UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN "SEGURIDAD INFORMATICÁ"

TEMA:

"SISTEMAS DE CONTROL DE ACCESO PARA GARANTIZAR LA SEGURIDAD DE LAS REDES INALÁMBRICAS DEL GOBIERNO PROVINCIAL DE TUNGURAHUA"

Trabajo de Graduación Modalidad: Seminario, presentado como requisito previo a la Obtención del Título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Edisson Israel Yungán Muzo

TUTOR: Ing. René Francisco Terán Rodríguez M.Sc.

Ambato – Ecuador

Octubre - 2012

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, nombrado por el H. Consejo Superior de Pregrado de la Universidad Técnica de Ambato:

CERTIFICO:

Que el trabajo de investigación: **"SISTEMAS DE CONTROL DE ACCESO PARA GARANTIZAR LA SEGURIDAD DE LAS REDES INALÁMBRICAS DEL GOBIERNO PROVINCIAL DE TUNGURAHUA"** presentado por el Sr. Edisson Israel Yungán Muzo, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato; reúne los requisitos y méritos suficientes para ser sometido a la evaluación del jurado examinador que el H. Consejo de Pregrado designe.

Ambato, octubre 2012

EL TUTOR

……..……

Ing. René Terán

AUTORÍA

El presente trabajo de investigación titulado: **"SISTEMAS DE CONTROL DE ACCESO PARA GARANTIZAR LA SEGURIDAD DE LAS REDES INALÁMBRICAS DEL GOBIERNO PROVINCIAL DE TUNGURAHUA"** es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, octubre 2012

…….

Edisson Israel Yungán Muzo

C.I. 180388311-3

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Alvaro Sánchez e Ing. Jaime Ruiz, revisó y aprobó el Informe Final del trabajo de graduación titulado **"SISTEMAS DE CONTROL DE ACCESO PARA GARANTIZAR LA SEGURIDAD DE LAS REDES INALÁMBRICAS DEL GOBIERNO PROVINCIAL DE TUNGURAHUA"**, presentado por el señor Edisson Israel Yungán Muzo de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

…….

PRESIDENTE DEL TRIBUNAL

Ing. Oswaldo Eduardo Paredes Ochoa M.Sc.

…….	……
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR
Ing. Alvaro Eduardo Sánchez Ríos	Ing. Jaime Bolívar Ruiz Banda

DEDICATORIA

El presente trabajo está dedicado con mucho cariño:

A mi madre María Mercedes, por apoyarme en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mi padre Daniel, por los ejemplos de perseverancia y constancia que lo caracterizan y me ha infundado siempre, por el valor mostrado para salir adelante.

A mis hermanas, Diana y Pamela por estar conmigo y apoyarme siempre, las quiero mucho.

Todo este trabajo ha sido posible gracias a ellos.

Edisson I. Yungán M.

AGRADECIMIENTO

Mi más sincero agradecimiento a la Universidad Técnica de Ambato, en especial a mi querida Facultad de Ingeniería en Sistemas, Electrónica e Industrial, por los conocimientos brindados durante toda mi vida estudiantil.

Al Ing. René Terán por su acertada dirección para culminar con éxito el presente proyecto.

A todos mis amigos que de una u otra forma aportaron a que este sueño se haga realidad.

Edisson I. Yungán M.

Índice General

Índice de Gráficos

Índice de Tablas

Resumen Ejecutivo

En este documento se presenta el diseño e implementación sistema de control de acceso para garantizar la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua, haciendo uso de certificados digitales para proporcionar autenticación y autorización para el cliente.

En el primer capítulo se detalla el problema planteado, desde el contexto en el que se encuentra, realizando el análisis de la situación actual del Gobierno Provincial de Tungurahua para justificar el desarrollo del presente proyecto, estableciendo los objetivos que permitirá desarrollar el problema.

En el capítulo dos se describe toda la fundamentación teórica utilizada para el desarrollo del problema, definiendo los conceptos y argumentos técnicos en los que se basa el presente proyecto.

En el capítulo tres se define la metodología necesaria para determinar una solución que permita verificar la hipótesis, utilizando los instrumentos de recopilación de información que contribuirán con datos significativos que ayudarán a determinar la mejor alternativa para el problema.

En el cuarto capítulo se analizan e interpretan los resultados obtenidos, por las técnicas de recolección de la información, determinando con los datos proveídos por los funcionarios del Gobierno Provincial de Tungurahua, si el proyecto es necesario y viable en beneficio de la institución.

En el quinto capítulo se establecen las conclusiones y recomendaciones de los resultados obtenidos en los cuatro primeros capítulos, para realizar un adecuado sistema de control de acceso a la red inalámbrica.

Por ultimo, en el capitulo seis se desarrolla la propuesta, dentro del cual se especifica paso a paso las configuraciones e instalaciones realizadas por el autor, basándose en la fundamentación teórica registrada en este documento para obtener la solución al problema planteado.

INTRODUCCIÓN

Las tecnologías inalámbricas se presentan como las de mayor auge y proyección en la actualidad siendo un de las tecnologías líderes en comunicación, dado que el soporte para redes inalámbricas se han incorporado cada vez más en los diferentes dispositivos ya sea computadores portátiles PDA's o teléfonos móviles, permitiendo superar las limitantes de espacio físico y ofrecen una mayor movilidad a los usuarios.

Actualmente en los diferentes lugares públicos como hoteles, aeropuertos, centros comerciales están ofreciendo el servicio de áreas Wi-Fi para satisfacer las necesidades de los usuarios que en su mayoría ya cuentan con dispositivos inalámbricos, para poder acceder a ella con solo solicitar el permiso de acceso.

Las redes inalámbricas de área local (WLAN *Wireless Local Area Networks*) desempeñan un papel importante en las comunicaciones debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red cableada.

La seguridad dentro del entorno de redes inalámbricas es un aspecto que cobra especial relevancia. Dentro de una red cableada es necesario tener una conexión física al cable de red, mientras que en una red inalámbrica desplegada en un establecimiento una tercera persona podría tener acceso a la red sin que tuviera la necesidad de encontrarse dentro de las instalaciones de la empresa, ya que la señal no está limitada a un área, a un cable o una fibra óptica solo le bastaría con estar dentro del alcance de la señal o dentro de su radio de cobertura.

Esto hace muy vulnerables a las redes inalámbricas, porque pueden existir terceras personas que estén monitorizando la red y se convierte en una amenaza de alto riesgo para las empresas, pero existen mecanismos de seguridad que permiten la encriptación de la comunicaciones mediantes diferentes algoritmos que permitan autenticar a los usuarios para evitar accesos no autorizados y evitar la intercepción de la información.

El Gobierno Provincial de Tungurahua cuenta con una red cableada, con el avance tecnológico vio la necesidad de expandir a una red inalámbrica pero no se han considerado los diferentes aspectos que conlleva esta tecnología, por eso fue necesario realizar un estudio de las redes inalámbricas con las que cuentan estas instalaciones, debido a que la información que manejan es de suma importancia.

Este estudio pretende analizar y presentar un modelo de implementación a llevar a cabo en el Gobierno Provincial de Tungurahua, bajo el cual se garantice como primer objetivo un acceso seguro a la red inalámbrica utilizando mecanismos de seguridad.

CAPITULO I

1. EL PROBLEMA DE INVESTIGACIÓN

1.1. Tema de Investigación

Sistema de control de acceso a las redes inalámbricas del Gobierno Provincial de Tungurahua.

1.2. Planteamiento del problema

1.2.1. Contextualización

Las redes inalámbricas últimamente están presentes en casi todas las empresas instituciones y organismos, sean públicos y privados, además de encontrarse en muchos hogares, y sea convertido en un factor clave para la mejora de calidad de servicios y aumento de la productividad. La implementación de esta nueva tecnología posee una serie de vulnerabilidades y ataques característicos a nivel de seguridad que son importantes conocerlos y distinguirlos para evitar los problemas de seguridad, por lo que la seguridad de las redes inalámbricas se ha convertido en uno de los principales aspectos a tener en cuenta. A nivel mundial se están realizando grandes esfuerzos en el desarrollo de estándares, tecnologías e implementando diferentes sistemas de control de acceso a las redes inalámbricas, siempre buscando garantizar la seguridad de la información que se transfiere por estos medios inalámbricos, manteniendo la filosofía de una conexión móvil.

A nivel nacional la implementación de redes inalámbricas se ha ido incrementando en las diferentes instituciones que están dentro del ámbito comercial, laboral y educativo, porque facilita la difusión de la información de forma ágil y sin complicaciones pero el aspecto de la seguridad ha sido descuidada dentro de un alto porcentaje por parte de las diferentes instituciones que cuentan con esta infraestructura. La mayor parte de los administradores de red no han tomado las medidas de seguridad apropiadas para proteger la información que transmite por este medio, ya que la mayoría de los administradores no establecen políticas para evitar problemas de seguridad, por lo general esperan sufrir un ataque y después establecer los mecanismos de seguridad para proteger su información.

El Gobierno Provincial de Tungurahua ha implementado una red inalámbrica como alternativa a una red cableada en la mayoría de sus departamentos. En los sistemas de control de acceso que vienen por defecto en los dispositivos inalámbricos son obsoletos y vulnerables lo que hace que la seguridad de la información se ponga en riesgo al momento de la comunicación entre dispositivos lo que convierte a la red en un canal inseguro.

1.2.2. Análisis crítico

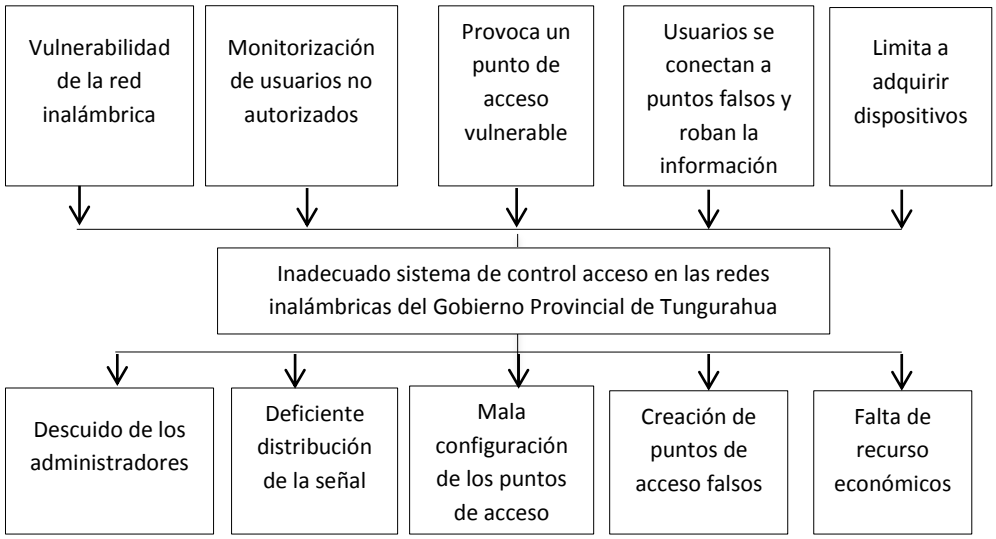

Figura 1.1: Análisis critico

La falta de atención de los administradores de red al tema de seguridad de las redes inalámbricas es un problema que a pesar de su gravedad no ha recibido la atención apropiada, ya que la red inalámbrica es el medio de comunicación principal del Gobierno Provincial de Tungurahua.

El acceso sin necesidad de cables a la red es uno de los problemas más importantes ya que cualquier equipo inalámbrico que se encuentre dentro del área de cobertura de la red podrá tener acceso a ella, esto hace muy vulnerable a las redes inalámbricas ya que cualquier usuario podría estar monitorizando los datos de las instalaciones.

Las configuraciones por defecto que vienen en los dispositivos de acceso inalámbrico no son cambiadas por muchos de los administradores de la red y dejan la configuración fijada por la fábrica distribuidora del dispositivo. Por ejemplo: parámetros como las claves y usuarios o el nombre de red se mantienen inalterados. La mayoría de las instalaciones se cambia el nombre de la red, pero lo más importante como la clave de acceso del administrador, en muchos casos, se mantiene la de fábrica, y esto provoca que sea un punto de acceso simple para cualquier intruso.

La creación de puntos de acceso falsos es una amenaza de las más comunes en las redes inalámbricas, también conocidos como puntos de acceso piratas que se hacen pasar como puntos de acceso legales confundiendo a los usuarios que se quieran conectar ella, el usuario puede llegar a revelar información y claves importantes de la empresa.

La falta de recursos económicos podría ser una de las falencias para no poder asegurar la red inalámbrica ya que no se podría obtener los dispositivos suficientes para diseñar una correcta topología de red que permita una correcta transmisión de la información y seguridad de la misma.

1.2.3. Prognosis

Al no implementar un correcto sistema de control de acceso a las redes inalámbricas del Gobierno Provincial de Tungurahua, las redes quedarían expuestas a ataques, de modo que cualquiera puede entrar en ellas. La falta de un sistema de control de acceso permitiría que personas que están detrás de las paredes de la institución viendo o descargando contenido ilegal o de dudosa moral, o utilizando la red como punto de acceso a otras redes para causar algún daño y estos actos pueden ser atribuidos a la institución la misma que pagaría las consecuencias por no prestar la suficiente atención a asegurar las redes inalámbricas.

Por lo anteriormente indicado, se hace necesaria la implementación de un sistema de control de acceso para las redes inalámbricas del Gobierno Provincia de Tungurahua.

1.2.4. Formulación del problema

¿De qué manera el sistema de control de acceso incide en la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua?

1.2.5. Preguntas directrices

- ¿Cuáles son los sistemas de control de acceso utilizados en las redes inalámbricas del Gobierno Provincial de Tungurahua?
- ¿Qué seguridades existen en las redes inalámbricas del Gobierno Provincial de Tungurahua?
- ¿Cuál es el sistema de control de acceso más adecuado para las redes inalámbricas del Gobierno Provincial de Tungurahua?

1.2.6. Delimitación

La investigación se desarrollará dentro del campo de seguridad de la información y dentro del área de las redes inalámbricas y especificando los mecanismos de control de acceso a las redes inalámbricas.

El presente proyecto se lo realizo en el Gobierno Provincial de Tungurahua que está ubicado en la ciudad de Ambato, que cuenta con dos instalaciones. La primera está ubicada en la calle Bolívar y Castillo esquina, y la segunda instalación se encuentra ubicada en la calle Sucre y Castillo esquina.

1.3. Justificación

La implementación de redes inalámbricas en el Gobierno Provincial de Tungurahua trae consigo importantes riesgos de seguridad que afrontar, por lo que se pretende implementar un sistema de control de acceso a las redes inalámbricas del Gobierno Provincial de Tungurahua suficientemente fuertes que protejan el acceso a los recursos tecnológicos y a la información.

Como las redes inalámbricas transmiten y reciben datos por aire mediante tecnología de radio frecuencia cualquiera podría estar escuchando la información transmitida y no solo eso, sino que también podría alterar la información o modificarla, para evitar estos ataques, se utiliza el sistema de autenticidad y encriptación de datos.

Los principales beneficiarios de la implementación del sistema de control de acceso serán los funcionarios de la institución, debido a que el sistema de control de acceso realizará los procedimientos de identificación, autenticación y autorización para permitir o denegar el uso de los recursos de la red, dando al usuario la suficiente garantía y seguridad en la transmisión de la información.

1.4. Objetivos

1.4.1. Objetivo General

Implementar un sistema de control de acceso para garantizar la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua.

1.4.2. Objetivos Específicos

- Analizar los sistemas de control de acceso utilizados en las redes inalámbricas del Gobierno Provincial de Tungurahua.
- Determinar un sistema de autenticación utilizando protocolos de seguridad para garantizar la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua.
- Proponer un sistema de control de acceso que permita establecer políticas de seguridad para la utilización de las redes inalámbricas del Gobierno Provincial de Tungurahua.

CAPITULO II

2. MARCO TEORICO

2.1. Antecedentes investigativos

Se ha tomado como referencias de estudio las siguientes tesis, ya que hacen relación con la seguridad de las redes inalámbricas.

"ASPECTOS DE SEGURIDAD DE REDES INALÁMBRICAS DE RED DE ÁREA LOCAL" Autor: Hernán Santiago Analuisa Yancha; Año: 2006.

Se ha tomado como referencia de estudio esta tesis porque se refiere a la seguridad de redes inalámbricas, dentro del cual hace un estudio de los diferentes sistemas de seguridad, los medios de transmisión y protocolos de seguridad. Además realiza la implantación de un sistema de seguridad en un pequeño entorno inalámbrico.

"ANALISIS A LA SEGURIDAD DE REDES INALAMBRICAS COMO EXTENSIÓN DE UNA RED LAN" Autores: Reascos Irving; Cabrera Proaño, Claudio Armando

Se ha tomado como referencia esta tesis porque se enfoca en la seguridad de las redes inalámbricas. Y propone mecanismos de seguridad para evitar ataques a la red WLAN utilizando sistemas de autenticación y encriptación de datos como son: estándar 802.1x, 802.1i y los mecanismos WEP y WPA como mecanismos básicos y avanzados respectivamente.

2.2. Fundamentación legal

La presente investigación se rige a la Constitución de la República del Ecuador

Sección tercera

Comunicación e Información

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Sección novena

Personas usuarias y consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de

estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

Art. 53.- Las empresas, instituciones y organismos que presten servicios públicos deberán incorporar sistemas de medición de satisfacción de las personas usuarias y consumidoras, y poner en práctica sistemas de atención y reparación.

El Estado responderá civilmente por los daños y perjuicios causados a las personas por negligencia y descuido en la atención de los servicios públicos que estén a su cargo, y por la carencia de servicios que hayan sido pagados.

Art. 54.- Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente por la deficiente prestación del servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore.

Las personas serán responsables por la mala práctica en el ejercicio de su profesión, arte u oficio, en especial aquella que ponga en riesgo la integridad o la vida de las personas.

Sección octava

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

2.3. Categorías fundamentales

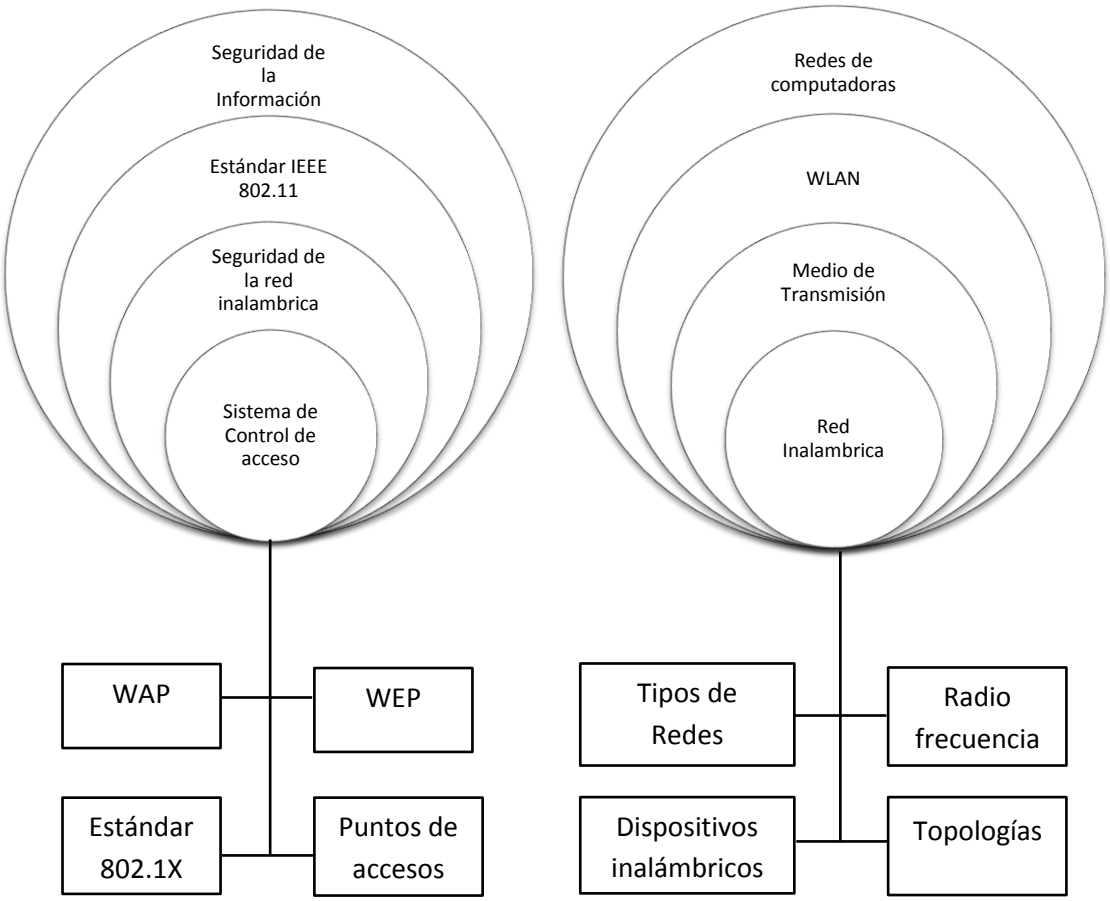

Figura 2.1. Categorías Fundamentales

2.3.1. Redes de Computadoras

UYLESS, Black (1997, Pág. 1) "Una red de computadoras es el conjunto de computadores (y generalmente terminales) conectados mediante una o más vías de transmisión. La vía de transmisión es a menudo la línea telefónica, debido a su comodidad y a su presencia universal. La red existen para cumplir un determinado objetivo: la transferencia e intercambio de datos es la base de muchos servicios basados en computadores que utilizamos en nuestra vida diaria, como cajeros automáticos, terminales de punto de venta, realización de transferencias, e incluso el control de un transbordador espacial".

RAYA, José; RAYA, Cristina (2002, Pág. 1) "Una red de computadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello es necesario contar, además de con los computadores correspondientes con las tarjetas de red, los cables de conexión, los dispositivos periféricos y el software conveniente".

SANCHEZ, Jairo (Internet; 26/11/1999; 25/10/2011; 12h00) "Las redes constan de dos o más computadoras conectadas entre sí y permiten compartir recursos e información. La información por compartir suele consistir en archivos y datos. Los recursos son los dispositivos o las áreas de almacenamiento de datos de una computadora, compartida por otra computadora mediante la red. La más simple de las redes conecta dos computadoras, permitiéndoles compartir archivos e impresos. Una red mucho más compleja conecta todas las computadoras de una empresa o compañía en el mundo."

Básicamente una red de computadoras es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos.

2.3.2. Redes Inalámbricas

MADRID, Juan (Internet, 20/04/2004; 02/10/2011, 15h00) Cuando se habla de tecnología WIFI, realmente se está haciendo referencia a la WI-FI Alliance. Se trata de una organización sin ánimo de lucro, que engloba a un amplio grupo de fabricantes, con el objetivo de promocionar el uso de la tecnología inalámbrica en redes de área local, y asegurando la compatibilidad entre fabricantes en base a los estándares IEEE 802.11. La proliferación de este tipo de tecnología ha sido explosiva y se prevé que la mayoría de los equipos ya dispongan de dispositivos WIFI.

CURQUEJO, Alejandro (Internet; 16/1/2005; 25/10/2011; 11h00) Las tecnologías de interconexión inalámbrica van desde redes de voz y datos globales, que permiten a los usuarios establecer conexiones inalámbricas a través de largas distancias, por luz infrarroja y radiofrecuencia que están optimizadas para conexiones inalámbricas. Entre los dispositivos comúnmente utilizados para la interconexión inalámbrica se encuentran los equipos portátiles, equipos de escritorio, asistentes digitales personales (PDA), teléfonos celulares, equipos con lápiz y localizadores.

Una red inalámbrica dentro del espectro radio eléctrico utiliza ondas de radio para conectar dispositivos inalámbricos, como equipos portátiles a internet y a la red de su empresa y sus aplicaciones, con el propósito de compartir información.

2.3.2.1. Ventajas y desventajas de las Redes Inalámbricas

Ventajas

Las principales ventajas que ofrecen las redes inalámbricas, y que deben ser consideradas para complementar una red cableada, son las siguientes:

- Movilidad. Cualquier dispositivo móvil que cuente con interfaz WIFI puede moverse a través del área de cobertura sin perder conectividad con la red.

- Flexibilidad. Se puede colocar un dispositivo portátil en cualquier lugar dentro del área de cobertura sin hacer cambios en la configuración de la red.
- Ahorro de costos. La adopción de una red inalámbrica como una solución de conectividad, puede permitir ahorrar costos en el sentido de que, se puede requerir de un menor número de equipos, la configuración e instalación se simplifica, y no es necesario cambiar la infraestructura física del lugar.
- Escalabilidad. Se puede añadir más dispositivos de conectividad sin que esto implique grandes cambios respecto a la configuración inicial.

Desventajas

Los principales inconvenientes de las redes inalámbricas son los siguientes:

- Menor capacidad de canal. Las redes cableadas pueden trabajar hasta 10Gbps, mientras que las redes inalámbricas WIFI lo hacen teóricamente hasta 108Mbps.
- Seguridad. Cualquier persona con una computadora portátil y con un programa adecuado puede localizar la red y tratar de obtener la clave de autenticación para ingresar a los recursos para usuarios legítimos.
- Interferencias. Las redes inalámbricas funcionan en las bandas de frecuencia de 2.4GHz y 5.8GHz, las cuales no requieren de licencias administrativas, y por lo tanto son altamente utilizadas.

2.3.2.2. Infraestructura de una WLAN

Existen tres componentes principales que forman la base de una WLAN. Estos son:

2.3.2.2.1. Adaptadores Inalámbricos

Los adaptadores inalámbricos tienen componentes equivalentes a los de los adaptadores usados en redes cableadas como adaptadores USB y tarjetas de red

inalámbricas. También tienen la misma función, permitiendo a los usuarios acceder a la red. En una LAN, los adaptadores proveen la interface entre el sistema de operación de la red y el cable. En una WLAN, estos proveen la interface entre el sistema de operación de la red y una antena para crear una conexión transparente a la red.

2.3.2.2.2. Punto de acceso

El punto de acceso es el equivalente inalámbrico al hub en una LAN. Este recibe y transmite los datos entre la WLAN y la red cableada, que soporta un grupo de usuarios con dispositivos inalámbricos. Típicamente, un punto de acceso se conecta con el eje principal de la red, es decir, el enlace principal de conexión entre nodos de una red, a través de un cable Ethernet estándar, y se comunica con los dispositivos inalámbricos a través de una antena. El punto de acceso o la antena conectada al mismo, generalmente se instala en una pared alta o en el techo. Como las células en redes de telefonía celular, múltiples puntos de acceso pueden realizar handoff de un punto de acceso a otro mientras el usuario se mueva de un área a otra. Los puntos de acceso tienen un rango de 20 a 500 metros. Un punto de acceso puede soportar entre 15 y 250 usuarios, dependiendo de la tecnología, configuración y el uso. Es relativamente fácil extender una WLAN agregando más puntos de acceso para reducir la congestión de la red y expandir el área de cobertura. Las redes grandes que requieren múltiples puntos de acceso crean células que se traslapan, creando una conectividad constante a la red.

2.3.2.2.3. Puentes LAN para exterior

Los puentes LAN en el exterior conectan LAN's en diferentes edificios. Cuando se considera el costo de comprar un cable de fibra óptica que una a edificios, una WLAN puede ser una alternativa económica. Los puentes usados en WLAN soportan tasas de transferencia altas y rangos de varios kilómetros con el uso de antenas direccionales con línea de vista. Algunos puntos de acceso también pueden usarse como puentes entre edificios que se encuentren relativamente cerca.

2.3.2.3. Topología WLAN

UYLESS, Black (1997, Pág. 8) “Una configuración de red se denomina topología de red. Por tanto, la topología establece la forma (en cuanto a conectividad física) de la red. El termino topología se utiliza en geometría para describir la forma de un objeto”

SANCHEZ, Jairo (Internet; 26/11/1999; 25/10/2011; 12h00) “Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman. Los Criterios a la hora de elegir una topología, en general, buscan que eviten el coste del encaminamiento (necesidad de elegir los caminos más simples entre el nodo y los demás), dejando en segundo plano factores como la renta mínima, el coste mínimo, etc.”

Una WLAN se puede conformar de dos maneras:

2.3.2.3.1. En estrella

Esta configuración se logra instalando una estación central denominada punto de acceso (Access Point), a la cual acceden los equipos móviles. El punto de acceso actúa como regulador de tráfico entre los diferentes equipos móviles. Un punto de acceso tiene, por lo regular, un cubrimiento de 100 metros a la redonda, dependiendo del tipo de antena que se emplee, y del número y tipo de obstáculos que haya en la zona. Figura 2.2.

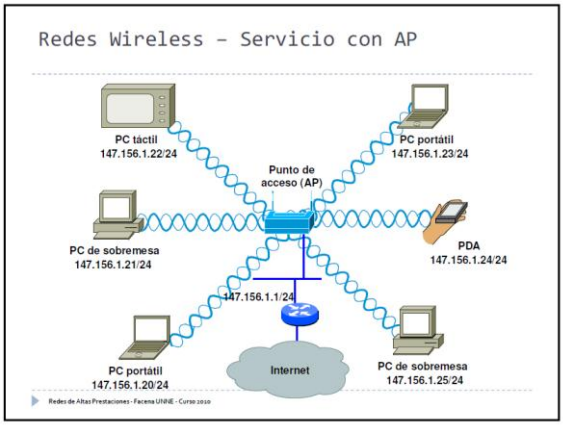

Figura 2.2: Topología Estrella

2.3.2.3.2. Red ad hoc

En esta configuración, los equipos móviles se conectan unos con otros, sin necesidad de que exista un punto de acceso. Figura 2.3.

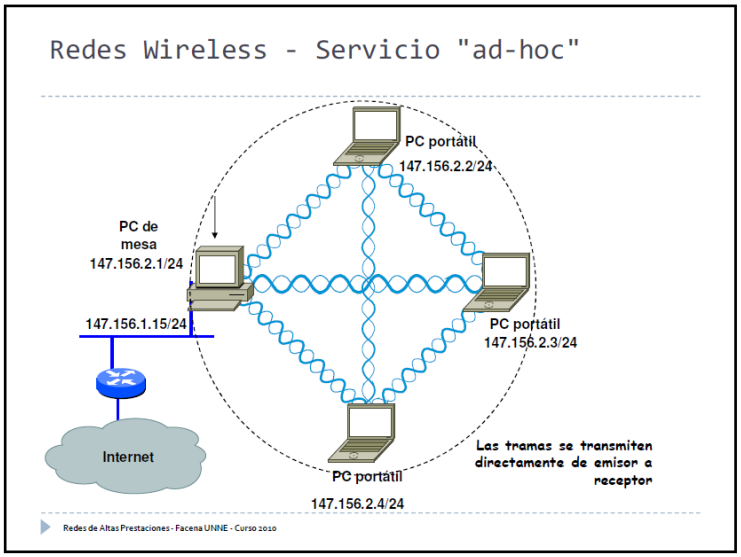

Figura 2.3: Topología ad-hoc

2.3.2.4. Medios de transmisión en WLAN

José, Raya; Cristina Raya (2002, Pág. 43) "Se entiende por medios de transmisión a cualquier medio físico que pueda transportar información en forma de señales electromagnéticas. Los medios de transmisión permiten mandar la información de una estación de trabajo al servidor o a otra estación de trabajo, y son una parte esencial de una red local".

CHORNOGUBSKY, Enrique (Internet; 15/12/2010; 25/10/2011; 12h00) "Si observamos la naturaleza estamos rodeados de fenómenos que involucran el concepto de ondas, desde la simpleza de una nota musical hasta la luz de las estrellas que llega a nuestros ojos. Como podrá adivinar, quienes realmente dominan este campo son los físicos, a nosotros nos basta con saber que las ondas pueden ser emitida por una fuente, que viaja a cierta velocidad (dependiendo de la frecuencia de la onda) y que son susceptibles de ser captadas por un receptor."

En los sistemas modernos de comunicación inalámbricos utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que estas únicamente realizan la función de llevar la energía aun receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. Por este motivo, la señal ocupa más ancho de banda que una sola frecuencia. Además, varias ondas portadoras pueden existir en el mismo tiempo y espacio sin interferir entre ellas, siempre que estas ondas sean transmitidas a distintas frecuencias de radio.

Existen, dos opciones de transmisión en las WLAN:

2.3.2.4.1. Infrarrojo

De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas de infrarrojos pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido o de línea de vista y en sistemas de gran apertura, reflejados o difusos.

2.3.2.4.2. Radio frecuencia

Las redes inalámbricas que utilizan radio frecuencia pueden clasificarse en sistemas de banda ancha o de frecuencia dedicada, y en sistemas basados en espectro disperso o extendido.

2.3.3. Seguridad de la información

MARTIN, Toni (Internet; 5/27/2010; 25/10/2011; 10h00) La seguridad de la información es la suma de estos tres elementos; confidencialidad, integridad y disponibilidad. Los cuales se encarga de proteger la información para que solos los usuarios permitidos accedan a ella, que la información sea exacta sin alteraciones, y siempre esté disponible.

CASTELLANOS, Wilmer (Internet; 7/2/2011; 25/10/2011; 10h00) “La estrategia de seguridad de la información es un patrón frente al cual una compañía toma sus decisiones de protección de la información con base en sus objetivos y propósito. El proceso de toma decisiones requiere de la definición de una política y de un plan de acción para alcanzar los objetivos de seguridad de la información. La estrategia permite definir los procesos y estructuras requeridos para satisfacer las necesidades de seguridad de la información de los accionistas, empleados, clientes y comunidad”.

RUBIO, Jaime (Internet; 2005; 25/10/2011; 10h15) “La Seguridad de la información es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recurso humano integrado para proveer toda la protección debida y requerida a la información y a los recursos informáticos de una empresa, institución o agencia gubernamental”.

La seguridad de la información integra la confidencialidad, integridad y disponibilidad de la información. Y trata de evitar amenazas y ataques que perjudiquen a los dueños de la información. Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza. Figura 2.4.

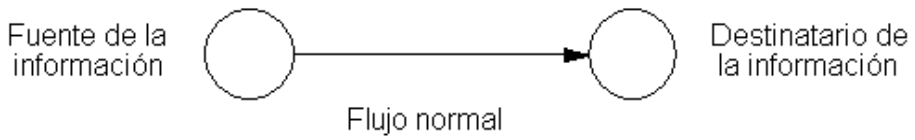

Figura 2.4: Flujo normal de la información

Las cuatro categorías generales de amenazas o ataques son las siguientes:

2.3.3.1. Interrupción

Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros. Figura 2.5.

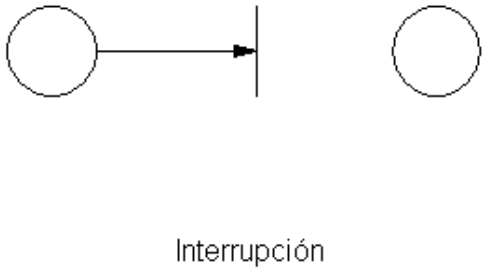

Figura 2.5: Interrupción de la información

2.3.3.2. Intercepción

Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad). Figura 2.6.

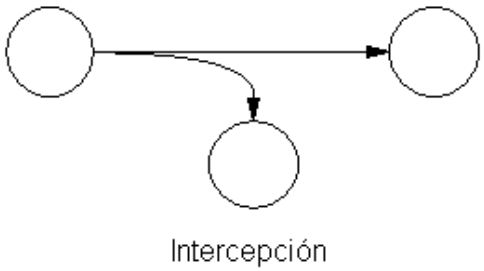

Figura 2.6: Intercepción de la información

2.3.3.3. Modificación

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de estos ataques son; el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red. Figura 2.7.

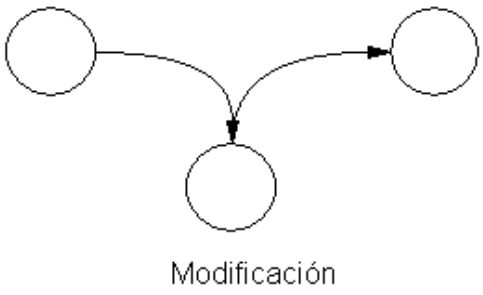

Figura 2.7: Modificación de la información

2.3.3.4. Fabricación

Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo. Figura 2.8.

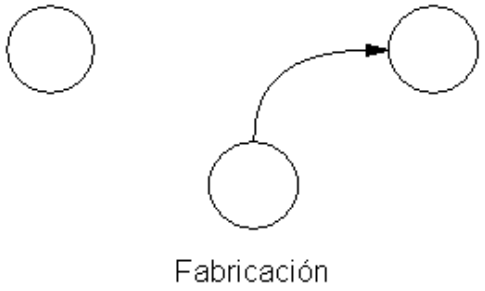

Figura 2.8: Fabricación de la Información

2.3.4. Estándares IEEE 802.11

RANDALL, Nichols; PANOS, Lekkas (2003, Pag.362) "El estándar IEEE 802.11 proporciona un mecanismo de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o solo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, solo aquellas estaciones que posean una clave cifrada serán autenticadas".

Las redes inalámbricas se caracterizan por no requerir de un medio guiado (cable) para interconectar a los equipos; sino que hace uso del aire para poder transmitir y recibir los datos. Como es de suponerse, el envío y recepción de las señales se realiza por medio de ondas electromagnéticas, las cuales se propagan por cualquier medio, teniendo al aire como principal y mejor medio aunque también pueden propagarse penetrando por obstáculos (paredes, puertas, ventanas, etc.) sufriendo una atenuación considerable y provocando que la señal se pierda como ruido.

HEATHER, Lane (Internet 06/02/2005; 5/10/2011, 16h15) Las redes inalámbricas 802.11, desarrolladas por el grupo de trabajo IEEE802.11 (formado en 1990) y dadas a conocer comercialmente como Wi-Fi por la Wireless Fidelity Alliance (organización conformada por las distintas compañías que desarrollan hardware

para esta tecnología y cuya principal misión es el de promover su uso en el hogar y en ambientes empresariales), operan en las dos capas inferiores del modelo de referencia OSI.

Este estándar define y gobierna las redes de área local inalámbricas (WLAN) que operan en el espectro de los 2,4 GHz (Giga Hercios) y fue definida en 1.997. El estándar IEEE 802.11b permite operar hasta 11Mbps y el 802.11a, que opera a una frecuencia mucho mayor (5 GHz), permite hasta 54Mbps. Figura 2.9.

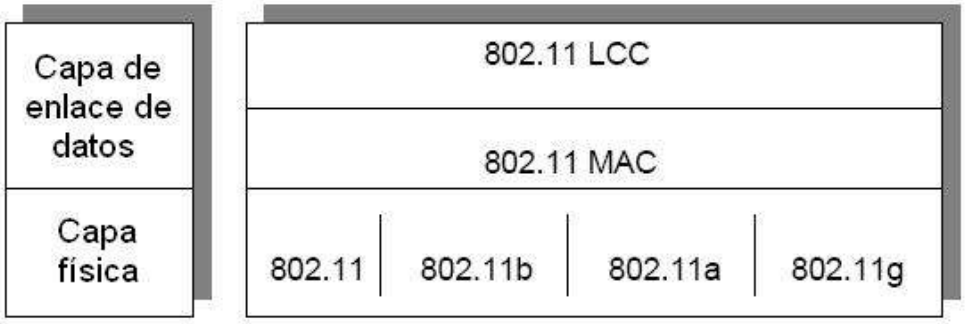

Figura 2.9: Ubicación del estándar 802.11 dentro del modelo OSI

2.3.4.1. 802.11b

Introducido en 1999, como extensión al estándar 802.11 publicado en 1997. Los equipos inalámbricos que operaban con la norma 802.11 nunca llegaron a tener una buena acogida, porque la máxima velocidad de conexión que ofrecían era de 2 Mbps. La norma 802.11b subsanó este problema al permitir lograr una velocidad más alta de transferencia de datos. Dicha velocidad tiene un límite de 11 Mbps (similar al de una red Ethernet convencional). En la práctica, se logran velocidades entre 2 y 5 Mbps, lo que depende del número de usuarios, de la distancia entre emisor y receptor, de los obstáculos y de la interferencia causada por otros dispositivos. El factor interferencia es uno de los que más influye, porque los equipos 802.11b operan en la banda de 2.4 GHz, en la que se presenta interferencia de equipos como teléfonos inalámbricos y hornos microondas. A pesar de sus problemas, el estándar 802.11b se ha convertido en el más popular.

2.3.4.2. 802.11a

Se introdujo al mismo tiempo que 802.11b, con la intención de constituirla en la norma para redes inalámbricas para uso empresarial (802.11b se enfocó hacia las redes caseras y para pequeños negocios). Ofrece velocidades de hasta 54 Mbps (típicamente 22 Mbps) y opera en la banda de 5 GHz. Su alto precio, el hecho de que la banda de 5 GHz esté regulada en algunos países, y su menor cubrimiento ha hecho que los equipos 802.11a sean menos populares que los 802.11b.

2.3.4.3. 802.11g

Surgió en 2003, como la evolución del estándar 802.11b. Esta norma ofrece velocidades hasta de 54 Mbps (22 Mbps típicamente) en la banda de 2.4 GHz, y es compatible hacia atrás con los equipos 802.11b, por lo cual ha tenido una gran acogida.

2.3.5. Seguridad en redes inalámbricas

Se han desarrollado una gran variedad de protocolos de seguridad para brindar protección a los recursos informáticos, y garantizar la integridad, confidencialidad y control de acceso de información.

Para minimizar el peligro que supone la implementación de una red inalámbrica, existen una serie de normas básicas a tener en cuenta a la hora de configurar la red, tales como:

2.3.5.1. Configuraciones por defecto

En contra de lo que suele pensarse, son muchos los administradores de la red que no cambian la configuración fijada en fábrica. Parámetros como las claves y usuarios o el nombre de red se mantienen inalterados. Es cierto que la en la mayoría de las instalaciones se cambia el nombre de la red, pero algo tan importante como la clave de acceso del administrador, en muchos casos, se mantiene inalterada, provocando un punto de acceso simple para cualquier intruso.

2.3.5.2. Activar encriptación

Es una de las prácticas claves y necesarias. Es el método básico y más inmediato de impedir accesos no autorizados a la red, así como capturas de tráfico y datos privados. Existen varios sistemas de encriptación que analizaremos en un punto posterior.

2.3.5.3. Uso de claves seguras

Puesto que es la llave a la red, las claves utilizadas han de ser suficientemente seguras y complejas de averiguar para asegurar la seguridad de la red. Es frecuente usar claves de solo letras, con palabras comunes y muy habitualmente referenciado a datos personales del administrador, como nombres de hijos, edades, etc. que hacen dicha clave fácil de averiguar.

2.3.5.4. Ocultar el nombre de red (SSID)

Aunque no es viable en todos los casos, la desactivación del anuncio del nombre de la red es un elemento de seguridad añadido. Por un lado, impedirá al atacante identificar la naturaleza y propietario de la red, y por otro hará necesario introducir el nombre de la red manualmente para permitir la asociación a la red Wi-Fi, por lo que previamente deberá ser conocida por el atacante.

2.3.5.5. Filtrados de direcciones MAC

En la mayoría de los puntos de acceso es posible especificar una lista de direcciones MAC que serán admitidas, siendo todas las demás rechazadas. La dirección MAC es una dirección de nivel 2 que lleva la tarjeta de red Wi-Fi grabada de fábrica (análoga a la dirección MAC-Ethernet). Por tanto, si se permite solo el acceso a las direcciones MAC pertenecientes a los equipos propios se impedirá que algún sistema externo pueda conectarse de forma accidental o premeditada. Sin embargo, hay que hacer notar que existen tarjetas de red que permiten el cambio de la dirección MAC, y en ese caso sería posible para un atacante de nuestra red, asignarle una dirección válida de alguno de nuestros equipos y evitar esta medida de seguridad. No obstante para ello, el atacante,

debería conocer la dirección MAC de alguno de nuestros equipos, lo cual si las medidas de seguridad física e informática están correctamente implementadas no resultará fácil.

2.3.5.6. Uso de direcciones IP estáticas

No un problema real para un hacker con conocimientos, peor si dificulta el acceso a intrusos ocasionales. Es habitual tener en las redes Wi-Fi la asignación automática de direcciones IP, Gateway y DNS. La práctica de asignar las direcciones manualmente a los terminales inalámbricos tiene la ventaja de que el atacante ha de averiguar en primer lugar los datos de la red, y más importante, nos permite habilitar filtros de manera que solo las direcciones IP asignadas sean permitidas. En caso de que el atacante utilice alguna de las IP asignadas, eventualmente podrá ser detectado pues entrará en conflicto con los terminales legales.

2.3.5.7. VLAN

Son propias para la red Wi-Fi. Es interesante la implementación, en aquellos equipos que lo permitan, de una VLAN específica para la red Wi-Fi. Al ser una red insegura por su propia naturaleza, es recomendable mantenerla separada en todo momento de la red cableada. Así pues, si el punto de acceso, o el controlador asociado, es capaz de gestionar VLAN’s, mantener el tráfico proveniente de la red Wi-Fi en una VLAN distinta permitirá implementar mecanismos de seguridad y acceso suplementarios que controlen el acceso de los usuarios Wi-Fi a los datos de la red corporativa.

2.3.5.8. Firewall

Relacionado con el punto anterior, el acceso de los clientes Wi-Fi a la red cableada debería ser gestionado por un Firewall, ya sea actuando de puente entre las correspondientes VLAN’s o como elemento físico de control, interponiéndose en flujo de tráfico Wi-Fi. En cualquier arquitectura, la inclusión de un firewall nos permitirá implementar políticas de acceso seguras y complejas que aseguren que,

aunque algún intruso hubiera conseguido conectarse a la red inalámbrica, no progrese hasta tener acceso a datos sensibles.

2.3.6. Tipos de ataques

GOMEZ, Álvaro (Internet; 6/10/2009; 25/10/2011; 10h30) "A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema".

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

2.3.6.1. Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.
- Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

2.3.6.2. Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesetas en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesetas en la cuenta B".
- Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

2.3.7. Mecanismos de control de acceso

BARRACHINA, Segio (Internet; 1999; 25/10/2011; 11h00) "El mecanismo de control de acceso se usa en el acceso a los objetos e indica la forma en que puede llevarse a cabo. Los componentes básicos de estos mecanismos son entidades, objetos y derechos de acceso. Los derechos de acceso delimitan los privilegios, las

condiciones y la manera como las entidades pueden acceder a los objetos. Por norma general, los sistemas actuales disponen de las herramientas necesarias para determinar estos derechos de acceso, aunque por razones prácticas suele generalizarse el acceso por agrupaciones de objetos".

REBAZA, Jorge (Internet; 22/11/2009; 25/10/2011; 11h00) "Las compañías de hoy en día, y en general cualquier organización, tienen diversos tipos de recursos de carácter privado y hasta de súper secretos que necesitan asegurar, sólo ciertas personas pueden acceder y para ello se necesita asegurar de que estas personas/usuarios deseados tengan el nivel de acceso requerido para lograr sus tareas. El control de acceso es más que simplemente requerir nombres de usuario y las contraseñas cuando los usuarios quieren acceder a los recursos. En el presente post se presenta un documento breve pero conciso que ilustra lo relacionado a los modelos y técnicas estándares para control de acceso".

MARTINEZ, Martha (Internet; 2000; 24/10/2011; 10h00) "Control de un sistema de información especializado en detectar los intentos de acceso, permitiendo el paso de las entidades autorizadas, y denegando el paso a todas las demás. Involucra medios técnicos y procedimientos operativos. Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos".

Es el control de un sistema de información especializados en detectar los intentos de acceso, permitiendo el paso de las entidades autorizadas y denegando el paso a las entidades no autorizadas. Involucrando medios técnicos y procedimientos operativos.

2.3.7.1. WEP

Características y funcionamiento

ANALUISA, Juan (2006, Pág. 61) "Wired Equivalent Privacy, (equivalencia de privacidad inalámbrica) es un protocolo de seguridad estipulado en el estándar para Wi-Fi IEEE 802.b diseñado para proveer una red de área local inalámbrica

con un nivel de seguridad comparable con el que usualmente se espera en un red alambrada."

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

FLUHRER, Scott; MANTIN, Itsik; SHAMIR, Adi (Internet, 31/07/2001; 4/10/2011,16h00) El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente, figura 2.10:

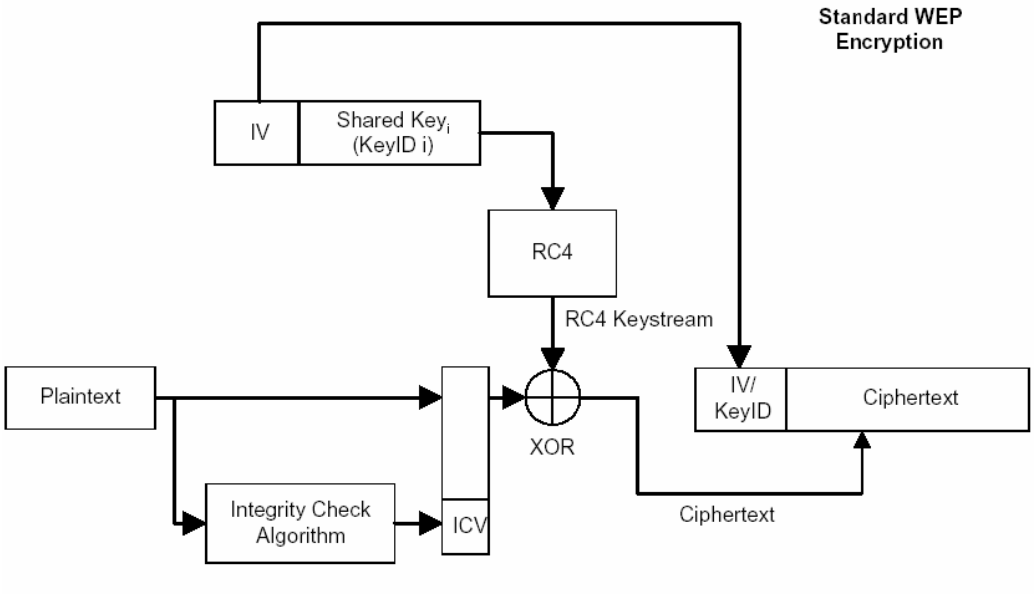

Figura 2.10: Algoritmo de encriptación WEP

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).
2. Se concatena la clave secreta a continuación del IV formado el seed.
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (framebody) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32), figura 2.11. A continuación se comprobara que el CRC-32 es correcto.

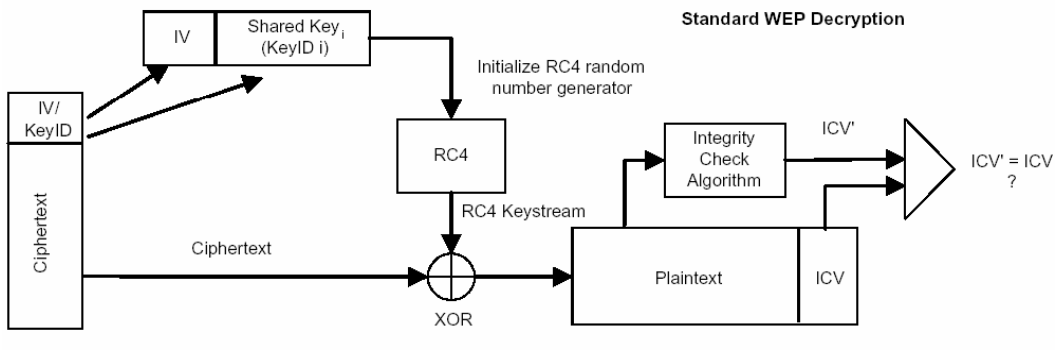

Figura 2.11: Algoritmo para descifrar la clave WEP

2.3.7.2. WAP

WONG, Stanley (Internet 20/05/2003; 01/10/2011, 8:10) WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

IEEE 802.1X.

Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA.

(Authentication Authorization Accounting) Como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el

punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso.

EAP

EAP, definido en la RFC, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).

TKIP

(Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.

MIC

(Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

Modos de funcionamiento de WPA

ROSER, Ken (Internet 18/04/2002; 02/10/2011, 13h00) WPA puede funcionar en dos modos:

Con servidor AAA, RADIUS Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad

Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso.

Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.4. Hipótesis

La implementación de un sistema de control de acceso influirá en las seguridades de las redes inalámbricas del Gobierno Provincial de Tungurahua.

2.5. Señalamiento de variables de la hipótesis

Variable independiente

Sistema de control de acceso.

Variable dependiente

Redes inalámbricas.

CAPITULO III

3. METODOLOGIA

3.1. Enfoque

La investigación tiene un enfoque cualitativo porque presenta las siguientes características: Los sistemas utilizados para el control de acceso a las redes inalámbricas del Gobierno Provincial de Tungurahua, se han convertido en sistemas obsoletos ya que se ha podido evidenciar las diferentes vulnerabilidades que presentan estos mecanismos de seguridad y no garantizan la integridad de la información. Y se maneja dentro de un ámbito participativo porque se mantendrá un contacto con el personal involucrado en la administración de las redes.

La investigación también presenta enfoque cuantitativo porque se basan en normativas de la empresa que permitirán determinar adecuadamente el problema. Es nomotética porque está orientado a la consecución de los resultados para satisfacer un solo fin, los resultado son manejados por el investigador y las decisiones serán tomadas desde un ámbito técnico, dentro de un contexto tangible y estable.

3.2. Modalidad básica de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad de campo: Se efectuara una investigación de campo ya que el escenario donde se realiza la investigación es el Consejo Provincial de Tungurahua, y se puede tomar contacto en forma directa con todos los funcionarios de la institución y así poder obtener información primaria directamente de los involucrados a través de una encuesta.

Modalidad bibliográfica o documentada: Se ha recopilado información de libros, revistas, tesis, con el propósito de recopilar toda la información pertinente para el estudio del problema, para poder profundizar y deducir diferentes enfoques, teorías, conceptualizaciones y criterios de diversos autores sobre el tema de investigación.

Modalidad experimental: Se ha considerado la relación de la variable independiente, Sistema de control de acceso y su influencia y relación con la variable dependiente, Redes inalámbricas del Gobierno Provincial de Tungurahua, para considerar sus causas y sus efectos.

3.3. Nivel o tipo de investigación

Se ha tomado la investigación exploratoria, ya que ha permitido focalizar el problema que se encuentra en el Gobierno Provincial de Tungurahua para lo cual hemos planteado el tema: Sistema de control de acceso para garantizar la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua. Como de la misma manera ayudo a plantear la hipótesis: La implementación de un sistema de control de acceso influirá en las seguridades de las redes inalámbricas del Gobierno Provincial de Tungurahua.

También nos hemos valido de la investigación descriptiva, ya que ha permitido realizar la contextualización, el análisis crítico y poder tener una mejor relación con el tema planteado.

Así mismo se ha planteado la investigación correlacional ya que hemos relacionado la variable independiente; Sistema de control de acceso, con la variable dependiente; Redes inalámbricas del Gobierno Provincial de Tungurahua.

3.4. Población y muestra

Para la presente investigación se ha tomado toda la población. La población a investigarse está conformada por la totalidad de los funcionarios del Gobierno Provincial de Tungurahua que utilizan las redes inalámbricas.

APELLIDOS	NOMBRES
CALLEJAS NARANJO	SILVIA MARIA
BARKLAY CALDERON	MYRIAN CECILIA
SANGUIL PORTERO	JOSE JOAQUIN
MARCIAL HERNANDEZ	MARTHA ALICIA
SOLIS GUTIERREZ	MARIA FERNANDA
GALLEGOS MOYA	NARCISA ALEJANDRA
PEÑA LOPEZ	MARCO BOLIVAR
PAZMIÑO VARGAS	MYRIAN SUSANA
ROSALES ALBAN	MARA EUGENIA
FRUTOS LEON	ALVARO ANTONIO
RODRIGEZ RIVAS	NEUN SALVATORI
MAYORGA PEREZ	FAUSTO GONZALO
PANGOL TORRES	NIKOLAY ALBERTO
ANDRADE PIEDRA	CARLA MONSERRAT
CAMPAÑA FREIRE	RITTA MARIBEL
ROSERO	MANUEL
LOPEZ VELASTEGUI	OLGA CECILIA
COBO MENDEZ	CRISTOBAL ABELARDO
LOZADA ANDALUZ	ROSARIO JEANETH
PANGOL TORRES	NIKOLAY ALBERTO
PAZMIÑO PAZMIÑO	YOLANDA BEATRIZ
ROBAYO JACOME	SANDRA MARIA
CHUGCHILAN ARROBO	MICHAEL ALADINO
ACUÑA GONZALEZ	SUSANA MAGDALENA
DAVILA PROAÑO	LIGIA FERNANDA
CATUTA SISA	MARTHA FABIOLA
QUINTANA GUERRA	SANDRA PATRICIA
ANDRADE ESPIN	MARCO ANTONIO
HIDALGO ABRIL	PABLO JAVIER
PAREDES RUIZ	MONICA ELIZABETH
VACA FALCONI	GLORIA SUSANA
SANGUIL VILLACIS	JOSE PATRICIO
SANTANA FREIRE	CARLOS MARCELO
MONTESDEOCA CRUZ	MARTHA YOLANDA
VELASTAGUI GALLEGOS	ELVIA PIEDAD
BARREZUETA BERMEO	VICTOR FELIX
GALLARDO BASTIDAS	BEATRIZ HERMINIA
MONTERO TAMAYO	VICTORIA ADELINA
MARAÑON GARCES	CONSUELO

CARRILLO SILVA	ENITH NERETHIA
ORTEGA SEVILLA	ROSA MARIA
BATALLAS	ANA
ULLAURI RIOS	MANUEL
MALIZA GOMEZ	MARIA ROSARIO
JACOME BARONA	WALTER ROBERTO
ORTEGA TOAPANTA	JOSE MARIA
ZAMORA CARRILLO	NELSON ROBERTH
MARTINEZ MAÑAY	JOSE LUIS
CAIZA NARANJO	RAMON SOFONIAS
MORA PROAÑO	MARIO VINICIO
PORTERO GAVILANEZ	IRMA FABIOLA
AROSTIGUI RODRIGEZ	DANILO EDUARDO
CASTELLANOS	MARIA EULALIA
RUBIO	GIOVANNY
SANCHEZ SANCHEZ	CARLOS OSWALDO
LALAMA HERDOIZA	ELVIA PIEDAD
AREVALO GARCES	BOLIVAR NAPOLEON
ALTAMIRANO CISNEROS	RAUL GEOVANNY
GUTIERREZ SALAZAR	JOSE MARCELO
VARGAS LOPEZ	RODRIGO ERNESTO
VELASTEGUI MEDINA	ABDON EMILIO
ESPINOZA VALENCIA	EDUARDO RAFAEL
ALVARADO GALARZA	CHRISTIAN ROBERTO
CACERES TERAN	IVAN CARLOS
HINOJOSA NUÑEZ	MERCEDES HIPATIA
LASLUISA AIMACAÑA	LUIS ARTURO
LOPEZ PAREDES	GLADYS ELENA
ACOSTA FIALLOS	JESSICA MARGARITA
PAREDES SANDOVAL	OLGA PATRICIA
ORTIZ BETANCOURT	SILVIA JACQUELINE
NARANJO LLANGA	GLORIA ELENA
ROSERO CAZAR	SORAYA GABRIELA
VILLACRES CAZAR	LUWINN RINZO
VILLACRES BORJA	MARIA EULALIA
BUCHELI BARONA	LUIS ERNESTO
ALVARADO TRICERRI	EDITH NANINA
MORETA VILLENA	SEGUNDO WILLIAN
VASCONEZ PROAÑO	LUIS ENRIQUE
JIMENEZ BRAVO	JUAN CARLOS
NARANJO PROAÑO	BEKER GIOVANNY
ALMEIDA LEMA	VINICIO FABIAN
GUZMAN PROAÑO	EDISON IVAN
PAREDES SARABIA	JUAN HUGO
MERA RAMOS	VICTOR FABIAN
MARIÑO RODRIGUEZ	IBAN HERBERTO
JACOME CEPEDA	LUIS FELIPE

TOAPANTA ULLOA	JORGE ANIBAL
GUACHIMBOZA VILLALBA	MARCO VINICIO
BRAVO MONCAYO	LUIS ALBERTO
TOALOMBO	MARCELO

Tabla 3.1: Listado de los usuarios de la red inalámbrica

3.5. Operacionalización de variables

Variable Independiente: Sistema de control de acceso				
Conceptualización	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
Es un sistema de seguridad de información especializada en la detención de accesos.	Sistemas de Seguridad	• Protección por contraseña WEP • Protección por contraseña WAP/WAP2 • Protección por contraseña desconozco el tipo de cifrado • Filtrado por dirección MAC	¿Qué nivel de seguridad utiliza las redes inalámbricas del Gobierno provincial de Tungurahua para garantizar una conexión segura?	Encuesta a través de cuestionarios al departamento de sistemas
			¿Regularmente se hacen test o auditorias de seguridad a la red inalámbrica a la red inalámbrica del Gobierno Provincial de Tungurahua?	Encuesta a través de cuestionarios al departamento de sistemas
			¿Existen políticas de seguridad inalámbrica implementadas en el Gobierno Provincial de Tungurahua?	Encuesta a través de cuestionarios al departamento de sistemas
	Acceso	• Acceso controlado • Acceso libre	¿Qué tipo de acceso utiliza las redes inalámbricas del Gobierno Provincial de Tungurahua para garantizar la integridad de la información?	Encuesta a través de cuestionarios al departamento de sistemas

Variable Dependiente: Redes inalámbricas				
Conceptualización	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
Una red inalámbrica es la comunicación entre dispositivos de tecnología inalámbrica y medios físicos en base a radio frecuencia. con el propósito de compartir información.	Señal de radio	• Señal excelente • Señal media • Señal regular • No hay señal	¿La señal que percibe su estación de trabajo en la red inalámbrica del Gobierno Provincial de Tungurahua es?	Encuesta a través de cuestionarios los usuarios de las redes inalámbricas del Gobierno Provincial de Tungurahua.
		• Excelente • Buena • Regular • Mala • Deficiente	¿Cómo calificaría la velocidad de conexión de las redes inalámbricas del Gobierno Provincial de Tungurahua?	Encuesta a través de cuestionarios los usuarios de las redes inalámbricas del Gobierno Provincial de Tungurahua.
	Información	• Perdida de información • Robo de información • Ninguna	¿Ha tenido problemas con la red inalámbrica del Gobierno Provincial de Tungurahua?	Encuesta a través de cuestionarios los usuarios de las redes inalámbricas del Gobierno Provincial de Tungurahua.
			¿Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua han recibido capacitación en el uso adecuado y los peligros de la tecnología de red inalámbrica?	Encuesta a través de cuestionarios al departamento de sistemas
	Comunicación	• Comunicación segura • Comunicación insegura	¿Le parece segura la conexión de la red inalámbrica del Gobierno Provincial de Tungurahua?	Encuesta a través de cuestionarios los usuarios de las redes inalámbricas del Gobierno Provincial de Tungurahua.

3.6. Recolección de información

Información Secundaria	Información Primaria
Se recolecta de estudios realizado anteriormente que reposan en tesis de grado. Se encuentra registrada en documentos y materiales impresos como libros, tesis de grado. Las fuentes de información son: bibliotecas, hemerotecas, internet.	Se recolecta la información directamente de los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua

Tabla 3.4: Recolección de la información

Técnicas de Investigación	
Bibliográficas	**De Campo**
El análisis de documentos a través de la lectura científica.	Permite recolectar información primaria: La encuesta La observación
Recolección de la información	
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis.
2. ¿A qué personas o sujetos?	A los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua.
3. ¿Sobre qué aspectos?	Variable Independientes: Sistema de control de acceso. Variable Dependiente: Redes

	inalámbricas del Gobierno Provincial de Tungurahua
4. ¿Quién?	Investigador
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de la información?	Gobierno Provincial de Tungurahua
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnicas de recolección?	Encuesta
9. ¿Con que?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiana

Tabla 3.5: Técnica de investigación

3.7. Procesamiento y análisis

- Revisión y codificación de la información
- Categorización y tabulación de la información
    - Tabulación Manual
- Análisis de los datos.
    - La presentación de los datos se lo hará a través de gráficos cuadros para analizar e interpretarlos.
- Interpretación de los resultados.
    - Describir los resultados
    - Analizar la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla.
    - Estudiar cada uno de los resultados por separado
    - Redactar una síntesis general de los resultados

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En el siguiente capítulo se presenta la tabulación de las preguntas realizadas a los usuarios de las redes inalámbricas y a los administradores de red del Gobierno Provincial de Tungurahua.

Interpretación de resultados de los usuarios de la red inalámbrica.

1. ¿La señal que percibe su estación de trabajo en la red inalámbrica del Gobierno Provincial de Tungurahua es?

N°	Indicadores	Frecuencia	Porcentaje
1	Señal excelente	75	83.3%
2	Señal media	15	16.7%
3	Señal regular	0	0%
4	No hay señal	0	0%
	Total	90	100%

Tabla 4.1: Tabulación pregunta 1

Fuente: Gobierno Provincial de Tungurahua

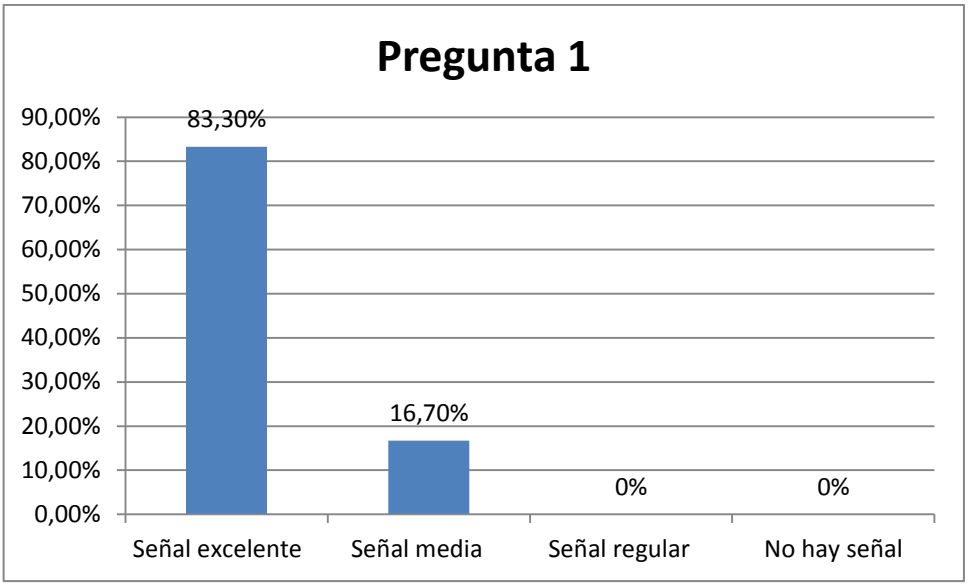

Figura 4.1: Grafico porcentual - Pregunta 1

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua, 75 que corresponden al 83.3% indican que la señal percibida es excelente y 15 usuarios que corresponden al 16.7% indican que la señal percibe su estación de trabajo es media.

2. ¿Cómo calificaría la velocidad de conexión de las redes inalámbricas del Gobierno Provincial de Tungurahua?

N°	Indicadores	Frecuencia	Porcentaje
1	Excelente	54	60,0%
2	Buena	34	33,3%
3	Regular	2	6,7%
4	Mala	0	0%
5	Deficiente	0	0%
	Total	90	100%

Tabla 4.2: Tabulación pregunta 2

Fuente: Gobierno Provincial de Tungurahua

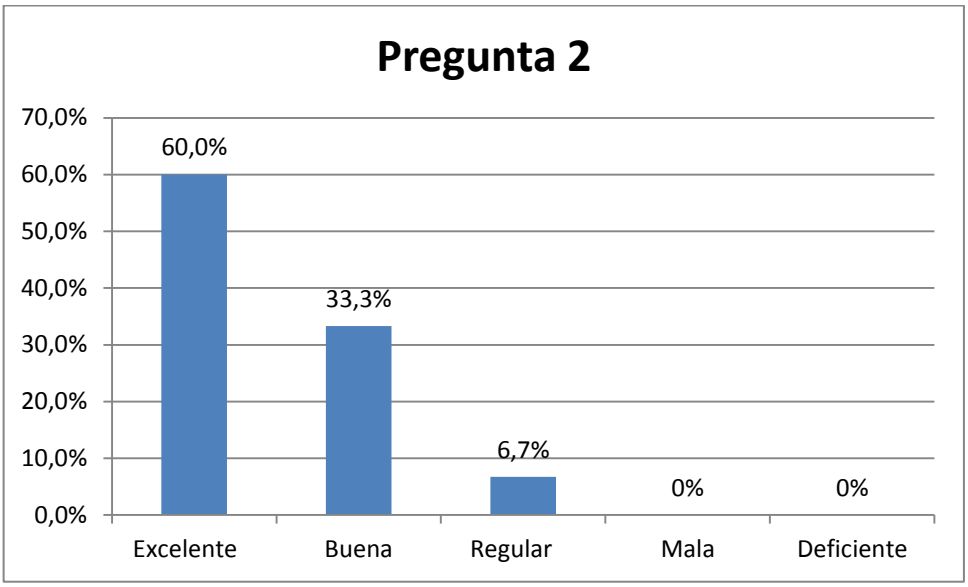

Figura 4.2: Grafico porcentual - Pregunta 2

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua, 54 que corresponden al 60% indican que la velocidad de la red es excelente, 34 usuarios que corresponden al 33.3% indican que la que la velocidad de la red es buena y 2 que corresponden al 6.7% indican que la velocidad de la red es regular.

3. ¿Ha tenido problemas con la red inalámbrica del Gobierno Provincial de Tungurahua?

N°	Indicadores	Frecuencia	Porcentaje
1	Perdida de información	12	13,3%
2	Robo de información	10	11,1%
3	Ninguna	68	75,6%
	Total	90	100%

Tabla 4.3: Tabulación pregunta 3

Fuente: Gobierno Provincial de Tungurahua

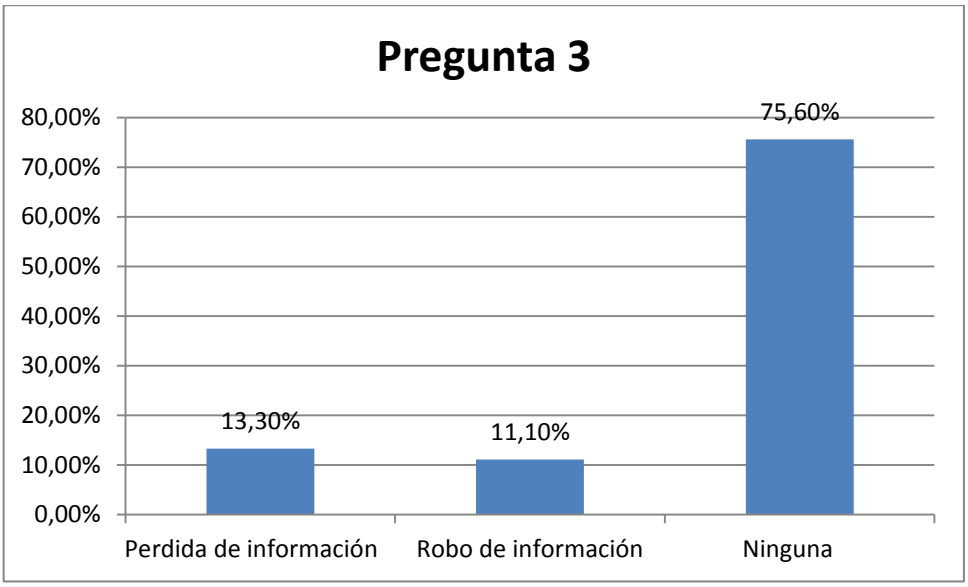

Figura 4.3: Grafico porcentual - Pregunta 3

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua, 12 que corresponden al 13.3% indican que han sufrido perdida de información, 10 usuarios que corresponde al 11.1% indican que han sufrido robo de la información y 68 usuarios que corresponden al 75.6% indican que no han tenido ningún problema con la red inalámbrica.

4. ¿Le parece segura la conexión de la red inalámbrica del Gobierno Provincial de Tungurahua?

N°	Indicadores	Frecuencia	Porcentaje
1	Si	21	23,3%
2	No	69	76,7%
	Total	90	100%

Tabla 4.4: Tabulación pregunta 4

Fuente: Gobierno Provincial de Tungurahua

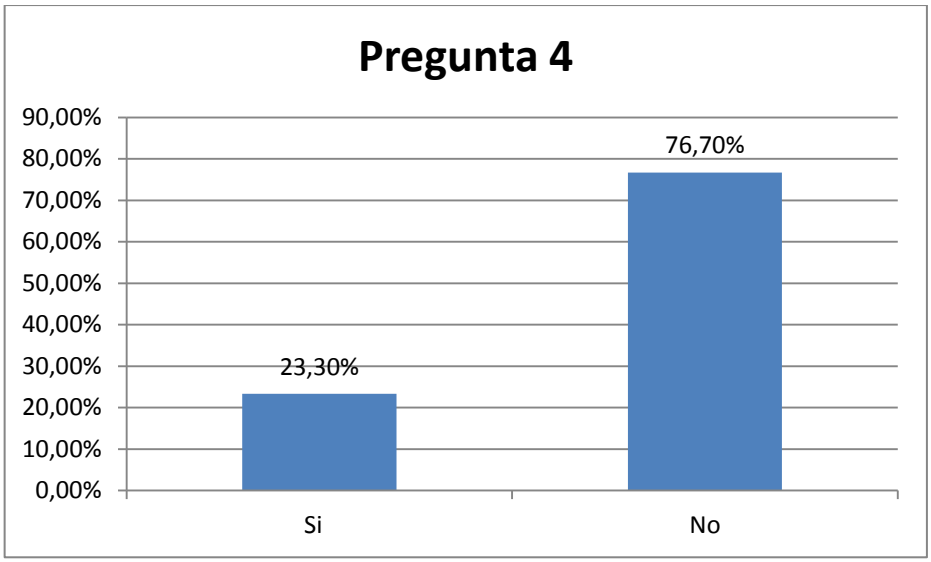

Figura 4.4: Grafico porcentual - Pregunta 4

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua, 21 que corresponden al 23.3% indican que les parece segura la conexión de la red inalámbrica del Gobierno Provincial de Tungurahua y 69 usuarios que corresponden al 76.7% indican que no le parece segura la conexión de la red inalámbrica del Gobierno Provincial de Tungurahua.

Interpretación de resultados del Departamento de Sistemas

1. ¿Qué nivel de seguridad utiliza las redes inalámbricas del Gobierno provincial de Tungurahua para garantizar una conexión segura?

N°	Indicadores	Frecuencia	Porcentaje
1	Protección por contraseña WEP	0	0%
2	Protección por contraseña WAP/WAP2	0	0%
3	Protección por contraseña desconozco el tipo de cifrado	0	0%
4	Filtrado por dirección MAC	3	100%
5	Desconozco	0	0%
	Total	3	100%

Tabla 4.5: Tabulación pregunta 1 - Administradores de red

Fuente: Gobierno Provincial de Tungurahua

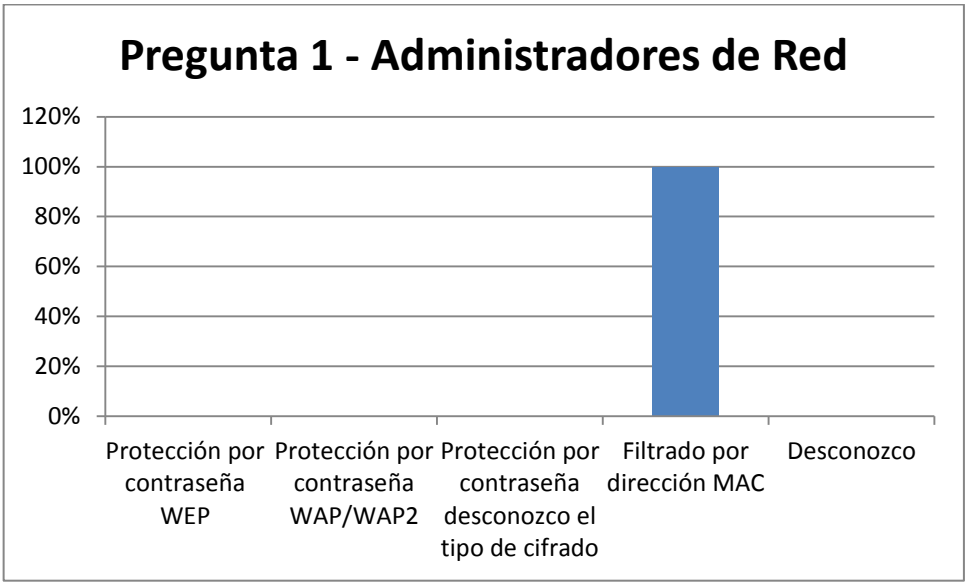

Figura 4.5: Grafico Porcentual - Pregunta 1 Administradores de Red

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua, 3 que corresponden al 100% indican que utilizan una seguridad de filtrado por dirección MAC.

2. ¿Qué tipo de acceso utiliza las redes inalámbricas del Gobierno Provincial de Tungurahua para garantizar la integridad de la información?

N°	Indicadores	Frecuencia	Porcentaje
1	Acceso libre	0	0%
2	Acceso controlado	3	100%
	Total	3	100%

Tabla 4.6: Tabulación pregunta 2 - Administradores de red

Fuente: Gobierno Provincial de Tungurahua

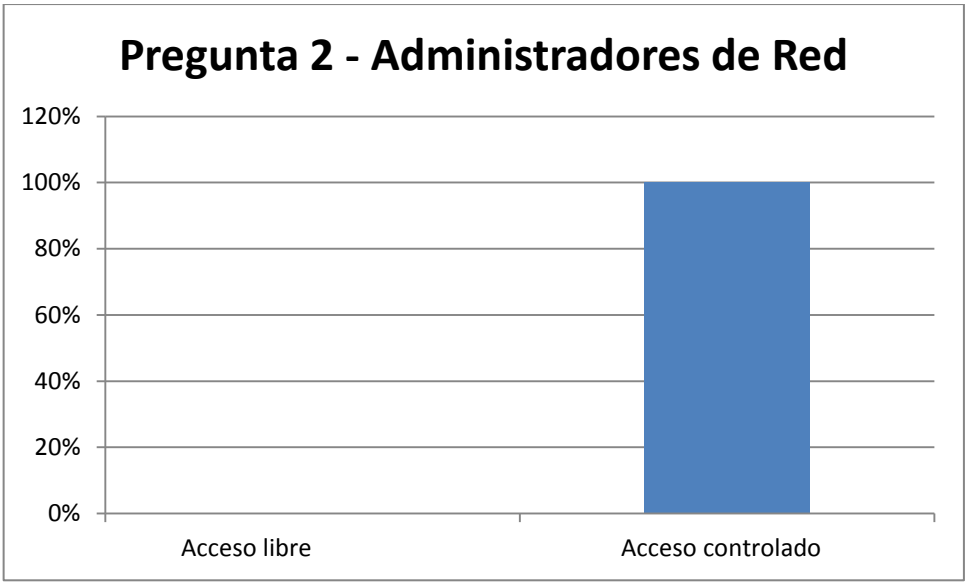

Figura 4.6: Grafico Porcentual - Pregunta 2 Administradores de Red

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua, 3 que corresponden al 100% indican que utilizan un acceso controlado a la red inalámbrica del Gobierno Provincial de Tungurahua.

3. ¿Regularmente se hacen test o auditorias de seguridad a la red inalámbrica del Gobierno Provincial de Tungurahua?

N°	Indicadores	Frecuencia	Porcentaje
1	Si	0	0%
2	No	3	100%
	Total	3	100%

Tabla 4.7: Tabulación pregunta 3 - Administradores de red

Fuente: Gobierno Provincial de Tungurahua

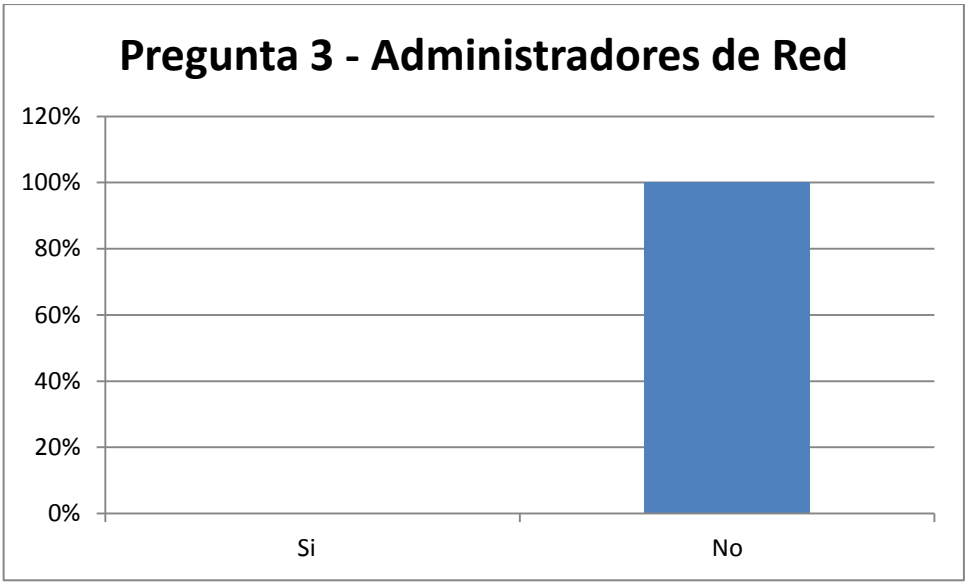

Figura 4.7: Grafico Porcentual - Pregunta 3 Administradores de Red

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua, 3 que corresponden al 100% indican que no realizan test o auditorias de seguridad a las red inalámbrica del Gobierno Provincial de Tungurahua.

4. ¿Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua han recibido capacitación en el uso adecuado y los peligros de la tecnología de red inalámbrica?

N°	Indicadores	Frecuencia	Porcentaje
1	Si	0	0%
2	No	3	100%
	Total	3	100%

Tabla 4.8: Tabulación pregunta 4 - Administradores de red

Fuente: Gobierno Provincial de Tungurahua

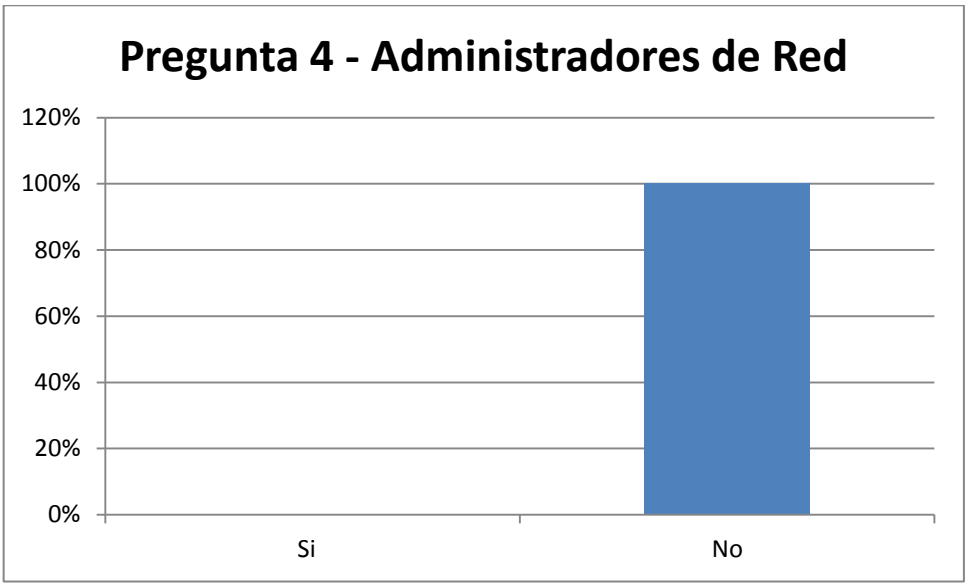

Figura 4.8: Grafico Porcentual - Pregunta 4 Administradores de Red

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua, 3 que corresponden al 100% indican que los usuarios de red inalámbrica del Gobierno Provincial de Tungurahua no han recibido capacitación en el uso adecuado y los peligros de la tecnología de red inalámbrica.

5. ¿Existen políticas de seguridad inalámbrica implementadas en el Gobierno Provincial de Tungurahua?

N°	Indicadores	Frecuencia	Porcentaje
1	Si	0	0%
2	No	3	100%
	Total	3	100%

Tabla 4.9: Tabulación pregunta 5 - Administradores de red

Fuente: Gobierno Provincial de Tungurahua

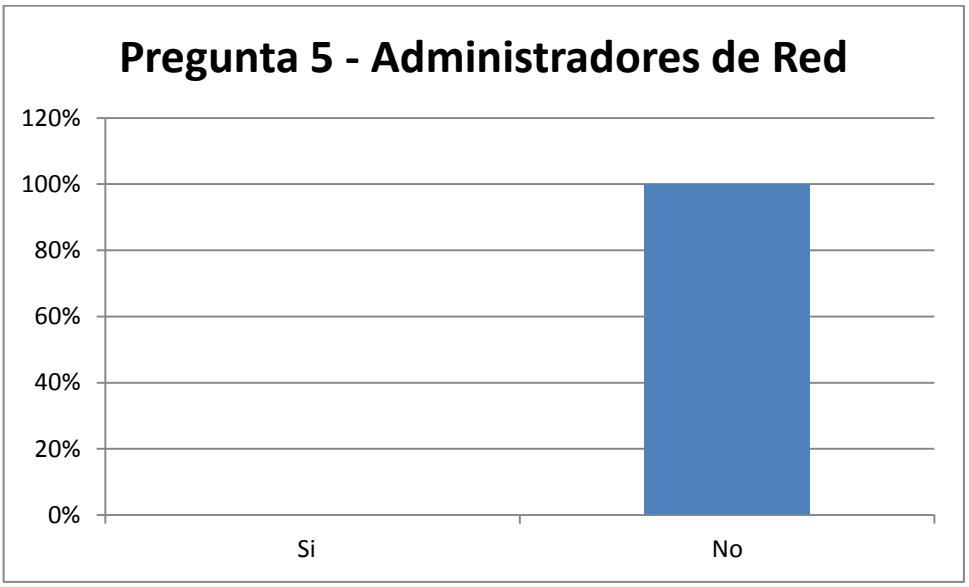

Figura 4.9: Grafico Porcentual - Pregunta 5 Administradores de Red

Fuente: Gobierno Provincial de Tungurahua

Interpretación:

Los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua, 3 que corresponden al 100% indican que no existen políticas de seguridad inalámbrica implementadas en el Gobierno Provincial de Tungurahua.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se utilizo la encuesta como instrumento de recolección de datos y se dirigió a toda la población ya que se ha considerado factible realizarlo y así poder obtener resultados verdaderos y poder verificar el estado de seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua.
- Las encuestas estuvieron dirigido a dos tipos de usuarios de la red inalámbrica: los usuarios comunes y los administradores de la red, debido al nivel de conocimiento de cada tipo de usuario y así poder realizar las preguntas pertinentes a los dos tipos de usuarios.
- Considerando los resultados obtenidos en las encuestas realizadas a los administradores de red, se pudo percatar que el nivel de seguridad implementado en las redes inalámbricas del Gobierno Provincial de Tungurahua es mínimo.
- La seguridad que utilizan actualmente en las redes inalámbricas del Gobierno Provincial de Tungurahua es el filtrado de direcciones MAC, siendo este uno de los métodos de protección de redes inalámbricas más primitivo y menos eficaz que existen porque se han encontrado diferentes métodos para poder vulnerar esta seguridad.

- En el departamento de sistemas del Gobierno Provincial de Tungurahua no cuenta con políticas de seguridad en cuanto a la transmisión de datos por medio de las redes inalámbricas, haciendo vulnerables a diversos tipos de ataques informáticos.

5.2. Recomendaciones

- Las preguntas deben ser realizadas en base a los conocimientos de cada tipo de usuario para poder evitar la recolección de datos erróneos. Por lo que, para este caso se realizaron dos tipos de encuestas, una para los usuarios comunes de la red y otra para los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua.
- Se recomienda verificar si el Gobierno Provincial de Tungurahua dispone del equipamiento tecnológico, las herramientas necesarias y la aprobación de las personas involucradas en el proyecto, antes de empezar a realizar la investigación y no exista ningún motivo ni razón que justifique un mal desarrollo del proyecto.
- Se recomienda realizar capacitaciones al personal que usa y administra las redes inalámbricas del Gobierno Provincial de Tungurahua para que se mantenga al tanto de los diversos tipos de ataques y vulnerabilidades que presenta esta tecnología.
- Se debe establecer políticas de seguridad para proteger los datos durante la transmisión, mediante el cifrado de la comunicación para desalentar a los usuarios no autorizados mediante autenticación de usuarios e impedir conexiones fraudulentas mediante la eliminación de puntos de acceso falsos o dudosos. Dando a los usuarios de la red la suficiente confianza que sus datos se transmitan de forma segura e integra.

CAPITULO VI

6. PROPUESTA

6.1. Datos Informativos

Tema: Sistema de control de acceso para garantizar la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua.

Ubicación:

Provincia: Tungurahua

Cantón: Ambato

Parroquia: La Matriz

Lugar: Gobierno Provincial de Tungurahua

Investigador: Edisson Israel Yungán Muzo

Investigados: Usuarios de red inalámbrica del Gobierno Provincial de Tungurahua.

Tutor: Ing. René Terán

6.2. Antecedentes de la propuesta

El Gobierno Provincial de Tungurahua cuenta con una red inalámbrica en sus instalaciones debido a la facilidad de conexión que presenta esta tecnología pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar el acceso de intrusos o la intercepción de la información.

La seguridad implementada en la red inalámbrica del Gobierno Provincial de Tungurahua es por filtrado MAC, como ya se comento es unas de las típicas soluciones que se presentan para asegurar la red, pero este tipo de seguridad van siendo obsoletas y vulnerables.

Por lo que nace la necesidad de implementar un sistema de control de acceso en las redes inalámbricas del Gobierno Provincial de Tungurahua que determine los permisos de acceso apropiados a un determinado usuario dependiendo de sus privilegios establecidos y así evitar que personas no autorizadas o indeseables tengan la libertad de acceder a la red inalámbrica.

6.3. Justificación

La implementación de un sistema de control se acceso a las redes inalámbricas del Gobierno Provincial de Tungurahua se ha convertido en una necesidad debido a que la seguridad que se utiliza en la red inalámbrica es por filtrado de MAC que hace vulnerable a la red por tener varias desventajas. Un usuario no autorizado que este dentro del área de cobertura del punto de acceso podrá conectarse a la red con el solo hecho de cambiar su MAC por una que se encuentre registrada en el punto de acceso. Para cambiar la MAC de una máquina ahora se lo hace de formas muy sencillas debido a la gran cantidad de herramientas que existen para ello.

El sistema de control de acceso permitirá acceder solo a usuarios autorizados ya que trabaja en base a certificados digitales y claves compartidas que darán un

mayor nivel de seguridad a la red inalámbrica del Gobierno Provincial de Tungurahua.

6.4. Objetivos

6.4.1. Objetivo General

Implementar un sistema de control de acceso para garantizar la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua.

6.4.2. Objetivos Específicos

- Diseñar un sistema de control de acceso.
- Determinar las herramientas informáticas a utilizar.
- Desarrollar el sistema de control de acceso.
- Ejecutar pruebas del sistema de control de acceso a las redes inalámbricas.
- Implementar el sistema de control de acceso a las redes inalámbricas.

6.5. Análisis de factibilidad

6.5.1. Factibilidad técnica

Para la implementación de un sistema de control de acceso el Gobierno Provincial de Tungurahua se cuenta con el suficiente equipamiento tecnológico, dentro del cual utilizamos un servidor, un punto de acceso y el software necesario para realizar el proyecto sin ningún inconveniente.

6.5.2. Factibilidad operativa

El software utilizado para la implementación de un sistema de control de acceso a las redes inalámbricas del Gobierno Provincial de Tungurahua es libre por lo que no tendrá ningún costo.

6.5.3. Factibilidad legal

En la presente propuesta no existe impedimento legal para desarrollarla.

6.5.4. Factibilidad económica

El Gobierno Provincial de Tungurahua como es una institución pública los recursos económicos se establece en un presupuesto al comienzo del año y por lo tanto tiene la disponibilidad para desarrollar sin ningún inconveniente, pues esta asegura que la consecución del objetivo es viable.

6.6. Fundamentación

6.6.1. Software Libre

Software Libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software tal como fue concebido por Richard Stallman. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

- Libertad para ejecutar el programa en cualquier sitio, con cualquier propósito y para siempre.
- Libertad para estudiarlo y adaptarlo a nuestras necesidades. Esto exige el acceso al código fuente.
- Libertad de redistribución, de modo que se nos permita colaborar con vecinos y amigos.
- Libertad para mejorar el programa y publicar las mejoras. También exige el código fuente.

Estas libertades se pueden garantizar de acuerdo con la legalidad vigente por medio de una licencia. En ella se plasman las libertades, pero también restricciones compatibles con ellas, como dar crédito a los autores originales si redistribuimos. Incluso puede obligarnos a que los programas ajenos mejorados por nosotros también sean libres, promoviendo así la creación de más software libre.

6.6.1.1. Reseña histórica

Es en el MIT (Masachussets Institute of Technology), por los años 50, que aparecen los primeros programadores. Aunque lejos de buscar entrar por la fuerza en las bases de datos de los organismos oficiales, los hackers realizan su pasatiempo de forma legal, buscando ante todo sacar partido del potencial de los grandes computadores de la universidad. Es en ese medio fértil que nacerá más tarde la Free Software Foundation (FSF), el origen del software libre.

En los años 70, la comunidad de ingenieros y de investigadores del MIT había tomado el hábito de compartir el código fuente de sus programas, considerando la compra del computador como más importante que la propiedad del software. Richard Stallman quien llega al laboratorio de Inteligencia Artificial (AILab) del célebre instituto, quien más tarde fundará la FSF se forma en esta tradición. Lo que no parece ser el caso de los otros dos estudiantes de la universidad vecina Harvard, Bill Gates y Paul Allen, fundadores de Microsoft.

A algunos edificios de distancia del laboratorio de Stallman, los dos amigos escriben en 1975 un sistema operativo para la Altair 8800, una máquina grande con un arreglo de botones rojos por todo sistema de visualización (dispositivo de salida), ya se utilizaba el procesador Intel 8080.

Conforme a las costumbres de la época, alguien copia los programas y los distribuye a través de todo el campus universitario. Entonces Bill Gates monta en cólera y lanza "una carta abierta" en la prensa estudiantil local. En esta carta entre otras cosas dice "la mayor parte de ustedes roban sus programas (entre sí). Eso hace que no se molesten en escribir buenos programas. Quien puede permitirse realizar un trabajo profesional por nada". Es la forma de mostrar su indignación el joven de aquel entonces. Más tarde Gates, lanzará su MS Basic, prohibiendo efectuar copias, aún parciales o destinadas al uso personal. Nace así el modelo Microsoft, fundamentado sobre el pago de royalties y sobre la venta de software protegido por una licencia que prohíbe la copia entre usuarios y que exige el pago de royalties. Pero que no se responsabiliza por la calidad, ni por los daños que ese

software pueda hacerle a sus datos y que transfiere al usuario la responsabilidad por el uso del mismo.

De su lado, en el campus del MIT, Richard Stallman decide retomar la bandera de la tradición universitaria. En 1984, lanza el proyecto GNU, se escoge este nombre porque es el nombre más extraño que Stallamn encuentra en el diccionario, pero también porque se trata de un acronismo recursivo que resume de la mejor manera el programa que se fijó su creador "GNU's not Unix" (GNU no es Unix).

En su inicio el proyecto tenía por objetivo crear un Unix libre de derechos. Pero para concebir un sistema como este falta todavía disponer de un ambiente viable. Stallman se propone por misión crear los programas fundamentales para el futuro sistema operativo (compiladores, herramientas de desarrollo, editores de texto, etc.).

El año siguiente, Stallman da el siguiente paso y funda la Free Software Foundation (FSF), destinada a darle soporte (a sostener) el desarrollo de programas libre (Software Libre).

A él le debemos la pieza jurídica maestra del modelo del software libre, la licencia GPL o "GNU General Public License" el contrato de licencia sobre el que reposa la mayor parte del software libre.

6.6.1.2. GNU/LINUX

En 1991, en Helsinki, Linus Torvalds comenzó un proyecto que más tarde llegó a ser el núcleo Linux. Esto fue al principio un emulador terminal, al cual Torvalds solía tener acceso en los grandes servidores UNIX de la universidad. Él escribió el programa expresamente para el hardware que usaba, e independiente de un sistema operativo, porque quiso usar las funciones de su nueva computadora personal con un procesador 80386. Este es aún el estándar de hoy. El sistema operativo que él usó durante el desarrollo fue Minix, y el compilador inicial fue el GNU C compiler, que aún es la opción principal para compilar Linux hoy, él tarde o temprano comprendió que había escrito

un núcleo de sistema operativo. El 25 de agosto de 1991, 20:57:08 GMT, anunció este sistema en un envío a la red Usenet, en el newsgroup (grupo de noticias).

Después de muchas discusiones, él finalmente admitió que Linux era simplemente el mejor nombre. En el código original de la versión 0.01 de Linux, el nombre Freax fue, sin embargo, usado en el makefile. Sólo después fue usado el nombre Linux. Así el nombre, en realidad, no planificado en absoluto se hizo generalmente aceptado por todo el mundo.

6.6.1.3. Distribución CentOS

CentOS 5.5 (Community ENTerprise Operating System) es una distribución Linux de clase empresaria libremente ofrecida al público. Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de las fuentes de Red Hat.

CentOS usa yum para bajar e instalar las actualizaciones, herramienta también utilizada por Fedora

- La primera versión de CentOS llamada CentOs 3 build4-rc0, fue lanzada a finales de 2003. CentOS 3.1 fue lanzada el 19 de marzo de 2004.
- CentOS 2 (basado en la versión 2.1 de Red Hat Enterprise Linux) fue lanzada el 14 de mayo de 2004.
- CentOS 4.0, (basado en la versión 4 de Red Hat Enterprise Linux) fue lanzada el 1 de marzo de 2005 para arquitecturas i386 y IA-64.
- CentOS 5.5 (basado en la versión 5 de Red Hat Enterprise Linux) fue lanzada el 12 de abril de 2007.

6.6.2. Web Server Apache

Apache es en la actualidad el principal servidor de web. Es el más rápido, eficiente y el que evoluciona a mayor velocidad. Y Apache, por su naturaleza de software abierto, es ideal para instalar en máquinas GNU/Linux, que aseguran un S.O. con unas comunicaciones excelentes. Apache y GNU/Linux es una combinación que se está utilizando en el mundo empresarial, Apache ha ayudado a que el campo de GNU/Linux se amplíe de forma muy sólida en el mundo Internet, creando una Internet-box que difícilmente puede ser superada por otra plataforma en los sistemas actuales, tanto en coste como en potencia.

6.6.2.1. Características

- Soporte para los lenguajes perl, python, tcl y PHP.
- Módulos de autenticación: mod_access, mod_auth y mod_digest.
- Soporte para SSL y TLS.
- Permite la configuración de mensajes de errores personalizados y negociación de contenido.
- Permite autenticación de base de datos basada en SGBD.

6.6.2.2. Configuración del Servidor

Los ficheros de configuración de Apache se buscan por defecto dentro del directorio "/etc/httpd/conf" aunque esto es algo configurable. Allí deben de estar presentes los ficheros:

- httpd.conf: fichero principal de configuración de Apache.
- srm.conf: fichero de definición del espacio de nombres que los usuarios ven del servidor de web. En este fichero también se especifica donde se encuentran los cgi-bin, los iconos, el tipo de documento por defecto, como se responde ante los errores, que fichero es el índice dentro de un directorio, donde está la página personal de los usuarios del sistema.

- access.conf: fichero de control de acceso global a los datos del servidor de web. En él se especifica los permisos de accesos a directorios, ficheros y URLs dentro del servidor, así como diferentes configuraciones.
- mime.types: fichero de control de los tipos MIME que son enviados al cliente en función de la extensión del fichero.

6.6.2.3. Proyectos Asociados

Hay muchos proyectos asociados a Apache cuyo objetivo es aumentar su funcionalidad. Desde aquí vamos a destacar dos de ellos: uno muy útil para los desarrolladores, conocido como PHP, y otro orientado a la privacidad de las comunicaciones, Apache-SSL.

6.6.2.3.1. PHP

En la programación de aplicaciones en Internet, son importantes las herramientas de programación que se utilizan tanto en el lado del cliente, como del servidor. El usuario puede haber utilizado lenguajes como Javascript, JScript, o VBScript del lado del cliente, para aumentar la funcionalidad de las páginas HTML. De forma similar, hay lenguajes de programación del lado del servidor, que se introducen dentro de las páginas HTML.

En el servidor de web Apache, un lenguaje de programación que se puede embeber en las páginas HTML se conoce como PHP. Es un lenguaje similar a Perl, y muy sencillo de utilizar. Es un lenguaje en constante desarrollo, y cuya principal característica es que proporciona una librería de funciones que permite acceder a las principales bases de datos del mercado (Adabas, Ilustra de Informix, Oracle, MySQL, PostgresSQL entre muchas otras), lo que facilita mucho la integración del web con el mundo de las bases de datos.

PHP en la actualidad ha alcanzado la versión 5.0, y en cada nueva versión se aumenta su funcionalidad. Es un lenguaje muy potente en la programación del lado del servidor, y que sustituye de forma elegante a la programación de cgi-bin.

6.6.2.3.2. Apache SSL

El comercio electrónico es el campo que va a arrastrar a Internet con más fuerza, y es uno de los sectores con mayores perspectivas de futuro. En la actualidad, el único freno al comercio electrónico en Internet es la seguridad, o la falta de ella.

Debido al gran interés que hay, se están desarrollando rápidamente estándares que aseguran la seguridad en Internet, en especial, dentro del web. Apache-SSL presenta nuevas características de seguridad, como son la encriptación y la autenticación.

6.6.3. Certificados digitales

Uno de los problemas al usar servicios online es la falta de seguridad del medio tanto para proteger las transferencias de datos como para asegurar la identidad del usuario. Por estos motivos, se lanzó el concepto de certificado digital. Un sistema que permite vincular datos electrónicos con personas físicas a través de una entidad certificadora.

6.6.3.1. Definición

Un certificado digital es un documento otorgado por una autoridad de certificación que garantiza la asociación de una persona física con una firma digital.

6.6.3.2. Características

Un Certificado Digital con las características de seguridad necesarias, debe utilizar las más modernas y estables metodologías que la criptografía pueda ofrecer. Es por ello que internacionalmente se acepta a la criptografía asimétrica como la metodología más adecuada para la generación de un certificado digital.

Por esta razón un certificado digital está compuesto de un par de claves:

Clave Privada: La posee únicamente su dueño. También se la llama también porción privada y junto con la clave pública conforma un par de claves único.

Clave Pública: Esta es llamada también porción pública y es publicada en la web por la autoridad de certificación, después de ser aprobada por esta. Para aprobar un certificado digital, la autoridad de certificación firma con su clave privada la clave pública del certificado digital (no necesita conocer la clave privada del certificado digital para hacer esto).

Las Claves Privada y Pública conforman un par único.

Recuerde que el par de claves es generado por el usuario en su propio computador pues bien cuando la Autoridad de Certificación recibe y firma la clave pública del usuario utilizando su propia clave privada convierte al par de claves en un certificado digital.

6.6.3.3. Clases de certificado digital

Los certificados pueden ser clasificados según qué medios hayan sido utilizados para verificar la veracidad de los datos.

Clase 0: Se utilizan para probar el procedimiento de firma digital. Son gratuitos y pueden bajarse de diferentes sitios por ejemplo: www.certificadodigital.com.ar.

Clase 1: Certifican que la persona que posee el certificado es quien dice ser, y que la dirección de correo electrónico está bajo su control. Para cerciorarse la identidad de la persona la autoridad de registro solicita un documento que lo acredite.

Clase 2: Certifican que la persona que posee el certificado es quien dice ser, y que la dirección de correo electrónico está bajo su control. Para cerciorarse la identidad de la persona, la autoridad de registro requiere que el solicitante se presente con documentación de identificación oficial en el ámbito nacional.

Con cualquiera de las clases de certificado nombradas anteriormente pueden firmarse los mensajes de correo electrónico.

6.6.3.4. Órgano licenciante

Es el organismo del Estado que habilita a una Empresa de Certificación Digital como Autoridad de Certificación.

6.6.3.5. Entidad auditora

Es la entidad que ha sido designada para efectuar la auditoría y control de la Autoridad de Certificación.

6.6.3.6. Autoridad de certificación

La Autoridad de Certificación es responsable de brindar las herramientas para poder emitir, con calidad técnica y de manera segura e irrepetible por otros medios o en otras circunstancias, el par de claves, pública y privada, que constituye el eje del certificado, así como de :

- Aprobar o rechazar las solicitudes generadas por la autoridad de registro.
- Poner a salvo su propia clave privada que es la que utiliza para aprobar las solicitudes.
- Garantizar la calidad técnica del sistema informático.
- Proveer el libre y fácil acceso a las listas y directorios de claves públicas para la verificación de firmas emitidas por la misma.
- Publicar las claves públicas que ha aprobado y las revocaciones de certificados digitales que ha realizado.

La potestad para emitir certificados digitales le es concedida por el órgano licenciante y la calidad del servicio es controlada por una entidad auditante.

6.6.3.7. Autoridad de registro

La autoridad de registro es responsable de realizar la identificación de la persona física o jurídica en forma fehaciente y completa, debe efectuar los trámites con fidelidad a la realidad. Además es quien se encarga de solicitar la aprobación, y/o

revocación de un certificado digital. Su objetivo primario es asegurarse de la veracidad de los datos que fueron utilizados para solicitar el certificado digital.

Requerimientos de seguridad necesarios para el intercambio de documentos Digitales:

- Autentificación: Identificar al emisor y el receptor en un intercambio de documentación.
- Integridad: Se debe poder asegurar que el documento digital no ha sido alterado.
- Confidencialidad: Sólo el emisor y el receptor pueden acceder al contenido del documento digital.
- No Repudio: No puede negarse la participación en un intercambio de información o transacción.

6.6.3.8. Criptografía

Es la ciencia que se ocupa de la escritura secreta.

Si la clave de cifrado es igual a la clave de descifrado hablaremos de criptografía simétrica, por el contrario si las claves de cifrado y de descifrado son diferentes hablaremos de criptografía asimétrica.

6.6.3.8.1. Criptografía simétrica

Es aquella que usa para cifrar una clave igual a la usada para descifrar.

Define un conjunto de métodos que permiten efectuar una comunicación segura entre un emisor y un receptor una vez que se ha consensuado una clave secreta, con la cual se cifrará el mensaje en el origen y se descifrará en el destino.

- Ventajas: Gran velocidad de cifrado y descifrado.
- Desventajas: El emisor debe enviar la clave Secreta por algún medio seguro al receptor.

6.6.3.8.2. Criptografía asimétrica

Es aquella que usa para cifrar una clave diferente a la usada para descifrar.

Provee métodos que permiten efectuar una comunicación segura entre un emisor y un receptor utilizando dos claves diferentes por cada uno, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada.

Una clave pública se corresponde con una única clave privada. En la práctica no puede hallarse una clave privada utilizando la clave pública, pues requiere un tiempo de computación absolutamente descomunal aun para los más grandes supercomputadores.

Ejemplo: José quiere enviar un mensaje confidencial a María. Para ello José cifrará el mensaje con la clave pública de María. María al recibir el mensaje los descifrará con su propia clave privada. No hay forma de descifrar el mensaje sin tener la clave privada de María.

- Ventajas: La clave de cifrado no es igual a la de descifrado, por lo tanto puede ser conocida públicamente. No es necesario efectuar ningún intercambio de clave de descifrado.
- Desventajas: Requiere mayor potencia de cómputo para cifrar y descifrar que el método simétrico.

6.6.3.9. Cifrado

Para cifrar un documento digital se utiliza la clave pública de la persona que recibirá el documento digital cifrado. El proceso de cifrado se hace notablemente más lento cuanto más grande es el documento digital que se cifra, o cuanto más grande es la clave pública que se utiliza (512 bits, 1024, 2048, etc.).

Tengamos en cuenta que una clave pública se corresponde con una única clave privada. En la práctica no puede hallarse una clave privada utilizando la clave pública, pues requiere un tiempo de computación absolutamente descomunal.

6.6.3.10. Firma digital

Para firmar digitalmente un documento digital se utiliza la clave privada del certificado digital. El proceso de firma es rápido y puede ser usado con grandes volúmenes de datos sin observarse un decrecimiento importante de la velocidad del computador.

Después de firmarse un documento digital puede verificarse su integridad usando la clave pública correspondiente a la clave privada usada para firmar. El proceso de firma consiste en cifrar una cadena de texto llamada digesto, que es confeccionada utilizando funciones que resumen un texto a una cadena de caracteres de longitud fija predeterminada.

6.6.4. Secure Sockets Layer SSL

SSL (Secure Sockets Layer) traducido al español significa Capa de Conexiones Seguras. Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet. Recientemente ha sido sustituido por TLS (Transport Layer Security) el cual está basado en SSL y son totalmente compatibles.

Permite confiar información personal a sitios web, ya que tus datos se ocultan a través de métodos criptográficos mientras navegas en sitios seguros.

Es utilizado ampliamente en bancos, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas. No todos los sitios web usan SSL, por eso se debe ser cuidadoso.

6.6.4.1. Funcionamiento

SSL/TLS es una tecnología compleja, pero una vez entendidos los conceptos anteriores se comprenderá el funcionamiento de este protocolo de forma general. Usemos un ejemplo para poder explicarlo:

Supongamos que se intenta acceder al sitio de Facebook de forma segura, es decir, usando “https” en la dirección web. Inmediatamente, aparecerá la página en pantalla y en alguna parte de tu navegador observarás un “candado”, dependiendo del navegador que use, figura 6.1. Si no aparece ningún mensaje de advertencia (generalmente en tonos rojos), el protocolo SSL/TLS ha hecho su trabajo.

Figura 6.1: Uso de protocolo HTTPS

SSL/TLS funciona de forma transparente para el usuario, lo que en realidad ocurre cuando se intenta acceder a un sitio seguro se asemeja al siguiente diagrama de la figura 6.2.

Figura 6.2: Funcionamiento general de SSL/TLS

Iniciando comunicación segura

En el punto dos de la figura 6.2, cuando el navegador hace una petición al sitio seguro de Facebook, éste envía un mensaje donde indica que quiere establecer una conexión segura y envía datos sobre la versión del protocolo SSL/TLS que soporta y otros parámetros necesarios para la conexión.

En base a esta información enviada por el navegador, el servidor web de Facebook responde con un mensaje informando que está de acuerdo en establecer la conexión segura con los datos de SSL/TLS proporcionados.

Una vez que ambos conocen los parámetros de conexión, el sitio de Facebook presenta su certificado digital al navegador web para identificarse como un sitio confiable.

Verificación de validez del certificado

Una vez que el navegador tiene el certificado del sitio web de Facebook, realiza algunas verificaciones antes de confiar en el sitio:

- Integridad del certificado: Verifica que el certificado se encuentre íntegro, esto lo hace descifrando la firma digital incluida en él mediante la llave pública de la AC y comparándola con una firma del certificado generada en ese momento, si ambas son iguales entonces el certificado es válido.
- Vigencia del certificado: Revisa el periodo de validez del certificado, es decir, la fecha de emisión y la fecha de expiración incluidos en él.
- Verifica emisor del certificado: Hace uso de una lista de Certificados Raíz almacenados en la computadora y que contienen las llaves públicas de las ACs conocidas y de confianza.

Con base a esta lista, el navegador revisa que la AC del certificado sea de confianza, de no serlo, el navegador mostrará una advertencia indicando que el certificado fue emitido por una entidad en la cual no confía.

Estableciendo la conexión segura

Una vez que el certificado cumplió con todas las pruebas del navegador, se establece la conexión segura al sitio de Facebook, lo cual se traduce en seguridad para tus valiosos datos personales.

6.6.5. Domain Name System DNS

Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos. El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul V. Mockapetris publicó los RFC 882 y RFC 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno. (Estos RFCs han quedado obsoletos por la publicación en 1987 de los RFCs 1034 y RFC 1035).

Componentes

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio).
- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
- Y las Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

6.6.6. Dynamic Host Configuration Protocol DHCP

DHCP (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Este protocolo se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131. Para DHCPv6 se publica el RFC 3315.

Asignación de direcciones IP

Cada dirección IP debe configurarse manualmente en cada dispositivo y, si el dispositivo se mueve a otra subred, se debe configurar otra dirección IP diferente.

El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si fuera el caso en el dispositivo es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- Asignación manual o estática: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.
- Asignación automática: Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- Asignación dinámica: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

6.6.7. Mysql Server

MySQL Database Server es la base de datos de código fuente abierto más usada del mundo. Su ingeniosa arquitectura lo hace extremadamente rápido y fácil de personalizar. La extensiva reutilización del código dentro del software y una aproximación minimalística para producir características funcionalmente ricas, ha dado lugar a un sistema de administración de la base de datos incomparable en velocidad, compactación, estabilidad y facilidad de despliegue. La exclusiva separación del core server del manejador de tablas, permite funcionar a MyQSL bajo control estricto de transacciones o con acceso a disco no transaccional ultrarrápido.

Características

Inicialmente, MySQL carecía de elementos considerados esenciales en las bases de datos relacionales, tales como integridad referencial y transacciones. A pesar de ello, atrajo a los desarrolladores de páginas web con contenido dinámico, justamente por su simplicidad.

Poco a poco los elementos de los que carecía MySQL están siendo incorporados tanto por desarrollos internos, como por desarrolladores de software libre. Entre las características disponibles en las últimas versiones se puede destacar:

- Amplio subconjunto del lenguaje SQL. Algunas extensiones son incluidas igualmente.
- Disponibilidad en gran cantidad de plataformas y sistemas.
- Posibilidad de selección de mecanismos de almacenamiento que ofrecen diferente velocidad de operación, soporte físico, capacidad, distribución geográfica, transacciones, etc.
- Transacciones y claves foráneas.
- Conectividad segura.
- Replicación.
- Búsqueda e indexación de campos de texto.

6.6.8. Hotspot

Un Hotspot, traducido del inglés al español como “punto caliente”, corresponde a un punto, generalmente ubicado en un lugar público, donde las personas pueden acceder a Internet en forma gratuita o de pago a través del sistema de Internet inalámbrico denominado Wi-Fi.

Los hotspots, como ya se mencionaba, por lo general, se ubican en lugares públicos, específicamente en bibliotecas, aeropuertos, cafeterías, hoteles, etc. y se configuran como zonas de cobertura Wi-Fi en el que uno o varios puntos de acceso prestan servicios de red a través de un WISP o Proveedor de Servicios de Internet Inalámbrico.

El sistema de acceso inalámbrico a Internet o Wi-Fi, que proviene de Inglés Wireless Fidelity, posee ciertas desventajas en comparación a los accesos a Internet que cuentan con conexión por cables, ya que por ejemplo, el primero, pierde velocidad debido a las interferencias y pérdidas de señal que puedan existir en el ambiente, pero la ventaja de poder conectarse a la Internet sin la necesidad de cables en espacios públicos y abiertos, compensa por lejos estos inconvenientes.

Como vemos, la existencia de este tipo de sitios, los hotspots, se configuran como lugares donde toda persona que cuente con un computador portátil o notebook puede conectarse a Internet y disfrutar de los beneficios de la navegación en la World Wide Web. De este modo, si no se cuenta con una conexión en el hogar, los hotspost son una buena solución para la revisión del correo electrónico, para realizar compras vía Internet o simplemente navegar por la red. Por otra parte, contar con este tipo de servicios en lugares como restaurantes o cafeterías permite a la gente que trabaja on-line, no desconectarse del trabajo, pudiendo trabajar en los momentos de descanso como en el almuerzo o el café de media mañana. Es por estos motivos que la implementación de hotspots se ha incrementado considerablemente durante el último tiempo.

Por otra parte, cada vez son más las personas que configuran su propio hotspot en el hogar, usando para esto un "router" (aquel aparato que recibe la señal de Internet por un cable y la convierte para uso inalámbrico). De esta manera, todos los miembros del hogar pueden conectarse a la Internet desde cualquier ubicación de la casa, usando computadoras portátiles, sin la necesidad de cables.

6.6.9. Servidor de autenticación

6.6.10. Servidor Radius

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP (Provedor de Servicio de Internet) mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP (Protocolo Punto a Punto), quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como 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.

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.

Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP (Protocolo compacto de acceso a directorios), bases de datos varias, etc. A menudo se utiliza SNMP (Protocolo Simple de Administración de Red) para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada.

6.7. Metodología

El diseño de la red inalámbrica del Gobierno Provincial de Tungurahua se encontraba implementada y funcionando correctamente y solo nos centraremos en el sistema de control de acceso a la red inalámbrica para establecer un nivel de seguridad aceptable dentro la institución.

El proyecto se realizó de forma independiente sin afectar el funcionamiento de la red interna, al terminar las configuraciones del servidor RADIUS se integro al sistema y se paso a realizar las pruebas correspondientes.

6.8. Modelo operativo

6.8.1. Análisis del sistema

El Gobierno Provincial de Tungurahua cuenta con un punto de acceso en el edificio principal, en el cual todos los funcionarios tienen acceso a la red. Este diseño viene funcionando hace un año atrás.

Los usuarios registrados son alrededor de noventa, los cuales utilizan el método de autenticación por MAC address, esto quiere decir que todas las MAC address se encuentran registradas en el punto de acceso.

La administración de la red inalámbrica se realiza por los ingenieros del departamento de sistemas.

6.8.2. Requerimientos

6.8.2.1. Hardware

Para realizar el sistema de control de acceso a las redes inalámbricas del Gobierno Provincia de Tungurahua se ocupó el mismo punto de acceso que existía, y como servidor un computador de escritorio con características superiores de hardware, que se detalla a continuación:

Servidor

- Intel Pentium 4
- Memoria RAM 2GB
- Disco duro de 120Gb
- Dos tarjetas de red

Access Point

El D-Link DWL-3200AP es un poderoso, robusto y fiable Access Point para operar en entornos de empresas con diversos negocios. Diseñado para instalaciones Indoor, 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.

Principales Características y Facilidades:

- Soporte de Multiples SSID's
- Soporte 11g, 108Mbps Modo Turbo
- Robusto Access Point para soluciones Indoor
- Soporte de PoE (Power over Ethernet)
- Soporte WEP
- Soporte WPA, AES y 802.11i
- Seguridad Ampliada, con soporte de ACL, 802.1x y MAC Address Filtering
- Administración versátil, vía D-Link D-View, SNMP v3, Web, Telnet y AP Manager.

6.8.2.2. Software

Para la implantación de un sistema de control de acceso a la red inalámbrica del Gobierno Provincial de Tungurahua se utilizo la distribución de CentOS 5.5 la herramienta perfecta para las aplicaciones de servidor. Podemos usar CentOS como servidor Web, servidor de correo, servidor de bases de datos o servidor de aplicaciones. CentOS incorpora todas las sofisticadas funcionalidades de compatibilidad con Windows incluidas en Red Hat Enterprise Linux. Podemos usar CentOS como controlador de dominios primarios o secundarios, o como servidor de clientes Windows basado en Samba. CentOS es también un sistema de escritorio Linux plenamente funcional. Y es distribución gratuita.

Todos los paquetes necesarios para la implementación del sistema de control de acceso son de distribución gratuita.

Un gran número de proveedores ofrecen servidores Radius Open Source como:

- FreeRADIUS
- OpenRadius
- Cistron
- IC-RADIUS

En este caso se eligió FreeRADIUS, que es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como módulos para soporte en apache, y lo que más nos interesa en este punto, un servidor de RADIUS.

Chillispot es el encargado de establecer la conexión con los clientes a través del access point y envía las credenciales de autenticación al servidor RADIUS para que valide a los usuarios en base a los registros de la base de datos.

Para la administración de los usuarios se utilizo el software DaloRadius el cual es de distribución gratuita y ofrece una administración completa del sistema de control acceso.

6.8.3. Sistema de control de acceso

El esquema básico del sistema de control de acceso a la red inalámbrica del Gobierno Provincial de Tungurahua es el que se muestra en la figura 6.3.

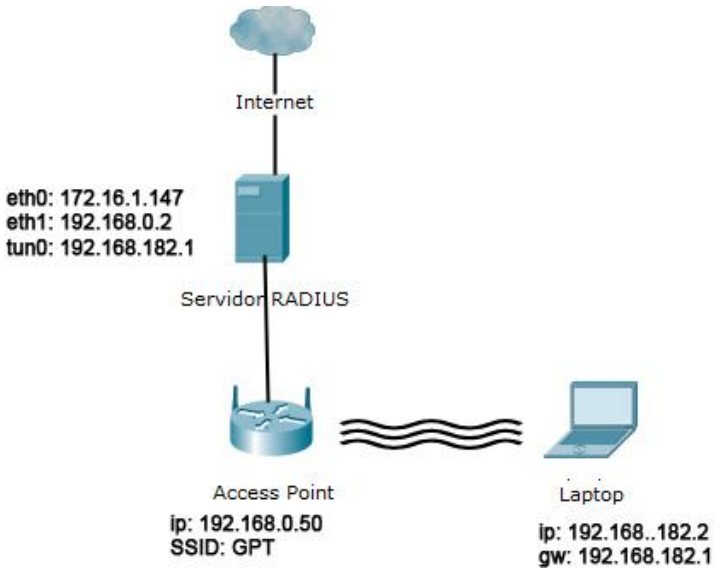

Figura 6.3: Esquema del sistema de control de acceso

6.8.3.1. Instalación del sistema operativo CentOS 5.5

Se comienza instalando CentosOS 5.5, arranca el sistema operativo como se indica en la figura 6.4, muestra la ventana de comprobación del CD de instalación como se indica en la figura 6.5, empieza la instalación en modo grafico como se indica en la figura 6.6, se elige el idioma que se utilizara para la instalación como se indica en la figura 6.7, a continuación se muestra la ventana de partición de disco duro y utilizamos todo el disco como se indica en la figura 6.8, asignamos la dirección IP al servidor como se indica en la figura 6.9, seleccionamos la región donde nos encontramos como se indica en la figura 6.10, asignamos una contraseña al root como se indica en la figura 6.11, seleccionamos todos los paquetes necesarios para la configuración como se indica en la figura 6.12, se muestra el progreso de instalación del sistema operativo como se indica en la figura 6.13, termina la instalación de CentOS como se indica en la figura 6.14.

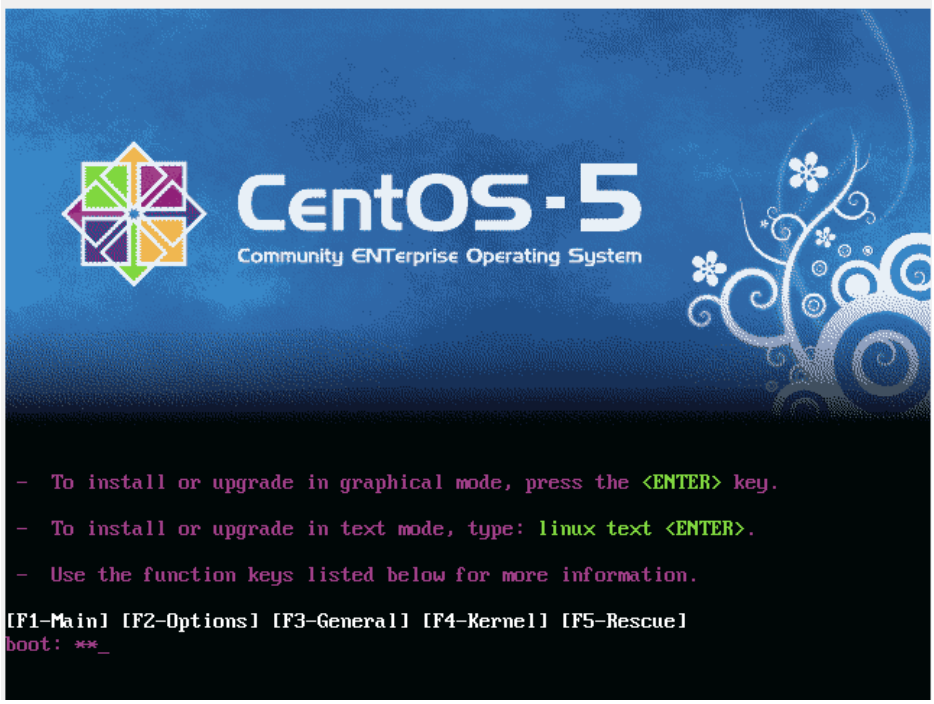

Figura 6.4: Arranque del sistema operativo

Figura 6.5: Comprobación del CD de instalación

Figura 6.6: Instalación en modo gráfico

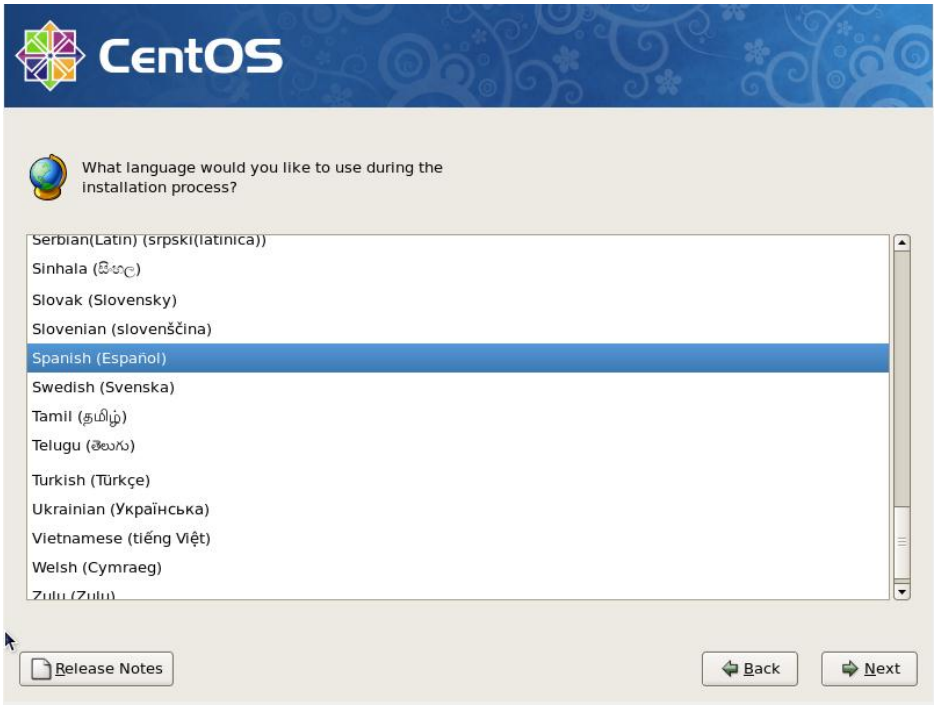

Figura 6.7: Elección de idioma para la instalación

Figura 6.8: Particion del disco duro

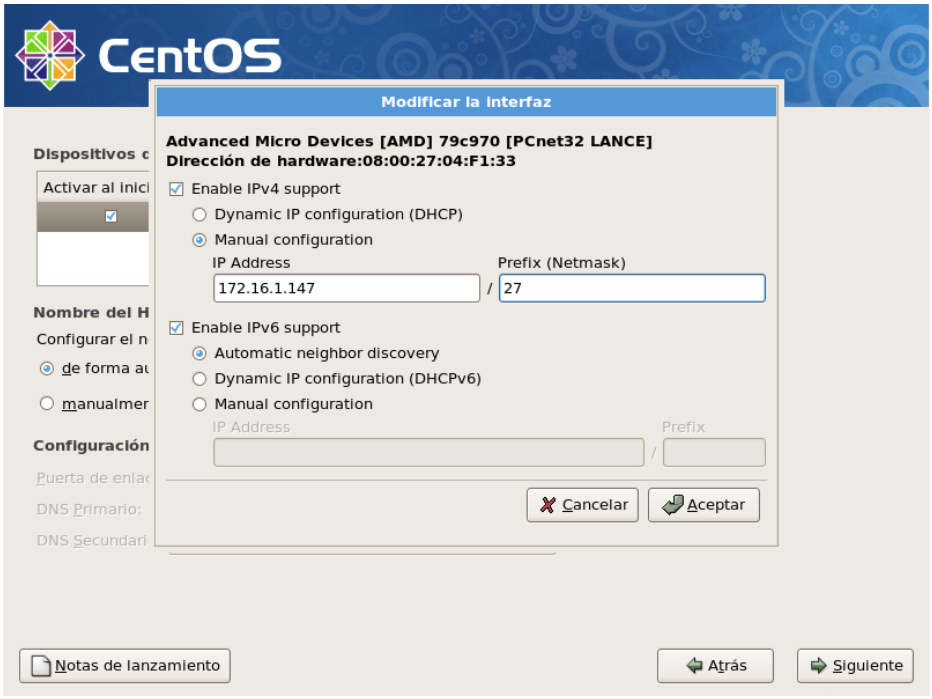

Figura 6.9: Direccionamiento IP

Figura 6.10: Selección de la región

Figura 6.11: Establecer contraseña del root

Figura 6.12: Selección de paquetes

Figura 6.13: Progreso de instalación

Figura 6.14: Instalación completa

6.8.3.2. Configuración de servicios y aplicaciones necesarias

Los paquetes y aplicaciones necesarios para realizar el sistema de control de acceso son los siguientes:

- Servidor Web Apache con soporte SSL
- Servidor Radius FreeRADIUS
- Servidor Mysql
- Chillispot
- DaloRadius
- Configuración de los Access Points

Se inicia verificando el direccionamiento IP de las dos tarjetas de rede que se encuentran en el servidor eth0 y eth1.

```
[root@gobierno ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0B:6A:98:DC:40
          inet addr:172.16.1.147  Bcast:172.16.1.159
Mask:255.255.255.224
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:209 Base address:0x4800

eth1      Link encap:Ethernet  HWaddr 00:E0:52:CB:D6:A3
          inet addr:192.168.0.2  Bcast:192.168.0.255
Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:201 Base address:0xc00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1798 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1798 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6405939 (6.1 MiB)  TX bytes:6405939 (6.1
MiB)
```

Como se puede observar se encuentran configurada correctamente las dos tarjetas de red, tanto eth0 como eth1, si se desea realizar algún cambio a la configuración se edita los siguientes archivos:

```
[root@gobierno ~]# nano /etc/sysconfig/network-
scripts/ifcfg-eth0

# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:0b:6a:98:dc:40
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
PEERDNS=yes
NETMASK=255.255.255.224
IPADDR=172.16.1.147
GATEWAY=172.16.1.129

[root@gobierno ~]# nano /etc/sysconfig/network-
scripts/ifcfg-eth1

# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:e0:52:cb:d6:a3
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
PEERDNS=yes
NETMASK=255.255.255.0
IPADDR=192.168.0.2
```

Se debe verificar que se disponga del modulo kernel TUN que crea un puente virtual de red y un enrutamiento para la conexión entre el cliente inalámbrico y el servidor.

```
[root@gobierno ~]# lsmod
Module                  Size  Used by
tun                    21441  0
vfat                   15937  1
fat                    51165  1 vfat
sg                     36573  0
usb_storage            81057  1
autofs4                29253  3
hidp                   23105  2
rfcomm                 42457  0
```

```
l2cap                  29505  10 hidp,rfcomm
bluetooth              53925  5 hidp,rfcomm,l2cap
lockd                  63337  0
sunrpc                146685  2 lockd
loop                   18761  0
dm_multipath           25421  0
```

Si el modulo TUN se muestra en la lista esta activado, y sino se encuentra en la lista se lo puede activar ejecutando el siguiente comando

```
[root@gobierno ~]# modprobe tun
```

Se procede a habilitar el renvió de paquetes entre las dos interfaces de red.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

También se lo puede realizar de siguiente editando el archivo **sysctl.conf,** cambiando el parámetro de net.ipv4.ip_forward a 1:

```
[root@gobierno ~]# nano /etc/sysctl.conf

# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See
sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
```

6.8.3.3. Instalación y configuración del servidor web Apache

Primero se comprueba si esta instalado el servidor web Apache:

```
[root@gobierno ~]# rpm -q httpd
httpd-2.2.3-43.el5.centos
```

Si en el caso que no se encuentre instalado se lo puede hacer directamente desde los repositorios.

```
yum -y httpd
```

Luego se configura el servidor web apache, editando el archivo httpd.conf donde se coloca la IP de la interfaz eth0 en la línea donde esta ServerName.

```
[root@gobierno httpd]# nano /etc/httpd/conf/httpd.conf

ServerName 172.16.1.147:80
```

Se levanta el servicio

```
[root@gobierno httpd]# service httpd start
Iniciando httpd:                           [  OK  ]
```

Para que inicie automáticamente al encender el servidor

```
[root@gobierno httpd]# chkconfig httpd on
```

Para comprobar que Apache funciona correctamente en el navegador colocamos la dirección IP de la interfaz eth0.

```
httpd://172.16.1.147
```

Si aparece la página web de Apache la configuración estará correctamente realizada.

6.8.3.3.1. Soporte SSL/TLS en el servidor web Apache

Se debe verificar que Apache tenga soporte para conexiones seguras a través de SSL, se puede chequear buscando el archivo **ssl.conf**

```
[root@gobierno ~]# ls /etc/httpd/conf.d/
auth_kerb.conf   daloradius.conf~  nss.conf
python.conf  webalizer.conf
auth_mysql.conf  gobierno.conf     perl.conf
README       welcome.conf
auth_pgsql.conf  gobierno.conf~    php.conf
squid.conf
authz_ldap.conf  manual.conf       proxy_ajp.conf
ssl.conf
```

Después se verifica que CentOS disponga de OpenSSl y mod_ssl esto permiten crear certificados digitales que pueden aplicarse al servidor Apache.

```
rpm –q openssl

openssl-0.9.8e-12.el5_4.6

rpm –q mod_ssl

mod_ssl-2.2.3-43.el5.centos
```

Si no se encuentran instalados se lo puede instalar de sus repositorios.

```
yum -y install openssl mod_ssl
```

Se procede a la creación del certificado digital que es el fichero digital intransferible y no modificable.

Se crea un directorio para almacenar los certificados digitales, este directorio para mayor seguridad solo debe ser accesible para el super-usuario.

```
[root@gobierno etc]# mkdir -m 700 -p
```

```
/etc/ssl/gobierno.ec
```

Creación de la clave publica RSA

```
[root@gobierno gobierno.ec]# openssl genrsa -des3 -out
server.key 1024
Generating RSA private key, 1024 bit long modulus
..++++++
....++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[root@gobierno gobierno.ec]# ls
server.key
[root@gobierno gobierno.ec]# openssl rsa -in server.key
-out server.pem
Enter pass phrase for server.key:
writing RSA key
[root@gobierno gobierno.ec]# ls
server.key  server.pem
```

Creación del certificado digital:

```
[root@gobierno gobierno.ec]# openssl req -new -key
server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that
will be incorporated
into your certificate request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some
blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
State or Province Name (full name)
[Berkshire]:Tungurahua
Locality Name (eg, city) [Newbury]:Ambato
Organization Name (eg, company) [My Company
Ltd]:Chulpi-soft
Organizational Unit Name (eg, section) []:Gobierno
Provincial
Common Name (eg, your name or your server's hostname)
[]:Rasta
Email Address []:snoweddi@yahoo.com

Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:clave
An optional company name []:rastalinux

[root@gobierno gobierno.ec]# ls
server.csr  server.key  server.pem
```

Firma del certificado digital por un periodo de 360 días:

```
[root@gobierno gobierno.ec]# openssl x509 -req -days
360 -in server.csr -signkey server.key -out server.crt
Signature ok
subject=/C=EC/ST=Tungurahua/L=Ambato/O=Chulpi-
soft/OU=Gobierno
Provincial/CN=Rasta/emailAddress=snoweddi@yahoo.com
Getting Private key
Enter pass phrase for server.key:

[root@gobierno gobierno.ec]# ls
server.crt  server.csr  server.key  server.pem
```

Se asegura que todos los archivos sean accesibles para el root:

```
[root@gobierno ~]# chmod 400
/etc/ssl/gobierno.ec/server.*
```

Luego se crea la estructura de directorios para el sitio que será creado como virtual en el servidor web.

```
mkdir -p /var/www/gobierno.ec/{cgi-

bin,html,logs,etc,var}
```

Se crea el archivo gobierno.conf dentro del directorio /etc/httpd/conf.d, con lo siguiente:

```
NameVirtualHost 172.16.1.147:80
      <VirtualHost 172.16.1.147:80>
            ServerAdmin root@gobierno.ec
            DocumentRoot /var/www/gobierno.ec/html
            ServerName www.gobierno.ec
            ServerAlias gobierno.ec
            Redirect 301 / https://www.gobierno.ec/
            CustomLog
/var/www/gobierno.ec/logs/access_log combined
            Errorlog /var/www/gobierno.ec/logs/error_log
      </VirtualHost>
NameVirtualHost 172.16.1.147:443
      <VirtualHost 172.16.1.147:443>
            ServerAdmin root@gobierno.ec
            DocumentRoot /var/www/gobierno.ec/html
            ServerName www.gobierno.ec
            ScriptAlias /cgi-bin/
/var/www/gobierno.ec/cgi-bin/
            SSLEngine on
            SSLCertificatefile
/etc/ssl/gobierno.ec/server.crt
            SSLCertificateKeyfile
/etc/ssl/gobierno.ec/server.pem
            SetEnvIf User-Agent ".*MSIE.*" nokeepalive
ssl-unclear-shutdown
            CustomLog
/var/www/gobierno.ec/logs/ssl request log \
            "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x
\"%r\" %b"
            CustomLog
/var/www/gobierno.ec/logs/ssl_access_log combined
            Errorlog
/var/www/gobierno.ec/logs/ssl_error_log
      </VirtualHost>
```

Por ultimo se debe reiniciar el servidor web apache, si arranca quiere decir que esta correctamente configurado.

```
service httpd restart
```

En las figuras se puede apreciar el correcto funcionamiento de una conexión segura a través de certificados digitales como se indican en las figuras 6.15, 6.16 y 6.17:

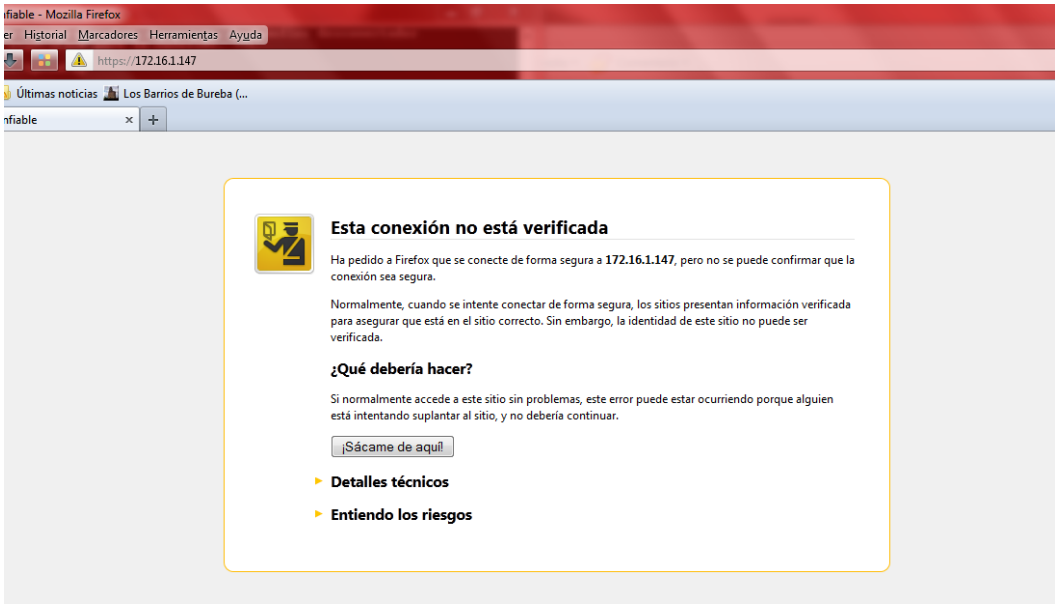

Figura 6.15: Conexión fallida

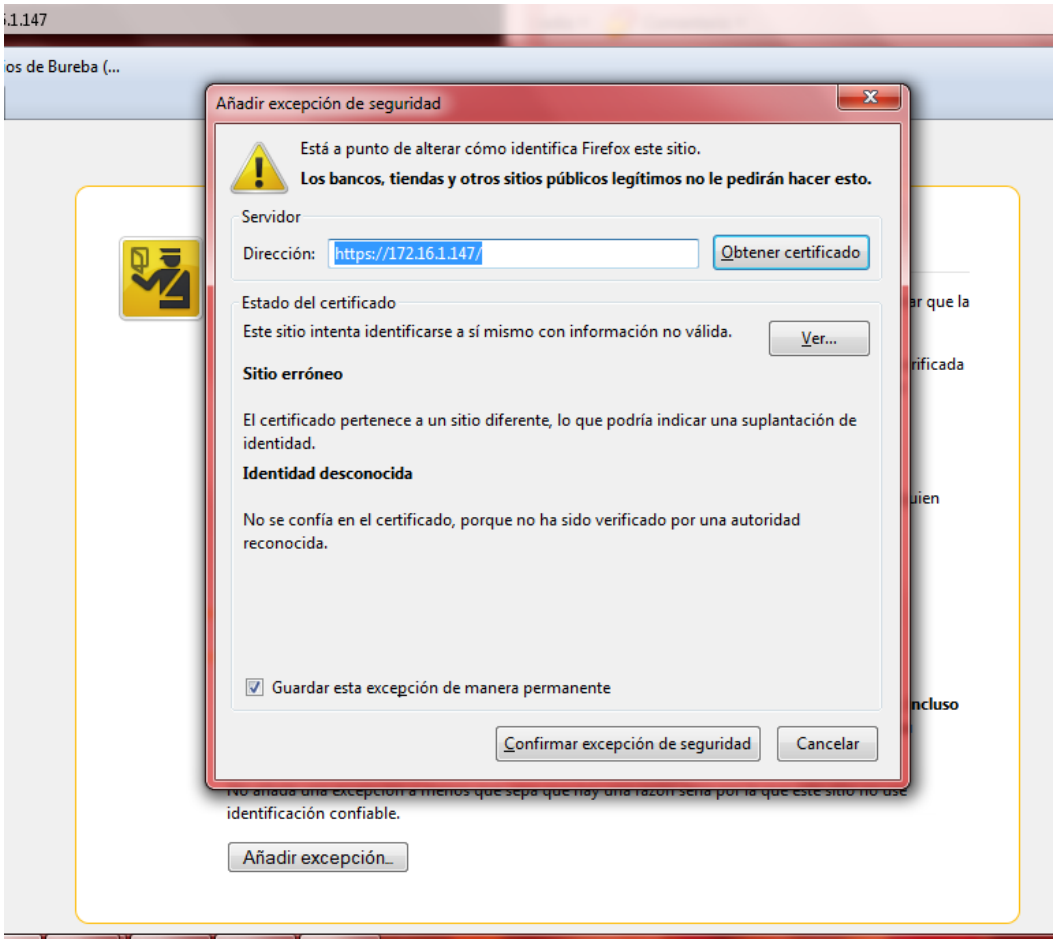

Figura 6.16: Obtención del certificado

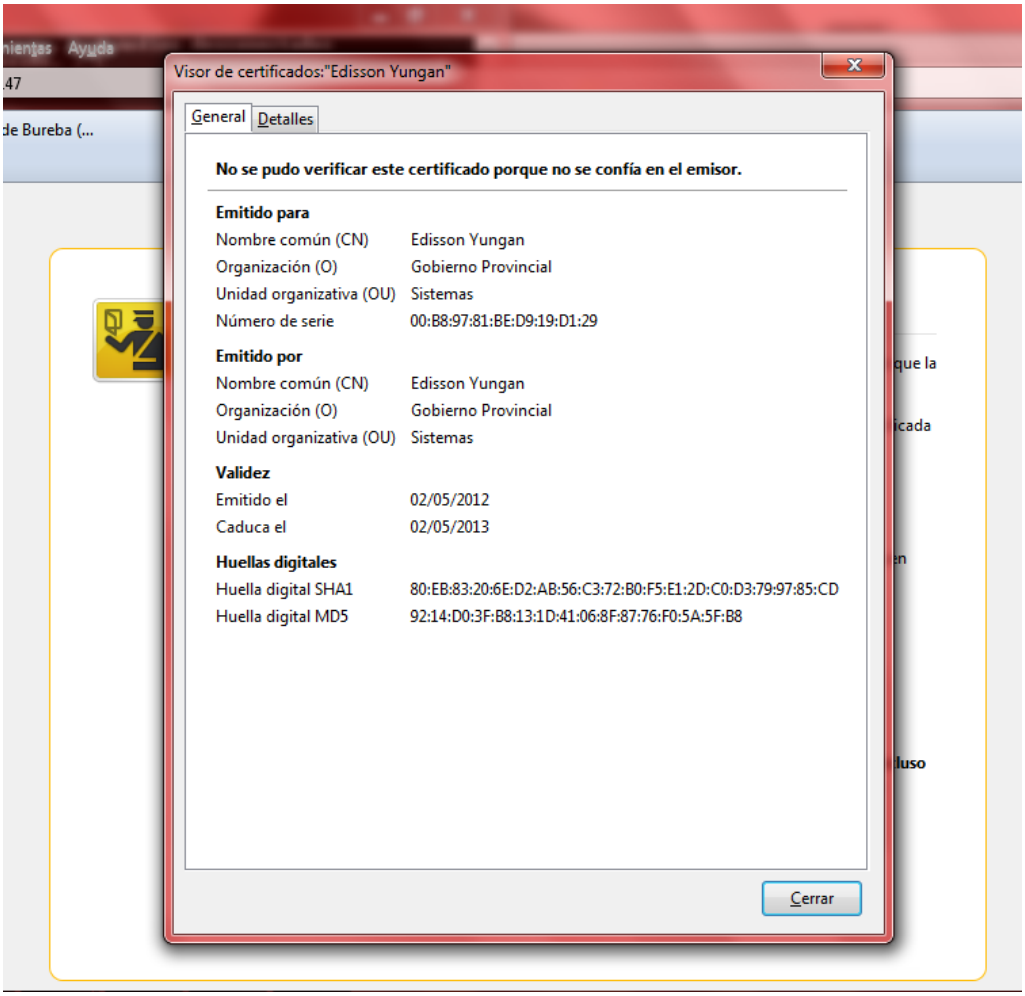

Figura 6.17: Detalles del certificado

6.8.3.4. Instalación y configuración del servicio MySql

El paquete de mysql se puede instalar directamente del cd de instalación del CentOS 5.5 pero también se lo puede realizar desde el repositorio:

```
yum -y install mysql mysql-server
```

Iniciamos el servicio MySql:

```
service mysqld start
```

Para que inicie automáticamente al prender el servidor añadimos el servicio MySQL al arranque del sistema:

```
service mysqld on
```

Asigna una clave de acceso al usuario **root** de MySQL:

```
mysqladmin -uroot password 'clavemysql'
```

Se crea una nueva base de datos con el nombre **radius**:

```
mysqladmin -uroot -pclavemysql create radius
```

Se ingresa al intérprete de comandos de MySQL:

```
mysql -uroot –pclavemysql
```

Asigna el usuario y la clave de acceso para acceder a la base de datos radius, el nombre del usuario es radius:

```
GRANT all ON radius.* TO radius@localhost IDENTIFIED BY
'radius123';
```

Salir de MySQL:

```
exit;
```

Utilizando el usuario **radius**, que se le asigno a la base de datos **radius**, se crea la base de datos con los esquemas incluidos con Freeradius:

```
mysql -uradius –pradius123 radius <
/etc/raddb/sql/mysql/cui.sql

mysql -uradius -pradius123 radius <
/etc/raddb/sql/mysql/ippool.sql

mysql -uradius -pradius123 radius <
/etc/raddb/sql/mysql/nas.sql

mysql -uradius -pradius123 radius <
/etc/raddb/sql/mysql/schema.sql

mysql -uradius -pradius123 radius <
/etc/raddb/sql/mysql/wimax.sql
```

6.8.3.5. Instalación y Configuración de Radius Server

La instalación se realizo directamente de los repositorios de CentOS

```
yum -y install freeradius2 freeradius2-mysql
freeradius2-utils
```

Añadir el servicio **radiusd** a los servicios de arranque del sistema:

```
chkconfig radiusd on
```

Para empezar la configuración edite el archivo **/etc/raddb/radiusd.conf**:

```
nano /etc/raddb/radiusd.conf
```

Descomentar la línea que dice **$INCLUDE sql.conf**:

```
        $INCLUDE sql.conf
```

Editar el archivo **/etc/raddb/sql.conf**:

```
nano /etc/raddb/sql.conf
```

Definir los valores que se crearon anteriormente para acceder a la base de datos:

```
        # Connection info:

        server = "localhost"

        #port = 3306

        login = "radius"

        password = "radius123"
```

Descomentar el parámetro **readclients** con valor **yes**:

```
readclients = yes
```

Editar el archivo **/etc/raddb/sites-enabled/default**:

```
nano /etc/raddb/sites-enabled/default
```

Descomentar el parámetro **sql** en la sección **authorize**:

```
        Sql
```

Descomentar el parámetro **sql** en la sección **accounting**:

```
        Sql
```

Al terminar la configuración de Radius regrese al símbolo de sistema y acceda a MySQL para dar de alta un usuario para realizar una prueba:

```
mysql -uradius -pradius123 radius
```

Desde el símbolo de sistema de MySQL, ingresar un usuario con los siguientes atributos:

```
INSERT INTO radcheck (username, attribute, value)
VALUES ('prueba', 'Password', '12345');
```

Verificar si el usuario se creo correctamente:

```
select * from radcheck where username='prueba';
```

```
+----+----------+-----------+----+--------+
| id | username | attribute | op | value  |
+----+----------+-----------+----+--------+
|  1 | prueba   | Password  | == | 12345  |
+----+----------+-----------+----+--------+
1 row in set (0.00 sec)
```

Inicie el servicio Radius con **radiusd**:

```
service radiusd start
```

Verificar que el servicio puede autenticar a través de MySQL:

```
radtest prueba 12345 localhost 1812 testing123
```

Lo anterior debe devolver algo similar como lo siguiente siempre y cuando la configuración se realice correctamente:

```
Sending Access-Request of id 222 to 127.0.0.1 port 1812

        User-Name = "prueba"

        User-Password = "12345"

        NAS-IP-Address = 127.0.0.1

        NAS-Port = 1812

rad_recv: Access-Accept packet from host 127.0.0.1 port
1812, id=222, length=20
```

6.8.3.6. Instalación y configuración de Chillispot

Chillispot se encarga de la autenticación de los usuarios de la rede inalámbrica del Gobierno Provincial de Tungurahua.

Primero descargamos el paquete rpm de la siguiente dirección http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm luego lo ejecutamos y quedara instalado.

Para configurar se edita el archivo chilli.conf con lo siguiente:

```
[root@gobierno httpd]# nano /etc/chilli.conf
```

```
#dirección de red que usaran los clientes de la red
net 192.168.182.0/24

#asigna direcciones ip dinámicamente
dynip 192.168.182.0/24

#servidor dns a utilizar por los clientes
dns1 172.16.1.147
dns2 172.16.1.129

#dominio que usaran los clientes
domain gobierno.ec
ipup /etc/chilli.ipup
ipdown /etc/chilli.ipdown

#direccion del servidor radius
radiuslisten 127.0.0.1

#puertos udp del servidor radius
radiusserver1 127.0.0.1
radiusserver2 127.0.0.1

radiusauthport 1812
radiusacctport 1813

#contraseña compartida con el servidor radius
radiussecret testing123

#interfaz a utilizar
dhcpif eth1

#dirección automática para la autenticación
uamserver https://192.168.182.1/cgi-
bin/hotspotlogin.cgi

#contraseña compartida con el script de autenticación
uamsecret ht2eb8ej6s4et3rg1ulp

#dirección permitida sin necesidad de autenticación
uamallowed 192.168.182.1
```

Copiar los siguientes archivos para su funcionamiento

```
[root@gobierno ]# cp /usr/share/doc/chillispot-
1.1.0/firewall.iptables /etc/rc.d

[root@gobierno ]# cp /usr/share/doc/chillispot-
1.1.0/hotspotlogin.cgi /var/www/gobierno.ec/cgi-bin/
```

Para que arranque automáticamente el firewall.iptables se lo coloca en el archivo rc.local.

```
[root@gobierno ]#echo "firewall.iptables">>
/etc/rc.d/rc.local
```

El archivo hotspotlogin.cgi contiene la pagina de autenticación de chillispot, el cual puede ser modificado su diseño a su conveniencia.

Para finalizar la configuración se arranca el servicio y se coloca para que inicie automáticamente.

```
[root@gobierno ]# service start chilli
[root@gobierno ]# chkconfig chilli on
```

6.8.3.7. Instalación y configuración de DaloRadius

Para que funcione correctamente DaloRadius se de instalar primero, PHP y sus ligaduras para MySQL, la biblioteca GD y Pear-DB:

```
yum -y install php php-mysql php-gd php-pear php-pear-
DB
```

Descargar el código fuente desde sourceforge.net/projects/daloradius el archivo correspondiente a la versión más reciente de DaloRadius, descomprimir el archivo descargado dentro del directorio /var/www/:

```
tar zxvf daloradius-0.9-9.tar.gz
```

Cambiar los permisos de todo el contenido del directorio recién descomprimido para que pertenezcan al usuario y grupo apache:

```
chown -R apache:apache daloradius-0.9-9
```

Entrar al directorio DaloRadius cargue las tablas de DaloRadius en la base de datos utilizada por Freeradius.

```
mysql -uradius -pradius123 < contrib/db/mysql-
daloradius.sql
```

Editar el archivo library/daloradius.conf.php:

```
nano library/daloradius.conf.php
```

Edite los valores correspondientes para establecer la conexión ala base de datos utilizada por Freeradius.

```
$configValues['CONFIG_DB_HOST'] = '127.0.0.1';

$configValues['CONFIG_DB_USER'] = 'radius';

$configValues['CONFIG_DB_PASS'] = 'radius123';

$configValues['CONFIG_DB_NAME'] = 'radius';
```

Reiniciar el servicio httpd:

```
service httpd restart
```

Para comprobar se debe acceder con cualquier navegador moderno hacia http://172.16.1.41/daloradius/. Para ingresar al sistema se utiliza el usuario Administrator y la clave de acceso radius que vienen por defecto. Desde esta

interfaz podrá añadir y administrar las cuentas de usuarios y administrar y añadir los puntos de acceso.

6.8.3.8. Configuración del punto de acceso

La configuración del Access Point marca DLINK -3200AP es la siguiente:

En el navegador digitamos la ip del Access Point y nos pide el usuario y contraseña para poder acceder, en este caso el usuario y contraseña son los que vienen por defecto; usuario admin y sin contraseña, luego muestra la pantalla principal de configuración como se indica en la figura 6.18, colocamos el SSID en este caso es GPT, elegimos el canal 6 y no colocamos ningún tipo de autenticación, como se indica en la figura 6.19, a continuación establecemos la ip como se indica en la figura 6.20, deshabilitamos el DHCP como se indica en la figura 6.21, verificamos la configuración realizada en el Access Point como se indica en la figura 2.22.

Figura 6.18: Pantalla principal del Access Point

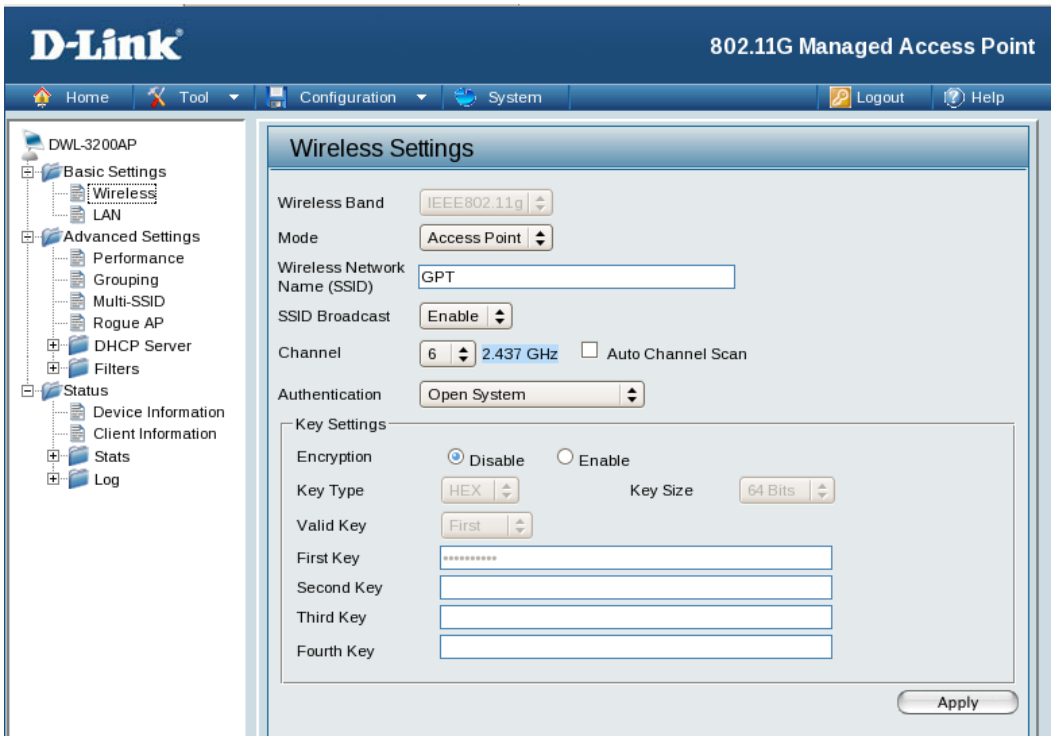

Figura 6.19: SSID, canal y autenticación.

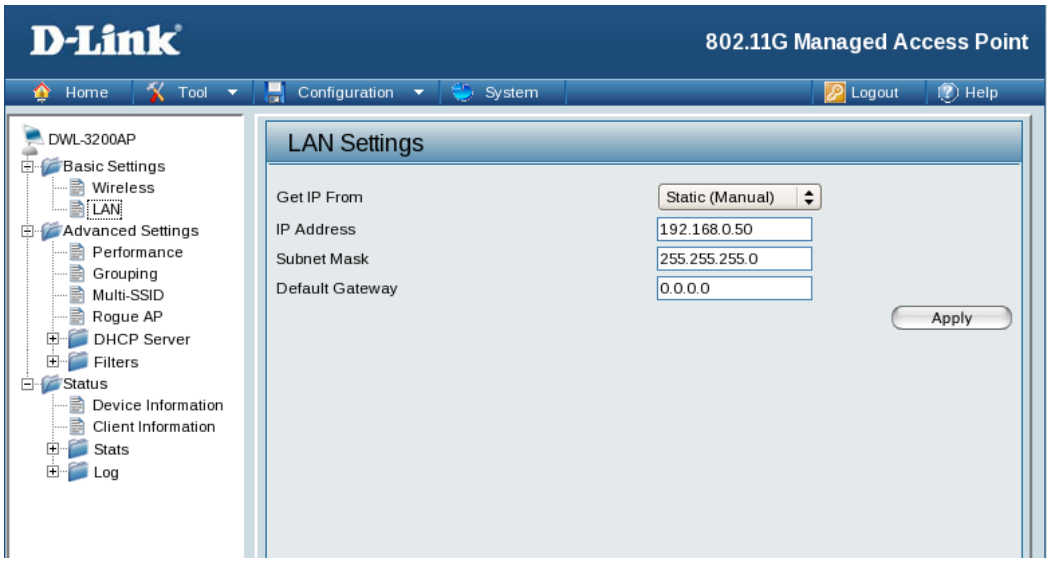

Figura 6.20: Configuración IP

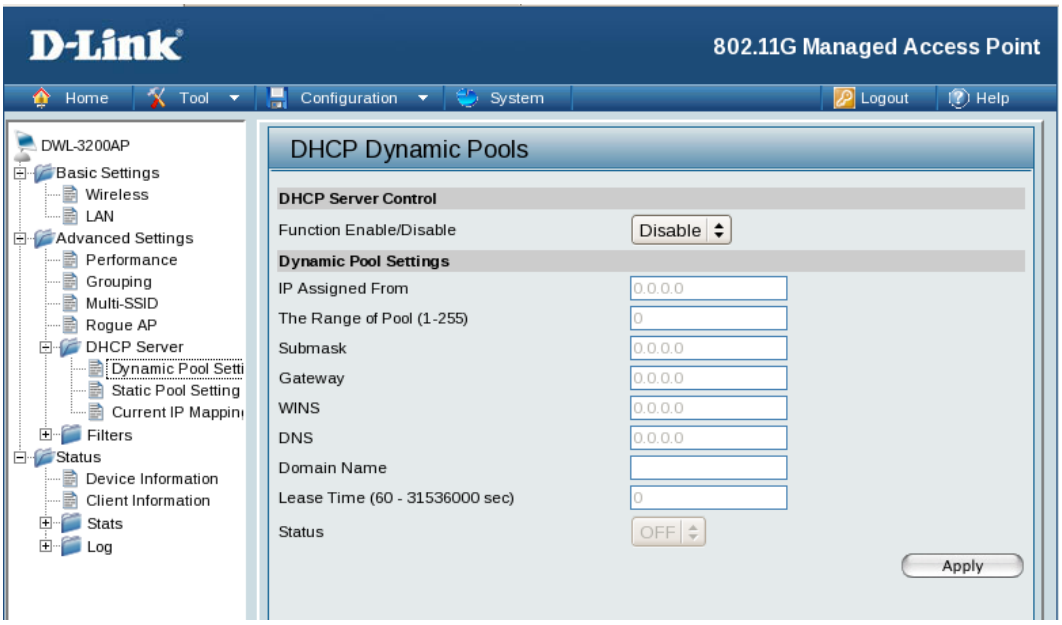

Figura 6.21: Configuración DHCP

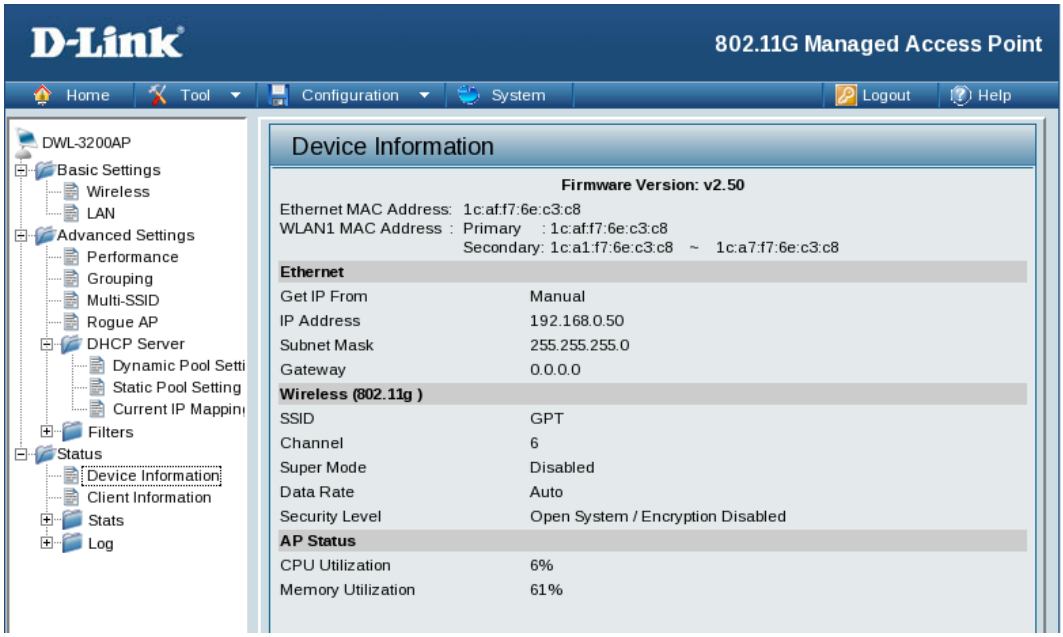

Figura 6.22: Información del AP

6.8.3.9. Prueba de acceso a la red inalámbrica

Para realizar las pruebas del sistema de control de acceso a la red inalámbrica del Gobierno Provincial de Tungurahua se procedió ingresando al navegador web desde una pc con dispositivo inalámbrico donde se muestra la validación del

certificado digital figura 6.23, luego se realiza el acceso por certificado como se indica en la figura 6.24, luego ingresa a la pantalla de autenticación donde pide usuario y contraseña como se indica en la figura 6.25, si el usuario y contraseña es correcta es autorizado para conectarse a la red inalámbrica como se indica en la figura 6.26.

Figura 6.23: Validación del certificado digital

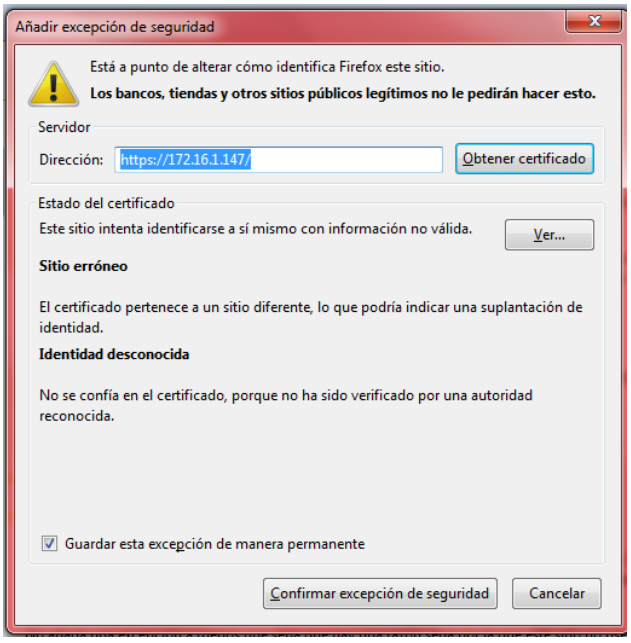

Figura 6.24: Acceso por certificado

Figura 6.25: Pagina de autenticación

Figura 6.26: Acceso autorizado a la red

6.9. Presupuesto

Para realizar el presente proyecto no se procedió a la compra de ningún equipamiento tecnológico ya que la institución contaba con todo lo necesario para realizar el proyecto.

RECURSOS MATERIALES				
N	Denominación	Tiempo / Unidades	Costo Unitario	Total
	Flash memory	1	20.00	30.00
	Resmas de papel bond	3	5.00	15.00
	Tinta de impresora	4	5.00	20.00
	Internet	400 horas	0.80	320.00
	Esferos	3	0.25	0.75
	Transporte			150.00
	Alimentación			120.00
Total				655.75

Tabla 6.1: Presupuesto

6.10. Administración

La administración del sistema de control de acceso a la red inalámbrica del Gobierno Provincial de Tungurahua está a cargo del personal del Área de Tecnologías Informáticas los cuales serán responsables del mantenimiento del sistema. La administración del sistema se realizara por medio de la aplicación web DaloRadius del cual se ha realizado un manual de las principales tareas que cubren las necesidades de la empresa.

6.11. Conclusiones y Recomendaciones

6.11.1. Conclusiones

- Las redes inalámbricas últimamente van cubriendo el mercado de forma mayoritaria en nuestro país debido a la fácil implementación de su tecnología y la movilidad que presta, caso contario de las redes cableadas. Cabe mencionar que las redes cableadas siempre estarán presentes para trabajar en conjunto con las redes inalámbricas estableciendo un espacio donde coexistan estos dos tipos de tecnología.
- En nuestro país el tema se seguridad de redes inalámbricas no tiene la suficiente atención que debería. Como es el caso del Gobierno Provincial

de Tungurahua, a través del estudio se pudo constatar que los administradores de la red implementaban un mínimo de seguridad en la red inalámbrica, pasando ha convertirse en un punto vulnerable, por lo que la implementación de un sistema de control de acceso fue necesario.

- El Gobierno Provincial de Tungurahua desde la implantación de la red inalámbrica no ha tomado las suficientes precauciones que con lleva esta tecnología, dejando expuesta para cualquier tipo de ataque. Al implementar el sistema de control de acceso a las redes inalámbricas dejan de ser un punto fácil de acceso, pero con ello no se quiere decir que la red está completamente segura, siempre será necesario seguir investigando e incorporar nuevos mecanismos de seguridad para mantener un nivel de seguridad aceptable dentro de la institución.
- La mayoría de los usuarios que utilizan las redes inalámbricas de Gobierno Provincial de Tungurahua, no contaban con la suficiente capacitación para saber los riesgos que implica utilizar esta tecnología, por lo que hace aún más vulnerable la red inalámbrica de la institución.
- La ubicación del Gobierno Provincial de Tungurahua se encuentra en el centro de la ciudad, por lo que la señal que emite el punto de acceso fácilmente llega a los edificios contiguos. Como la comunicación se realiza por el aire está expuesta a que cualquier persona que cuente con un dispositivo inalámbrico y con conocimientos fundamentales, por lo que pueda encontrar fácilmente un punto vulnerable de la red y acceder a la misma.
- El servidor que se implemento para el sistema de control de acceso es CentOS 5.5 por su alto rendimiento en cuanto a servidores se refiere, como también su distribución gratuita, aunque las configuraciones sean un poco complejas y su administración sea realizada por usuarios capacitados.

6.11.2. Recomendaciones

- Con la implantación de la red inalámbrica en el Gobierno Provincial de Tungurahua, es necesario establecer políticas de seguridad que estén acorde a los requerimientos de la institución, siempre teniendo en cuenta

que la saturación de políticas puede mermar el redimiendo de la red inalámbrica.

- Los administradores de la red inalámbrica deben mantenerse al tanto de las posibles vulnerabilidades que se presenten, ya que el avance de la tecnología va a pasos agigantados y no falta inescrupulosos que esté buscando vulnerabilidades a los sistemas de seguridad implementadas en la red inalámbrica.
- Es recomendable utilizar dispositivos inalámbricos como alámbricos que se basen en estándares similares y si es posible que sean de la misma marca, para que el acoplamiento y rendimiento de la red inalámbrica sea eficiente dentro de la institución.
- Se debe realizar un estudio de la distribución de la señal inalámbrica, como en este caso el diseño de la red inalámbrica ya estaba implementado no fue realizada, esto con el propósito de establecer la posición más adecuada de los Access Point y disponer de una mejor señal para todas las estaciones de trabajo.
- La administración de los usuarios se lo puede realizar directamente desde la consola de la base de datos, pero esto requiere personal capacitado para realizarlo, por lo que es recomendable la utilización de la interfaz gráfica proporcionada por la aplicación web DaloRadius para la administración de los usuarios de la red inalámbrica.

6.12. Bibliografía

Tesis

ANALUISA, Hernán. 2006. *Aspectos de seguridad de redes inalámbricas de red de área local*. Ambato – Ecuador.

CABRERA, Proaño; REASCOS Irving. 2011. *Análisis a la seguridad de redes inalámbricas como extensión de una red LAN*. Quito – Ecuador.

Libros

UYLESS, Black. 1997. *Redes de computadoras*. Protocolos, normas e interfaces. 2º edición. Madrid – España. RA-MA Editorial. Pág. 432

RAYA, José; RAYA, Cristina. 2002. *Redes Locales*. Madrid – España. RA-MA Editorial. Pág. 335

RANDALL, Nichols; PANOS, Lekkas. 2003. *Seguridad para comunicaciones inalámbricas*. Aravaca – España. McGraw Hill Editorial. Pág.

REGIS, J. 2003. *Comunicaciones inalámbricas de banda ancha*. Aravaca – España. McGraw Hill Editorial. Pág. 585

Internet

http://seguridad-informacion.blogspot.com/2010/05/definicion-del-concepto-seguridad-de-la.html *Seguridad de la Información*

http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/16-PlaneacionEstrategicaSeguridad.pdf *Seguridad de la Información*

http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%20Y%20MATERIAL%20DE%20ESTUDIO/Introducci%F3n%20a%20los%20conceptos%20de%20Seguridad.pdf *Seguridad de la información*

http://www.x-net.es/tecnologia/wireless.pdf *Estándar 802.11*

http://www.sans.org/reading_room/whitepapers/wireless/security-vulnerabilities-wireless-lan-technology_1629 *Estándar 802.11*

http://www.mundointernet.es/IMG/pdf/ponencia95.pdf *Tipos de ataques e intrusos en las redes informáticas*

http://www4.uji.es/~al024444/mecanismosdeseguridad.html#2 *Mecanismos de control de acceso*

http://sistemasoperativos.angelfire.com/html/5.5.html *Control de Acceso*

http://blyx.com/public/wireless/redesInalambricas.pdf *Redes Inalámbricas*

http://multingles.net/docs/alezito/alezito_inalamb.htm *Redes Inalámbricas*

http://www.angelfire.com/mi2/Redes/topologia.html *Topologías*

http://www.jegsworks.com/lessons-sp/lesson7/lesson7-2.htm *Medios de Transmisión*

http://www.wikilearning.com/curso_gratis/curso_de_criptografia_basica_para_principiantes/4306-9 *Protocolos de Seguridad*

6.13. Anexos

6.13.1. Anexo 1: Encuesta realizada a los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua

UNIVERSIDAD TÉCNICA DE AMBATO

Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Encuesta

Lugar a encuestar: Gobierno Provincial de Tungurahua

Fecha de aplicación:

Objetivo de la encuesta

Señoras y señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo entrono a la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua. Agradecemos su colaboración y garantizamos absoluta reserva de su información.

1. ¿La señal que percibe su estación de trabajo en la red inalámbrica del Gobierno Provincial de Tungurahua es?

( ) Señal excelente

( ) Señal media

( ) Señal regular

( ) No hay señal

2. ¿Cómo calificaría la velocidad de conexión de las redes inalámbricas del Gobierno Provincial de Tungurahua?

( ) Excelente

( ) Buena

( ) Regular

( ) Mala

( ) Deficiente

3. ¿Ha tenido problemas con la información a causa de la red inalámbrica del Gobierno Provincial de Tungurahua?

( ) Perdida de información

( ) Robo de información

( ) Ninguna

4. ¿Le parece segura la conexión de la red inalámbrica del Gobierno Provincial de Tungurahua?

SI ( ) NO ( )

6.13.2. Anexo 2: Encuesta realizada a los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua

UNIVERSIDAD TÉCNICA DE AMBATO

Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Encuesta

Lugar a encuestar: Gobierno Provincial de Tungurahua

Fecha de aplicación:

Objetivo de la encuesta

Señoras y señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo entrono a la seguridad de las redes inalámbricas del Gobierno Provincial de Tungurahua. Agradecemos su colaboración y garantizamos absoluta reserva de su información.

1. ¿Qué nivel de seguridad utiliza las redes inalámbricas del Gobierno provincial de Tungurahua para garantizar una conexión segura?

( ) Protección por contraseña WEP

( ) Protección por contraseña WAP/WAP2

( ) Protección por contraseña desconozco el tipo de cifrado

( ) Filtrado por dirección MAC

( ) Desconozco

2. ¿Qué tipo de acceso utiliza las redes inalámbricas del Gobierno Provincial de Tungurahua para garantizar la integridad de la información?

( ) Acceso libre ( ) Acceso controlado

3. ¿Regularmente se hacen test o auditorias de seguridad a la red inalámbrica a la red inalámbrica del Gobierno Provincial de Tungurahua?

SI ( ) No ( )

4. ¿Los usuarios de la red inalámbrica del Gobierno Provincial de Tungurahua han recibido capacitación en el uso adecuado y los peligros de la tecnología de red inalámbrica?

SI ( ) No ( )

5. ¿Existen políticas de seguridad inalámbrica implementadas en el Gobierno Provincial de Tungurahua?

SI ( ) No ( )

6.13.3. Anexo 3: Manual de software de administración DaloRadius

DaloRadius es una aplicación web que permite administrar el sistema de control de acceso.

La aplicación web de DaloRadius tiene diferentes opciones para administrar la red, pero para redactar este manual nos centraremos en las opciones que cubren los aspectos necesarios para cubrir las necesidad de los administradores de la red inalámbrica del Gobierno Provincial de Tungurahua.

Para empezar a manipular la aplicación web abrimos el navegador donde colocamos la dirección, luego aparece la pantalla de logeo de DaloRadius como se indica en la figura 6.27 donde existe un campo de usuario y clave. El usuario por defecto es administrator y la clave radius.

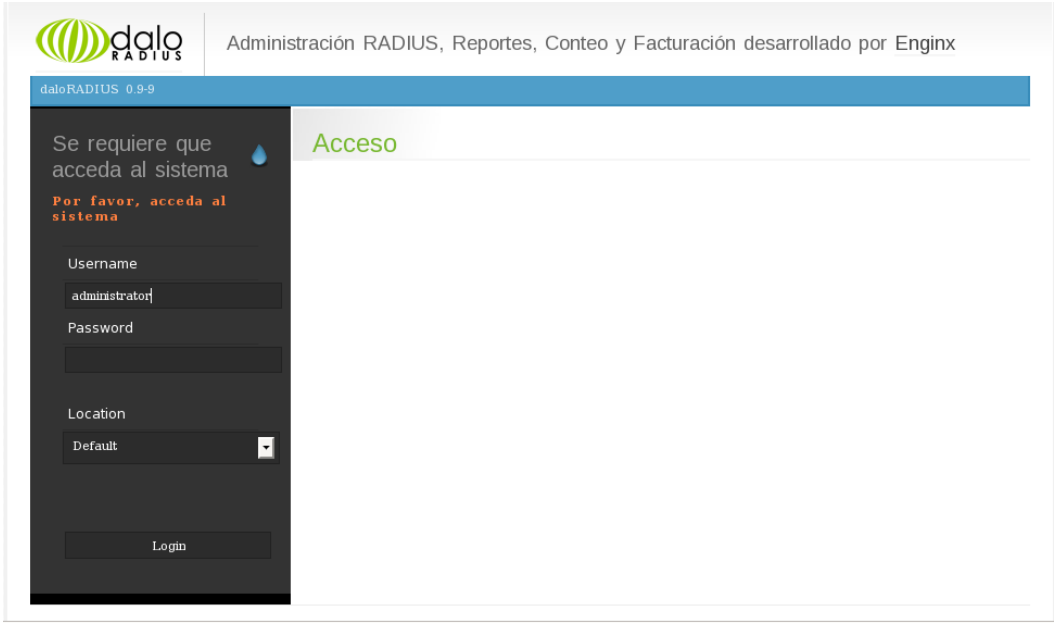

Figura 6.27: Pantalla de inicio de DaloRadius

Luego de logearse correctamente muestra la pantalla de bienvenida de DaloRadius como se indica en la figura 6.28 dentro de la cual podemos observar un menú de herramientas.

Figura 6.28: Pantalla de bienvenida

Vamos a comenzar explicando el menú principal.

Gestión: Usuarios

- Listado de usuarios
- Nuevo usuario
- Editar usuario
- Buscar usuario
- Eliminar usuario

Dentro de la opción gestión se encuentra un grafico de barras indicando la cantidad de usuarios y hotspots registrados en el sistema, como se indica en la figura 6.29.

Figura 6.29: Grafico de barras del numero de usuarios.

Listado de usuario

Dentro de esta opción se podrá encontrar a todos los usuarios registrados que tendrán acceso a la red inalámbrica con se indica en la figura 6.30.

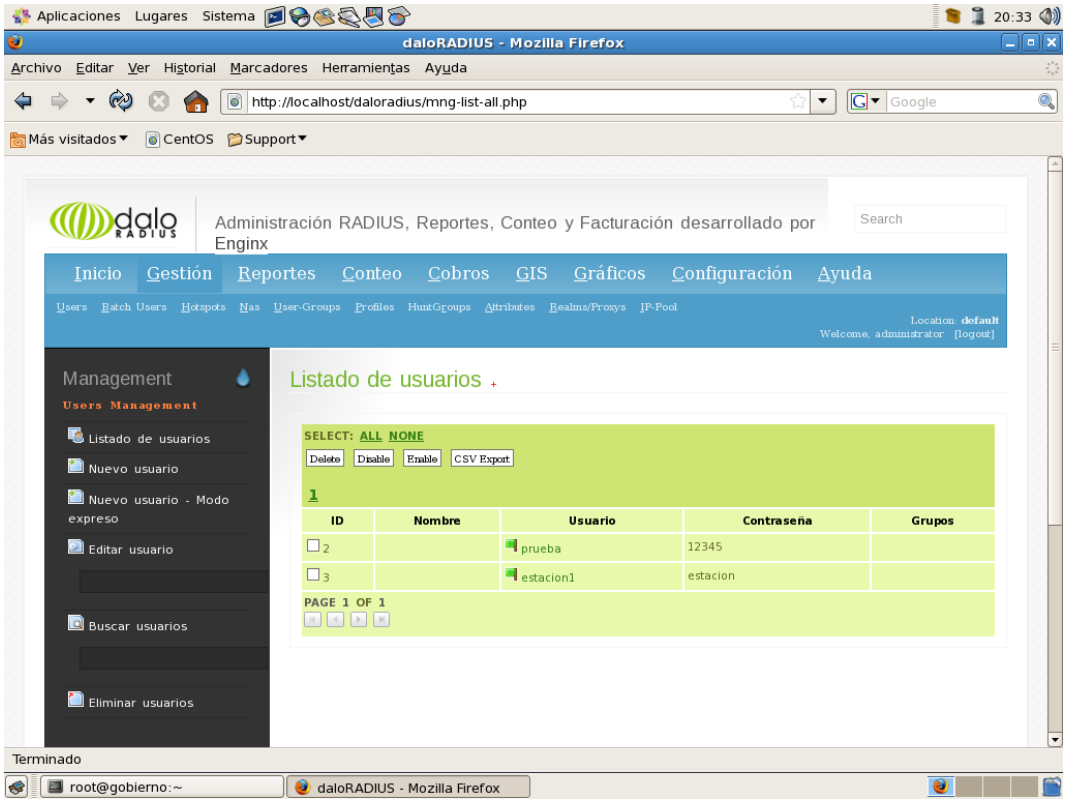

Figura 6.30: Listado de usuarios

Nuevo usuario

En esta opción se puede agregar nuevos usuarios al sistema, de cada usuario se puede ingresar diferente información como:

Información de la cuenta: Indica de que manera se va autenticar a los usuarios, existe tres formas de hacerlo: Autenticación por usuario y contraseña, autenticación por MAC address y por código PIN como se puede observar en la figura 6.31.

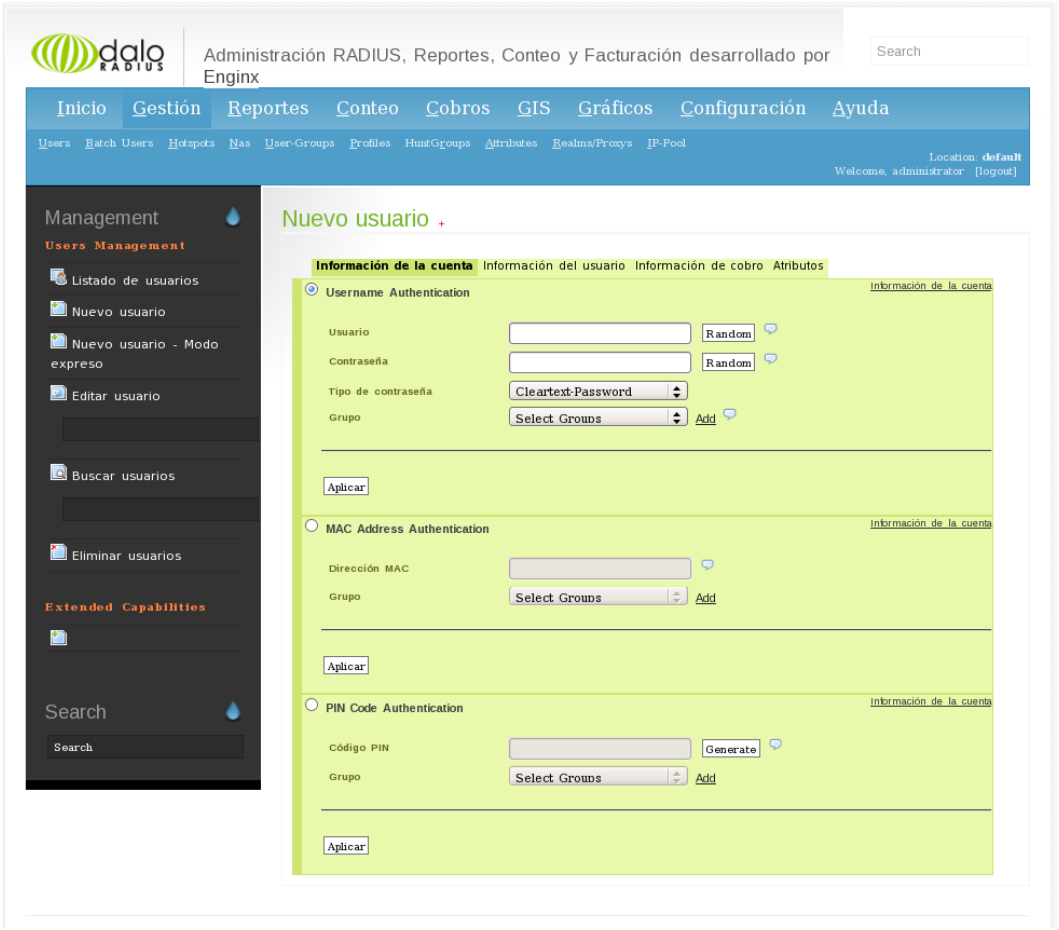

Figura 6.31: Información de la cuenta

Información del usuario: En esta pestaña se ingresa los datos personales e información adicional del usuario como se indica en la figura 6.32.

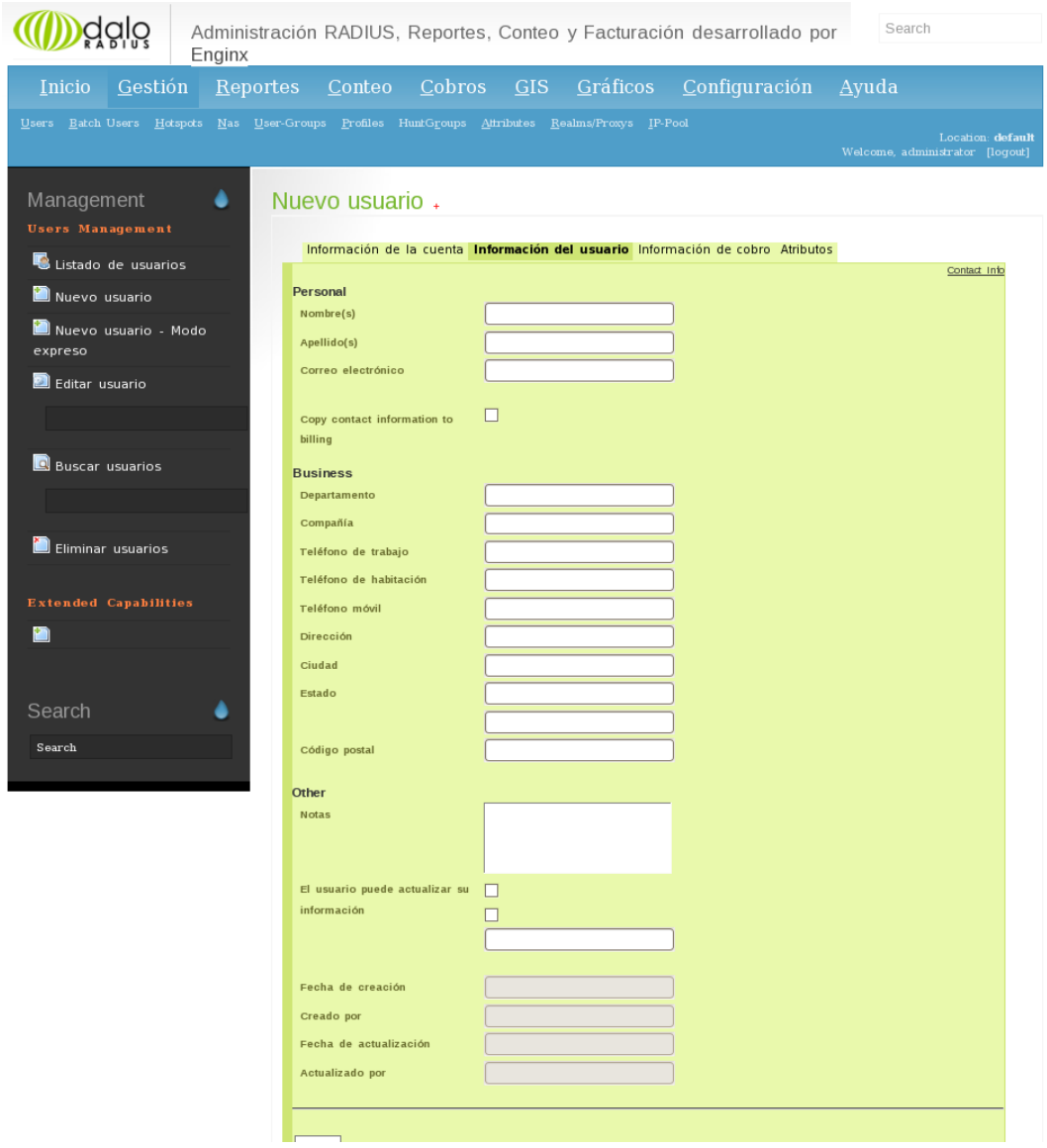

Figura 6.32: Información del usuario

Editar usuario

En esta opción se puede realizar cambios a la información de los usuarios registrados en sistema como se indica en la figura 6.33.

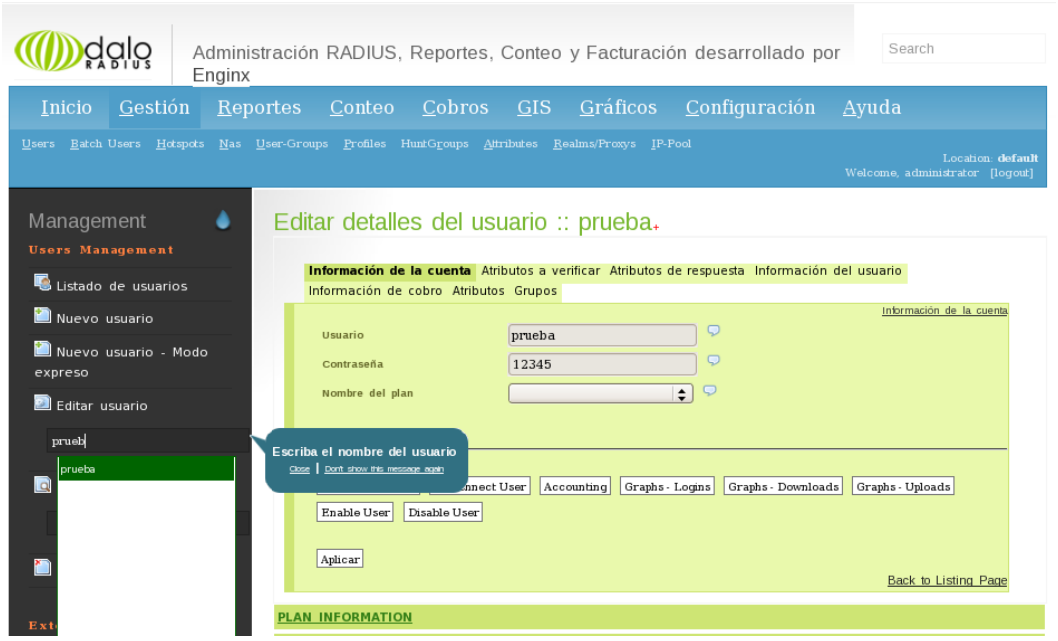

Figura 6.33: Editar usuarios

Eliminar usuario

En esta opción se puede eliminar la información de los usuarios registrados en sistema como se indica en la figura 6.34.

Figura 6.34: Eliminar usuario

Reportes:

Usuarios en línea: Dentro de esta opción se puede encontrar a los usuarios que están conectados en tiempo real a red inalámbrica, como se indica en la figura 6.35

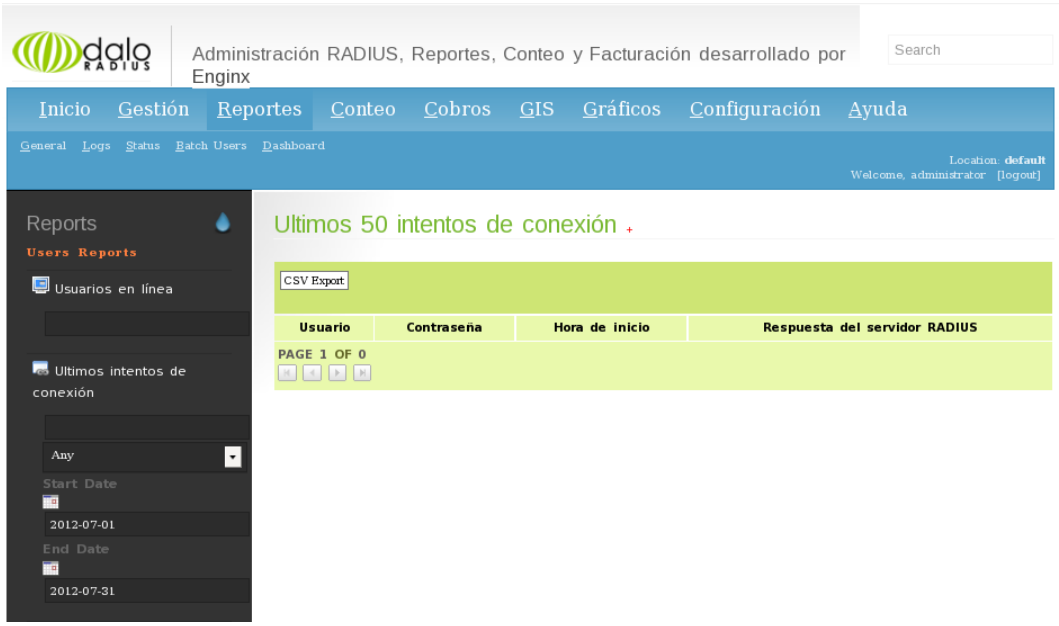

Figura 6.35: Usuarios en línea.

Configuración

- Ajuste de la base de datos
- Ajuste del lenguaje
- Ajuste de acceso
- Ajuste de la interface

Ajuste de la base de datos: En esta opción se puede elegir el motor de la base de datos a utilizar, el nombre del servidor de la base de datos, usuario y contraseña de la base de datos y el nombre de la base de datos, como se indica en la figura 6.36.

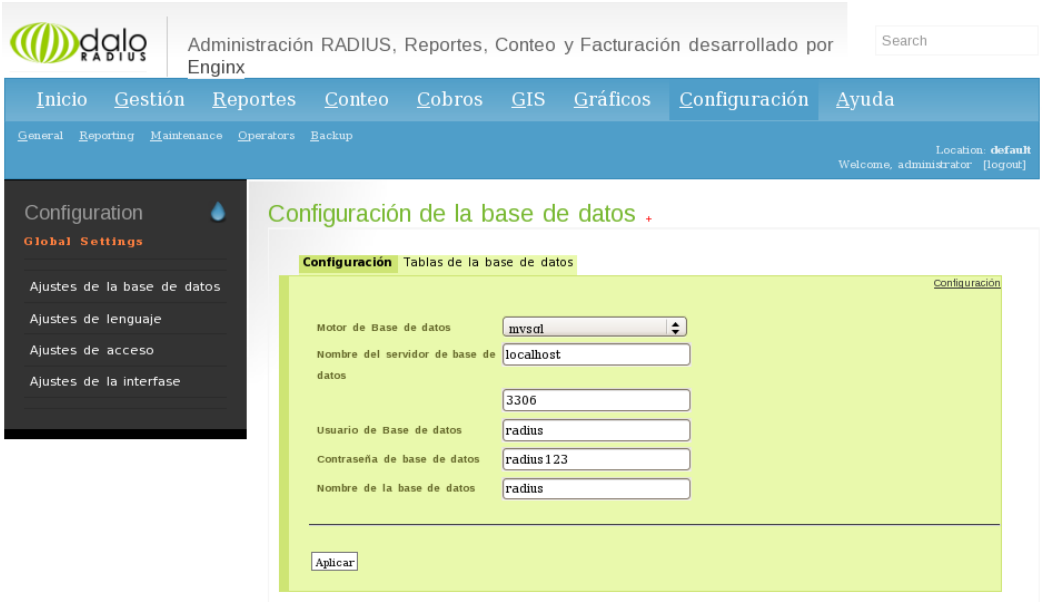

Figura 6.36: Ajuste de la base de datos

Ajuste del lenguaje: Permite elegir el idioma que más le convenga al usuario administrador, como se indica en la figura 6.37.

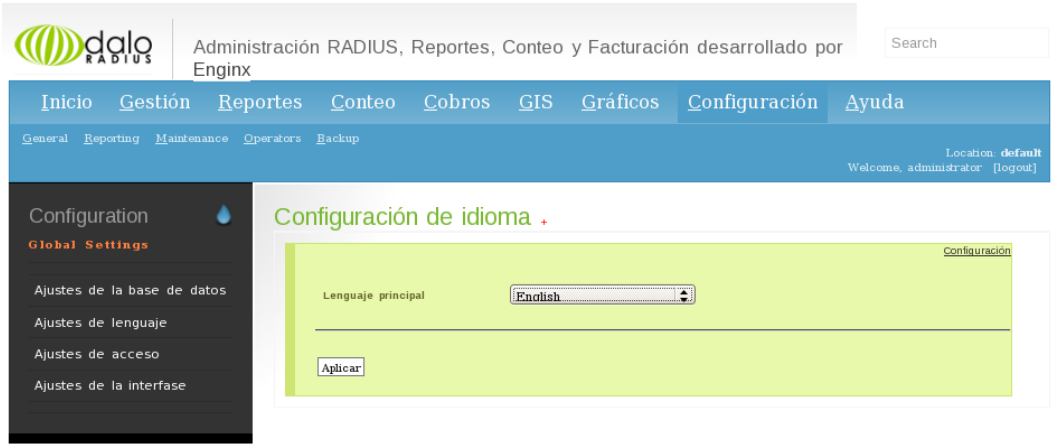

Figura 6.37: Ajuste del lenguaje

Ajuste de acceso: Permite guardar un registro de las páginas visitadas en internet y todas las acciones que se ejecuten por el usuario, como se indica en la figura 6.38.

Figura 6.38: Ajuste de acceso

Ajuste de la interface: Permite realizar cambios como esconder la contraseña, mostrar una cantidad específica de filas por tabla, enumerar las filas en las tablas y habilitar la autocompletación, como se indica en la figura 6.39.

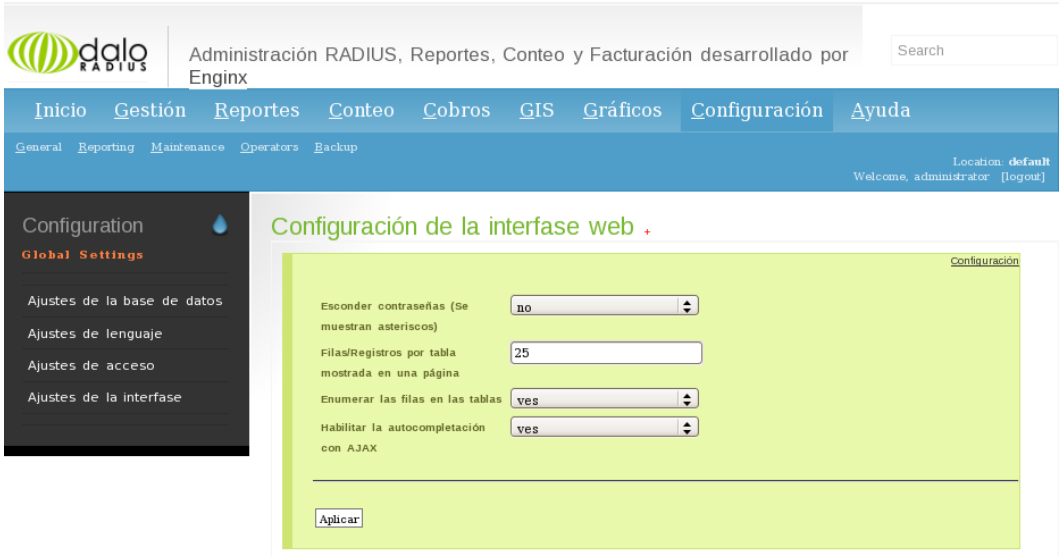

Figura 6.39: Ajuste de interfaz

6.13.4. Anexo 4: Especificaciones del punto de acceso

Las especificaciones del Access Point de modelo DW-3200AP son:

FICHA TECNICA

ESTÁNDAR	IEEE 802.11g/11b IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet IEEE 802.3af PoE
INTERFAZ	Puerto 10/100 Base-Tx
SEGURIDAD	- 64/128/152-bit WEP - IEEE 802.1x - MAC Address filtering - WPA/WPA2 EAP - WPA/WPA2 PSK - AES (Advanced Encryption Standard) - 802.11i-ready - SSID Broadcast enable/disable - 802.1Q Multiple SSID's (máximo 4)
TASA DE TRANSFERENCIA	**802.11g :** 108, 54, 48, 36, 24, 18, 12, 9 y 6 Mbps **802.11b :** 11, 5.5, 2 y 1 Mbps
SENSIBILIDAD DE RECEPCIÓN	- 802.11b: 1Mbps: -94dBm 2Mbps: - 90dBm 5.5Mbps: -89dBm 11Mbps: -85dBm - 802.11g: 1Mbps: -94dBm 2Mbps: - 90dBm 5.5Mbps: -89dBm 6Mbps: -90dBm 9Mbps: -84dBm 11Mbps: -85dBm 12Mbps: -82dBm 18Mbps: -80dBm 24Mbps: -77dBm 36Mbps: -73dBm 48Mbps: -72dBm 54Mbps: -72dBm
POTENCIA DE TRANSMISIÓN	- 802.11b: 1mW (0dBm) 5mW (7dBm) 10mW (10dBm) 20mW (13dBm) 30mW (15dBm) 50mW (17dBm) 100mW (20dBm) - 802.11g: 1mW (0dBm) 5mW (7dBm) 10mW (10dBm) 20mW (13dBm) 30mW (15dBm) 63mW (18dBm) 100mW (20dBm)
RANGO OPERACIÓN WIRELESS VALORES NOMINALES	- Indoors: 30m : 54Mbps 34m : 48Mbps

* FACTORES DEL ENTORNO PUEDEN AFECTAR ADVERSAMENTE LOS RANGOS DE COBERTURA.	39m : 36Mbps 47m : 24Mbps 56m : 18Mbps 66m : 12Mbps 79m : 9Mbps 99m : 6Mbps
ANTENA	Antenas Dual dipolo, con 5dBi de ganancia Diversidad RSMA
RANGO DE FRECUENCIA	2.4000 – 2.4835GHz, ISM band
TÉCNICAS DE MODULACIÓN	- 802.11g: OFDM- BPSK: 6 y 9 Mbps, QPSK: 12 y 18 Mbps, 16QAM: 24 y 36 Mbps, 64QAM: 48 y 54 Mbps DSSS- DBPSK:1Mbps, DQPSK: 2Mbps, CCK: 5.5 y 11 Mbps - 802.11b: DBPSK: 1 Mbps, DQPSK: 2 Mbps, CCK: 5.5 y 11Mbps
MODOS DE OPERACIÓN	Access Point Point-to-Point (PtP) Bridge Point-to-Multipoint (PtMP) Bridge
LEDS	- Power - LAN - 802.11b/g
MÉTODO DE ACCESO	CSMA/CA con Ack
ADMINISTRACIÓN	Web-based : IE v.6 ó superior Netscape Navigator v.7 ó superior Telnet SNMP v.3 AP Manager
CARACTERÍSTICAS FÍSICAS	
DIMENSIONES	277,7 x 155 x 45 mm
ALIMENTACIÓN	PoE Input : 100 – 240V AC, 50 – 60 Hz Output : 48V DC +/- 10%
TEMPERATURA DE OPERACIÓN	- 40ºC a 60ºC
TEMPERATURA DE ALMACENAJE	- 40ºC a 65ºC
HUMEDAD DE OPERACIÓN	10% a 90% no condensado
HUMEDAD DE ALMACENAJE	5% a 95% no condensado
CERTIFICACIONES	FCC Class B CE Wi-Fi

Figura 6.40: Ficha técnica del Access Point