, ¿Cuáles de los siguientes aspectos son de mayor preocupación en el área de seguridad?

- Informática móvil ( )
- Memoria extraíbles ( )
- Redes inalámbricas ( )
- Telefonía voz sobre IP ( )
- Servidores ( )
- Ninguno ( )
- Otros ( )

  ¿Cuáles?

  ……

  ……..

14. Cuáles de los siguientes mecanismos de protección a nivel de transporte utilizan?

- Protocolo de transporte Secure Sockets Layer (SSL) ( )
- Transport Layer Security (TLS) ( )
- Wireless Transport Layer Security (WTLS) ( )
- Ninguno ( )
- Otros

  ¿Cuáles?

  ……

  ……..

Gracias por su Colaboración

……..

Firma

ANEXO 3: ENTREVISTAS DIRIGIDAS A ENCARGADOS DE LOS CENTROS DE COMPUTOS

UNIVERSIDAD NACIONAL DE LOJA

Área De Energía, Industrias Y Recursos Naturales No Renovables

CARRERA DE INGENIERIA EN SISTEMAS

ENTREVISTA

Como **Egresado de la Carrera de Ingeniería en Sistemas** le solicitamos de la manera mas comedida que se digne colaborar en la contestación de la siguiente entrevista, cuyos datos nos servirán de apoyo en el desarrollo de nuestra tesis, acerca de la "**SEGURIDAD EN LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA"**

Nombre: _____
Área: _____
Cargo:_____
Fecha:_____

1. ¿Qué entiende usted sobre seguridad informática?
   ……
   ……
   ……
2. ¿Qué medidas implementarías usted para tener una mayor seguridad de los datos tanto inalámbrica como alámbricas?
   ……
   ……
   ……
3. ¿Qué tipo de mecanismos de seguridad informática se ejecuta en la actualidad?
   ……
   ……
   ……
4. ¿Qué opina acerca del Control de Acceso (Autenticación, Autorización) en redes de datos?
   ……
   ……
   ……

5. ¿Considera usted que la seguridad en la red inalámbrica y alámbricas, implementado en la Universidad Nacional de Loja es segura?

   ……
   ……
   ……

6. ¿Qué sugerencias ayudarían a mejorar la seguridad en la red de datos de la Universidad Nacional de Loja?

   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……

RESUMEN:

Gracias por su Colaboración.

…….

Firma

ANEXO 4: VIDEO DE ENTREVISTAS REALIZADAS A LOS RESPONSABLES DE LOS CENTROS DE COMPUTOS

ANEXO 5: VIDEO DE LA DISTRIBUCION DE LA RED DE DATOS INTERNA DE LA UNIVERSIDAD NACIONAL DE LOJA

ANEXO 6: ENCUESTAS DIRIGIDAS A LOS USUARIOS DE LA RED INALAMBRICA AEIRNNRSEGWIFI

UNIVERSIDAD NACIONAL DE LOJA

Área De Energía, Industrias Y Recursos Naturales No Renovables

CARRERA DE INGENIERIA EN SISTEMAS

ENCUESTA

Como Egresados de la Carrera de Ingeniería en Sistemas le solicitamos de la manera más comedida que se digne colaborar en la contestación de la siguiente encuesta, cuyos datos nos servirán de apoyo en el desarrollo de nuestra tesis, acerca de la "SEGURIDAD EN LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA"

Nombre: _____
Carrera: _____
Fecha: _____

Instrucción:

- Instale el certificado del servidor (root.der) y (RADIUS.der), seleccionamos colocar todos los certificados en almacén de certificados de confianza.
- Para configurar la red por favor revise el manual de usuario que se le adjunta en la encuesta.
- Acceda al Nombre de Red (SSID): AEIRNNRSegWifi

1. ¿Pudo configurar satisfactoriamente la tarjeta de red inalámbrica?

SI ( ) NO ( )

¿Qué inconvenientes tubo?
.....
.....

2. Dados su usuario-contraseña pudo acceder a la red inalámbrica AEIRNNRSegWifi

SI ( ) NO ( )

¿Que inconvenientes tubo?
.....
.....

3. Conoce Ud. acerca de seguridades en redes inalámbrica?

SI CONOCE ( ) CONOCE POCO ( ) NO CONOCE ( )

4. Considera que el servicio de Seguridad en redes inalámbrica es una prestación que se debería implementar en el AEIRNNR definitivamente?

SI ( ) NO ( )

Porque?.....
.....

5. De las siguientes alternativas que Ud. conoce escoja. Cual (es) cree que se debería implementar para mejorar la seguridad en las redes inalámbricas en el AEIRNNR.

WEP ( ) **Wired Equivalent Privacy** o "Privacidad equivalente a cableado"

WPA ( ) **Wifi Ptorected Access** o "Acceso Protegido Wifi"

RADIUS ( )

6. ¿Qué nivel de satisfacción tubo al conectarse a la red inalámbrica del AEIRNNRSegWifi?

EXELENTE ( ) SATISFACTORIA ( ) FALLIDA ( )

Firma:……..

GRACIAS POR SU COLABORACION

ANEXO 7: ACRONIMOS

ACRÓNIMOS

WLAN	Red inalámbrica de área local
IP	Protocolo de Internet
AAA	Protocolo de autentificación, autorización y manejo de cuentas
WAP	*Wireless Application Protocol*
WEP	*Wired Equivalent Privacy*
IEEE	*Institute of Electric and Electronic Engineers*
AP	Punto de Acceso
RADIUS	*Remote authentication dial-in user service*
PAP	Protocolo de autentificación por contraseña
CHAP	Protocolo de autentificación por desafío de saludo
EAP	Protocolo de autentificación extensible
WPA	*Wi-fi Protected Access*
SSID	*Service Set IDentifier*
MAC	*Media Access Control*