ESTRATEGIA COMERCIAL DE SEGURIDAD EN REDES 802.11X (WIFI) EN EMPRESAS DE PUERTO BERRIO

Ricardo Alfonso Sanabria Silva
Diego Alejandro Valencia Rivera
Danny Francisco Hernández Godoy

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BÁSICA E INGENIERIA
LA DORADA
2013

ESTRATEGIA COMERCIAL DE SEGURIDAD EN REDES 802.11X (WIFI) EN EMPRESAS DE PUERTO BERRIO

Ricardo Alfonso Sanabria Silva
Diego Alejandro Valencia Rivera
Danny Francisco Hernández Godoy

Trabajo de grado para optar al título de
Tecnólogo de Sistemas

Tutor
YESID AGUIRRE SANCHEZ
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BÁSICA E INGENIERIA
LA DORADA
2013

Nota de aceptación

_____

_____

_____

_____

Presidente Jurado

_____

Jurado

_____

Jurado

La Dorada, Octubre de 2013

AGRADECIMIENTOS

Los autores:

Queremos expresar nuestros agradecimientos a las empresas de Puerto Berrio, Antioquia, quienes con su ayuda han contribuido a que pudiera realizar y culminar este trabajo.

En especial agradecemos a Yesid Aguirre, su desinteresada y eficaz colaboración en la realización del presente trabajo, por su intensa labor en la orientación, dirección y supervisión realizada.

CONTENIDO

Pág.

LISTA DE MAPAS

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

Las redes inalámbricas han ganado mucha popularidad en los últimos tiempos, esta popularidad ha crecido hasta tal punto en que las podemos encontrar en casi cualquier ámbito de nuestra vida cotidiana, teléfonos inalámbricos, Ipad, computadoras y teléfonos móviles son algunos de los ejemplos más evidentes en nuestra sociedad.

A medida que las redes 802.11 han crecido, son más evidentes los riesgos de seguridad en su diseño. El protocolo WEP (Wired Equivalent Privacy) diseñado en años anteriores para proporcionar confidencialidad en este tipo de redes, pero no fue capaz de aguantar mucho tiempo, y muy pronto cualquier atacante sin demasiado conocimiento era capaz de desmantelar las defensas de una red utilizando la seguridad WEP.

A pesar de que han surgido sustitutos que parecen ofrecer ciertas garantías, como el estándar 802.11i, aún existen diversas amenazas como los ataques de hombre en el medio y ataques de denegación de servicio. La naturaleza del medio inalámbrico además ofrece múltiples retos, un administrador necesita conocer qué está ocurriendo en su red, tanto desde el punto de vista de la seguridad, como desde el punto de vista de la depuración de errores y optimización del rendimiento, tareas en las que la encriptación sólo cubre algunos aspectos y dificulta otros.

En respuesta a esta demanda, ya han surgido soluciones que estaban ampliamente implantadas en los sistemas cableados, los sistemas de detección de intrusiones, estos sistemas permiten al administrador conocer si se están realizando ataques sobre su red, también pueden proporcionar servicios de localización del atacante e incluso implementan medidas activas para evitar intrusiones, como por ejemplo ataques DoS, evitando que los dispositivos de nuestra red sean víctimas de intrusiones ejecutadas por agentes extraños de su entorno. A pesar de la necesidad de este tipo de herramienta, el estándar 802.11

es relativamente nuevo y complejo para la implementación de sistemas de seguridad para empresas relativamente medianas o pequeñas.

En los capítulos correspondientes al proyecto de implementación de seguridad inalámbrica en las empresas ubicadas en la región del Magdalena Medio, se hará un estudio exhaustivo sobre los ataques existentes para el protocolo 802.11 y también sobre las técnicas de detección de intrusiones, haciendo especial hincapié en la clasificación de los ataques y las técnicas, y profundizando en las técnicas de detección spoofing.

Este proyecto presenta una propuesta que conllevará a la implementación, configuración y uso de dispositivos que brinden seguridad inalámbrica en empresas ubicadas en la ciudad de Puerto Berrio, con el fin de prevenir interrupciones en el servicio de la señal y detección de posibles infiltraciones causadas por actores externos de la organización.

En este documento se da la descripción general del proyecto donde se plantea la carencia de seguridad inalámbrica para la red de algunas empresas de la región del Magdalena Medio, como problemática inicial, se muestra la no existencia de una configuración adecuada ante posibles intrusiones al sistema, de ahí nace la necesitad de ofrecer técnicas que permitan y ofrezcan confiabilidad en la transmisión de la información.

Este proyecto determina la viabilidad técnica, administrativa, financiera, social y ambiental de la implementación de un programa comercial de productos que garantizan la seguridad para estos sistemas de redes.

I. DEFINICION DEL PROBLEMA

El presente proyecto de desarrollo empresarial que implica la implementación de un sistema de redes inalámbricas con tecnología de seguridad en redes 802.11X (WIFI**),** aplicada de manera innovadora en empresas del sector productivo ubicadas en la región del Magdalena Medio, específicamente en la ciudad de Puerto Berrio, el impacto tecnológico esperado se traduce en mayor seguridad y control de datos e información en los sistemas informáticos de cada empresa lo cual redundara en términos de producción y desarrollo de los sistemas informáticos y la aplicación del conocimiento en redes a fin de optimizar el control en los equipos informáticos de la zona.

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas. Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.

1.1 FORMULACION DEL PROBLEMA

¿Se han implementado sistemas de seguridad en la redes inalámbricas en las empresas de Puerto Berrio?

¿Se han aplicado medidas de seguridad en las diferentes estaciones de trabajo que se conectan inalámbricamente ya sea mediante Acces Point o modem inalámbrico, haciendo énfasis que todos estos a su vez se relacionan con un servidor principal?

¿Cuáles son las condiciones del mercado de productos y servicios que suplen esta necesidad de seguridad de redes?

II. JUSTIFICACION

Las empresas implementan sistemas inalámbricos en sus sedes para brindar comodidad y movilidad en sus áreas laborales, utilizando dispositivos para cobertura de transmisión, a la vez se han utilizado sistemas como Wireless Watchen en redes cableadas que permiten la detección de intrusos haciendo un escaneo a usuarios activos conectados a la red, ofreciendo acceso a muchas de sus funcionalidades, pero siendo herramientas comerciales se desconoce el funcionamiento de las técnicas de detección empleadas.

Estos factores entre otros, determinan que no exista actualmente una configuración adecuada que evite intrusiones para redes 802.11, empleando métodos avanzados que permitan restringir el acceso a usuarios extraños.

Actualmente existe un gran vacío en este aspecto. Por tal motivo se realiza un estudio exhaustivo sobre los ataques existentes para el protocolo 802.11 y también sobre las técnicas de detección de intrusiones, haciendo especial hincapié en la clasificación de los ataques y las técnicas, y profundizando en las técnicas de detección de MAC spoofing, por lo cual nos lleva a investigar factores de riesgo y proponer soluciones rigurosas que hagan sistemas con seguridad más eficientes en las redes de radio frecuencia.

III. OBJETIVOS

3.1 General

Determinar la viabilidad de una unidad de negocio que permita implementar métodos y procedimientos basados en redes 802.11 (Wifi) que garanticen la confidencialidad, integridad y autenticidad de los datos e información comercial de los clientes en las empresas ubicadas en Puerto Berrio.

3.2 Específicos

- ✓ Determinar si las empresas de Puerto Berrio tienen implementado un sistema de seguridad en redes 802.11x (wifi) en empresas de Puerto Berrio y en qué condiciones lo utilizan desde el punto de vista de su aplicación y configuración del Active Directory en Windows Server 2008; de su configuración del protocolo RADIUS; y, cómo funciona la generación de certificados de autentificación.

- ✓ Realizar un estudio técnico, financiero, social y ambiental para la puesta en marcha de una unidad de negocio que brinde el servicio de seguridad de redes en empresas de Puerto Berrio.

IV. MARCO REFERENCIAL

4.1 MARCO CONTEXTUAL

Identificación del municipio:

- ✓ **Nombre del municipio:** PUERTO BERRIO
- ✓ **NIT:** 890980049-3
- ✓ **Código Dane:** 05579
- ✓ **Gentilicio:** Porteños
- ✓ **Otros nombres que ha recibido el municipio:** Remolino Grande, Corazón de Colombia, Antesala y Puerta Grande de Antioquia.

4.1.1 Historia

Fecha de fundación: 01 de septiembre de 1875

Nombre del fundador: Francisco Javier Cisneros

4.1.2 Reseña histórica: El territorio de Puerto Berrío, hacía parte de la jurisdicción del Distrito de Santo Domingo del estado Soberano de Antioquia. En la vigencia del Presidente Manuel Murillo Toro, y el Gobernador de Antioquia, Pedro Justo Berrío, se dio comienzo a un proyecto vial que comunicara a Medellín con el río Magdalena por una ruta carreteable.

En 1871, el doctor Berrío dicto el Decreto que dispuso la apertura de un camino permanente para llegar al río Magdalena, se ejecutó hasta Barbosa. Se modificó luego por la construcción de una línea férrea, idea del mismo Pedro Justo Berrío, le correspondió a su sucesor, el doctor Recadero Villa Giraldo, adelantar la negociación con el Ingeniero cubano Francisco Javier Cisneros la obra que Antioquia emprendería.

El 27 de noviembre de 1874, Cisneros desembarcó en Puerto Berrío, iniciando los trabajos. El punto de partida tuvo una variación y fue localizado en el sitio “Remolino Grande” (sector sur de la zona urbana actual). En 1875, en honor al doctor Pedro Justo Berrío, se divide en dos (2) la fracción de la Magdalena, y una con el nombre de Puerto Berrío. En este mismo año, en el sitio “la Milla”, se colocó el primer riel; cinco años después se habían instalado 13 kilómetros.

Debido a su población y al gran auge económico en 1881, Puerto Berrío fue elevado a nivel de Distrito. En 1885, se da al servicio un tramo de 45 kilómetros del ferrocarril. En 1908 la línea llegaba hasta la estación Sofía y paralelamente se construía el tramo de Porce-Medellín en 1914. En 1929, se construye el túnel de la quiebra, obra monumental en su clase (6° lugar en el mundo) y conectándose a través de ella los 338 kilómetros de línea de ferrocarril existente.

Esta obra junto al desarrollo de empresas navieras, conectaban el interior del país con el mundo, utilizando la vía fluvial del rio Magdalena; razón por la cual hasta los 70, la vida de Puerto Berrío, giraba en torno a estas actividades. Luego, fenómenos sociales, políticos, económicos y culturales de gran impacto, hacen que el municipio entre en una profunda crisis.

Nuevas actividades, fenómenos de violencia, migraciones de diferentes grupos culturales, hacen que se modifiquen las normas de comportamiento, ideas, creencias, usos, costumbres y expresiones artísticas. Actualmente, Puerto Berrío está en un proceso de auto-reconocimiento cultural, durante algunos años, la gente creyó que la dificultad para reconocernos como habitantes paisas, costeños, pastusos, algo rolos, santandereanos y hasta llaneros, era sinónimo de la falta de una cultura municipal.

Hoy sin embargo debemos considerar estas condiciones propias como una ventaja y como el elemento principal para la transformación de nuestro municipio en la “CIUDAD REGIÓN” que motive y dinamice el desarrollo y sobre todo, como

un elemento cultural nuevo, la transculturalidad o cultura de los múltiples valores que trascienden lo espacial.

4.1.3 Descripción Física - Geografía:

Localización:

REGIÓN: Magdalena Medio (Oriente del Departamento)

EXTENSIÓN: 1.184 Km^2

ALTURA: 125 m.s.n.m.

TOPOGRAFÍA: Características de valle ribereño, alturas y pendientes considerables hacia la cordillera occidental; colinas y mesetas de poca altura entre este y el valle ribereño, 125 mts. m.s.n.m. Alto del Abismo, Alto del indio, Chipre, De la Virgen, San Martín, Ugayca.

TEMPERATURA: 29° C (promedio).

LATITUD: Norte 6º29'35'' y Longitud Este 74º24'26''

Límites del municipio:

Norte: Remedios y Yondó
Nor – Occidente: Yolombó
Occidente: Maceo y Caracolí
Sur: Puerto Nare
Oriente: Río Magdalena, Departamento de Santander y Boyacá.

Extensión total: 1.184 Km2 Km^2

Extensión área urbana: 5.6 Km^2

Extensión área rural: 1.178,5 Km^2

Altitud de la cabecera municipal (metros sobre el nivel del mar): 125 m.s.n.m.

Temperatura media: 29° C (promedio). º C

Distancia de referencia: 192 Km de Medellín.

Fuente. Alcaldía de Puerto Berrio. Disponible en línea en URL: http://www.puertoberrio-antioquia.gov.co/mapas_municipio.shtml?apc=bcxx-1-&x=2783307

4.2 MARCO TEÓRICO

La seguridad en redes inalámbricas[1]. Los múltiples motivos por los cuales merece importancia la seguridad de las redes inalámbricas es por causas que demuestran el desmejoramiento de la calidad de la señal, la transferencia de datos y perdida de la misma.

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

La falta de confianza en esta tecnología por parte de los responsables de T.I., posiblemente el principal factor que ralentiza su despegue, tiene cierto fundamento. Tras la publicación de los primeros estándares que determinaron el nacimiento de las redes wireless ethernet (IEEE 802.11a y b), también denominadas Wi-Fi por el consorcio que empuja su implantación e interoperabilidad de los productos, surgió la necesidad inmediata de proporcionar un protocolo que proporcionase seguridad frente a intrusiones en este tipo de transmisiones: WEP (Wired Equivalent Privacy). Este protocolo proporciona tres mecanismos de seguridad (por nombre de la red o SSID, por clave estática compartida y por autentificación de dirección MAC) que se pueden utilizar por separado pero que es más recomendable combinarlos. Sin embargo pronto se descubrió que todos ellos eran fácilmente desbloqueados en corto tiempo (incluso minutos) por expertos utilizando herramientas de escucha en redes (sniffers). Para paliar este grave inconveniente, se han diseñado soluciones no estandarizadas apuntando en diferentes áreas.

[1] La seguridad en Redes Inalámbricas. Disponible en línea desde la URL: http://redesinl.galeon.com/aficiones1342927.html

La primera de ellas es sustituir el mecanismo de clave estática por uno de clave dinámica WEP (TKIP u otros), lo que dificulta su identificación, puesto que el tiempo de computación que lleva es mayor que la frecuencia de cambio. Sin embargo debe ser complementada con otras técnicas como sistemas Radius para forzar la identificación del usuario, túneles VPN con cifrado IPSEC o análogo entre el terminal de usuario y un servidor seguro interno para imposibilitar el análisis de las tramas enviadas por radio.

Los consorcios reguladores, conscientes de la gravedad de esta debilidad y su fuerte impacto negativo en el crecimiento de las WLAN, han propuesto una recomendación provisional denominada WPA (Wi-Fi Protected Access) que conjuga todas las nuevas técnicas anteriormente expuestas. Se estima que a mediados del 2003 los productos Wi-Fi incorporen este mecanismo.

Desafortunadamente WPA no es el último movimiento: realmente es un subconjunto de una especificación final que prepara el consorcio IEEE que se denominará 802.11i y que pretende ser la clave definitiva para que las redes ethernet inalámbricas puedan ser equiparables en materia de seguridad a las cableadas. De nuevo seguramente habrá que esperar hasta el 2004 para que se cierre la recomendación y la incorporen los equipos.

Para resolver los problemas de seguridad, se han hecho investigaciones que arrojan un significativo número de usuarios y empresas que dejan al descubierto la información, los motivos apuntan al desconocimiento respecto a configuraciones que ofrecen seguridad en las organizaciones y que además es aplicable en las redes pequeñas de los hogares.

WEP, acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza

claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV).

Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

Comenzando en 2001, varias debilidades serias fueron identificadas por analistas criptográficos. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. Unos meses más tarde el IEEE creó la nueva corrección de seguridad 802.11i para neutralizar los problemas. Hacia 2003, la Alianza Wi-Fi anunció que WEP había sido reemplazado por Wi-Fi Protected Access (WPA). Finalmente en 2004, con la ratificación del estándar completo 802.11i (conocido como WPA2), el IEEE declaró que tanto WEP-40 como WEP-104 fueron revocados por presentar fallos en su propósito de ofrecer seguridad.

A pesar de sus debilidades, WEP sigue siendo utilizado, ya que es a menudo la primera opción de seguridad que se presenta a los usuarios por las herramientas de configuración de los routers aun cuando sólo proporciona un nivel de seguridad que puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección. Fue desaprobado como un mecanismo de privacidad inalámbrico en 2004, pero todavía está documentado en el estándar actual.

WEP es a veces interpretado erróneamente como Wireless Encryption Protocol.

Pasos para asegurar una red inalámbrica[2]. En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático. Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99.99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%. No es cierto. Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener.

Una vez situados vamos a ver los pasos que podemos seguir para introducir una seguridad razonablemente alta a nuestra red wireless. Debemos tener en cuenta que cuando trabajamos con una red convencional cableada disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma. En nuestro caso no, de hecho vamos a estar desperdigando la información hacia los cuatro vientos con todo lo que esto conlleva.

✓ **Paso 1**, debemos activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el/la cajero/a de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.

✓ **Paso 2**, debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por oes.

[2] Ibid.

✓ **Paso 3**, uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

✓ **Paso 4**, desactivar el DHCP y activar el ACL. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

✓ **Paso 5**, Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial reconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

✓ **Paso 6**, hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

✓ **Paso 7**, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall que filtre el tráfico entre los dos segmentos de red.

Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos wireless

realmente seguros. También, en este sentido hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de éstas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad. Posiblemente algún día estos métodos se conviertan en estándar.

4.3 MARCO CONCEPTUAL

- ✓ **Protocolos de Seguridad Estándar IEEE 802.11**

La expresión Wi-Fi, *Wireless Fidelity*, se utiliza genéricamente para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación inalámbricas conocidas como WLAN. En un principio, la expresión Wi-Fi se utilizó para los aparatos con tecnología 802.11b, el estándar dominante en el desarrollo de las redes inalámbricas de aceptación prácticamente universal. Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11: 802.11b, 802.11a, 802.11g.

Wi-Fi Alliance (anteriormente WECA, "*Wireless Ethernet Compatibility Alliance*") es una organización internacional, sin ánimo de lucro, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de redes de área local basados en la especificación del IEEE 802.11. Organizaciones de este tipo son totalmente imprescindibles para promover una determinada tecnología y lograr que los productos tengan la calidad requerida y la interoperabilidad necesaria.

Figura No. 1: Logo Alliance-"*Wireless Ethernet Compatibility Alliance*"
Fuente: Fundamentos de la Radiodifusión (2006)

- ✓ **Evolución Histórica Wireless y el Estándar IEEE 802.11**

- 1986: Primeras LANs inalámbricas. 860 Kb/s. Banda de 900 MHz (no disponible en Europa).
- 1993: Primeros sistemas propietarios de 1 y 2 Mb/s en banda de 2,4 GHz
- 1997: El IEEE aprueba estándar 802.11. 1 y 2 Mb/s (2,4 GHz e infrarrojos)
- 1998: Primeros sistemas pre-estándar 802.11b (11 Mb/s a 2,4 GHz)
- 1999: El IEEE aprueba suplementos 802.11b (hasta 11 Mb/s en 2,4 GHz) y 802.11a (hasta 54 Mb/s en 5 GHz)
- 12/2001: Primeros productos comerciales 802.11ª
- 12/2001: Publicación borrador 802.11e (QoS en WLANs)
- 2003: El IEEE ratifica 802.11g (hasta 54 Mb/s en 2,4 GHz)

- ✓ **Estándares Wi-Fi 802.11**

802.11 fue publicado en 1997, constituyéndose en el primero de los estándares definidos por el IEEE para aplicaciones WLAN. Funciona sobre infrarrojos y en la banda de 2,4 GHz permitiendo dos tipos de modulaciones:

- DSSS (*Direct Sequence Spread Spectrum*) o

- FHSS (*Frequency Hopped Spread Spectrum*)

La velocidad de transmisión que es capaz de alcanzar está entre 1 ó 2 Mbps, dependiendo del fabricante. Este estándar está prácticamente en desuso.

✓ **Estándares WI-FI 802.11b**

En 1999 se ratifica 802.11b, evolución natural de 802.11, diferenciándose en el uso exclusivo de la modulación DSSS (Acrónimo de "Direct Sequence Spread Spectrum", sistema de transmisión de datos usado por las redes sin hilos) con el sistema de codificación CCK. Este estándar lideró el tremendo éxito de las redes inalámbricas. Velocidades de transmisión: 1, 2, 5.5, y 11 Mbps.

Introduce la característica, denominada DRS (*Dynamic Rate Shifting*) que permite a los adaptadores de red inalámbricos reducir las velocidades para compensar los posibles problemas de recepción que se pueden generar por las distancias o los materiales que es necesario atravesar (paredes, tabiques, etc.).
En cuanto a las distancias a cubrir, dependerá de las velocidades aplicadas, del número de usuarios conectados y del tipo de antenas y amplificadores que se puedan utilizar.

- Entre 120m (a 11 Mbps) y 460m (a 1 Mbps) en espacios abiertos
- Entre 30m (a 11 Mbps) y 90m (a 1 Mbps) en interiores.

✓ **Estándar WI-Fi 802.11ª**

En 1999, simultáneamente a 802.11b, se ratifica también el estándar 802.11a, este utiliza la banda de frecuencia de 5 GHz y como técnica de modulación de radio OFDM (*Ortogonal Frequency Division Multiplexing*). Aumenta la velocidad de transmisión hasta 54 Mbps. Dispone de hasta 8 canales sin solapamiento, con el consiguiente aumento en la capacidad para las comunicaciones simultáneas.

Desventajas: Mayor nivel de consumo, Incompatibilidad con 802.11b al usar la banda de 5GHz, las distancias de cobertura se ven reducidas significativamente:

- 30 m (54 Mbps) y 300 m (6 Mbps) en exteriores
- 12 m (54 Mbps) y 90 m (6 Mbps) en interiores

✓ **Estándares Wi-Fi 802.11g**

En junio del 2003 se aprueba un nuevo estándar, 802.11g, basado en la norma 802.11b. Funciona en la banda de 2,4 GHz y es capaz de utilizar dos métodos de modulación DSSS (previenen interferencia separando la señal hacia fuera sobre varias frecuencias contemporáneamente. Es decir DSSS toma un octeto de datos, fractura en varios pedazos, y envía los pedazos hacia fuera en el mismo tiempo multiplexándolos sobre diversas frecuencias.

Mientras que se selecciona el octeto siguiente entonces se divide y el excedente es enviado a otro sistema de frecuencias. Esto ayuda a la anchura de banda del aumento y permite que los dispositivos múltiples funcionen un WLAN. Mientras no choquen los dominios del tiempo y de la frecuencia, seguirá habiendo datos intactos) y OFDM (puede conseguir a muchas más épocas los datos que pasan durante un ciclo, es decir, permite una frecuencia más grande dividirla en frecuencias más pequeñas para permitir su propia transmisión de datos.

Esto aceleró no sólo la transmisión de datos, sino también permite frecuencias múltiples, y reduce así la colisión con otras transmisiones sin hilos del dispositivo), lo que le hace compatible con el estándar de facto, 802.11b.

Este nuevo estándar es capaz de incrementar notablemente la velocidad de transmisión, pudiendo llegar hasta los 54 Mbps que ofrece la norma 802.11a, aunque manteniendo las características propias de 802.11b en cuanto a distancia,

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

- ✓ **Componentes de una red Wi-Fi**

El Punto de Acceso: Dispositivo que nos permite comunicar todos los elementos de la red con el Router. Cada punto de acceso tiene un alcance máximo de 90 metros en entornos cerrados. En lugares abiertos puede ser hasta tres veces superior.

Tarjeta de Red Wireless: Permite al usuario conectarse en su punto de acceso más próximo.

Router: Permite conectarse un Punto de Acceso a Internet.

- ✓ **Medios de Transmisión.**

▪ **Infrarrojos:** los mandos a distancia basados en transmisión por infrarrojos está ampliamente extendido en el mercado residencial para telecomandar equipos de audio y vídeo.

La comunicación se realiza entre un diodo emisor que emite una luz en la banda de IR, sobre la que se superpone una señal, convenientemente modulada con la información de control y un fotodiodo receptor cuya misión consiste en extraer de la señal recibida la información de control.

Los controladores de equipos domésticos basados en la transmisión de ondas en comodidad y la banda de los infrarrojos tienen varias ventajas, tales como, que admiten gran número de aplicaciones, flexibilidad, es inmune a las radiaciones electromagnéticas producidas por los equipos domésticos o por los demás medios

de transmisión (coaxial, cables pares, red de distribución de energía eléctrica, etc.). Sin embargo, también presenta interferencias electromagnéticas que afectan a los extremos del medio IR, es decir, a partir de los dispositivos optoelectrónicos (diodo emisor y fotodiodo).

- **Radiofrecuencias:** este medio de transmisión puede parecer, en principio, idóneo para el control a distancia de los sistemas domóticos, dada la gran flexibilidad que supone su uso. Sin embargo resulta particularmente sensible a las perturbaciones electromagnéticas producidas, tanto por los medios de transmisión, como por los equipos domésticos. Presenta alta sensibilidad, dificultad para la fácil intervención de las comunicaciones, interferencias, integración de las funciones de control y comunicación, en su modalidad de transmisión analógica.

- **Internet por microondas:** el servicio utiliza una antena que se coloca en un área despejada sin obstáculos de edificios, árboles y otras cosas que pudieran entorpecer una buena recepción en el edificio o la casa del receptor y se coloca un módem que interconecta la antena con la computadora. La comunicación entre el módem y la computadora se realiza a través de una tarjeta de red, que deberá estar instalada en la computadora. Este proceso se lleva a cabo en fracciones de segundo.

Es un tipo de red muy actual, usada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una Red de ordenadores. Los dispositivos inalámbricos que permiten la constitución de estas redes utilizan diversos protocolos como el Wi-Fi: El estándar IEEE 802.11. El cual es para las redes inalámbricas, lo que Ethernet para las redes de área local (LAN) cableadas. Además del protocolo 802.11 del IEEE existen otros estándares como el Home RF, Bluetooth y Zig Bee.

- ✓ **Métodos de Configuración Segura**

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas.

Es importante destacar que en conjunto se pueden mejorar o fortalecer las debilidades y convertir la comunicación de la red más segura, pues cada uno de ellos puede ser conexión, protocolos, canal, etc. Se detalla cada uno de ellos, con su funcionamiento principal y las desventajas de la posible vulnerabilidad o riesgo.

- ✓ **Filtrado de direcciones MAC**

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso.

- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.

- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack6 o WellenReiter, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.

- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración. Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

✓ Protocolo WEP

Para proteger los datos que se envían a través de las WLANs, el estándar 802.11b define el uso del protocolo WEP (Wired Equivalent Privacy). WEP intenta proveer de la seguridad de una red con cables a una red Wireless, encriptando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace). Este protocolo está basado en el algoritmo de encriptación RC4 (genera un flujo pseudoaleatorio de bits que, para cifrar, se combina con el texto plano usando la función XOR como en cualquier Cifrado Vernam. La fase de descifrar el mensaje se realiza del mismo modo), y utiliza claves de 64bits o de 128bits.

En realidad son de 40 y 104 bits, ya que los otros 24 bits van en el paquete como Vector de Inicialización (IV). La llave de 40 ó 104 bits, se genera a partir de una clave estática de forma automática, aunque existe software que permite introducir esta llave manualmente. La clave debe ser conocida por todos los clientes que quieran conectarse a la red wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.

A partir de la clave se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

Como se puede observar en la figura Nº 2 para generar las llaves se realiza una operación XOR con la cadena ASCII que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudoaleatorios (PRNG) para generar 40 cadenas de 32 bits cada una. Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves solo se utiliza una para realizar la encriptación WEP.

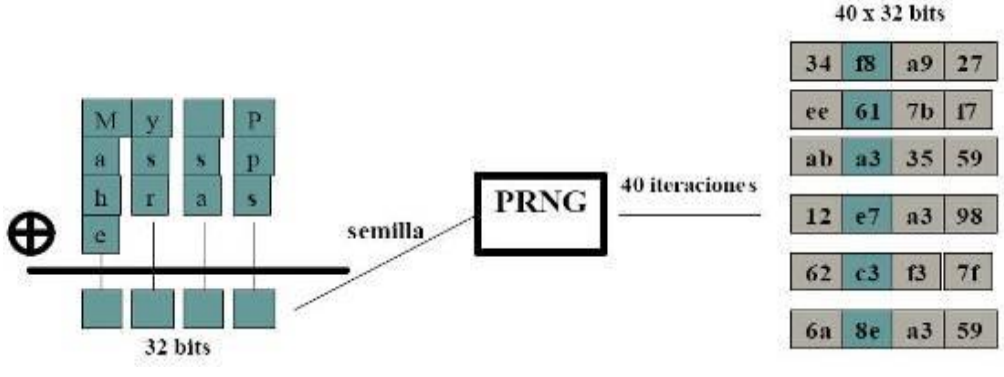


Figura No. 2: Generación de Llaves Protocolo WEP
Fuente: Átaro Wireless (http://www.matarowireless.net)

- ✓ **Proceso de Encriptar una Trama con WEP**

Se inicia a partir de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar.

El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como valor de chequeo de integridad (ICV:Integrity Check Value):

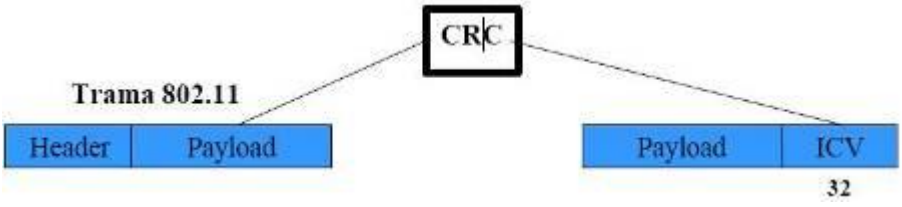


Figura No. 3: Trama Valor de Chequeo de Integridad
Fuente: Átaro Wireless (http://www.matarowireless.net)

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:

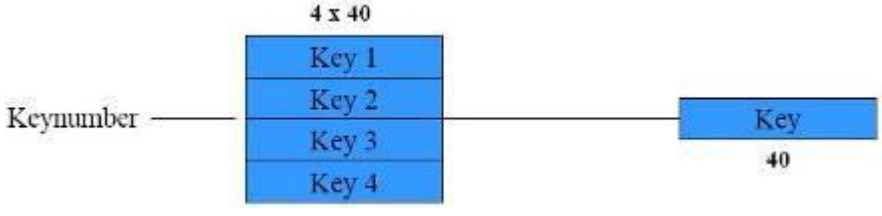


Figura No. 4: Llaves de 40 bits
Fuente: Átaro Wireless (http://www.matarowireless.net)

Y añadimos el Vector de Inicialización (IV) de 24 bits al principio de la llave seleccionada:

Figura No. 5: Estructura del vector de inicialización
Fuente: Átaro Wireless (http://www.matarowireless.net)

El IV es simplemente un contador que suele ir cambiando de valor a medida que se van generando las tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama.

En el caso de utilizar encriptación de 128 bits se tendría 24 bits de IV y 104 de llave. Luego se aplica el algoritmo RC4 al conjunto IV+Key y conseguiremos el

keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload+ICV obtendremos el Payload+ICV cifrado, este proceso puede verse en la figura.

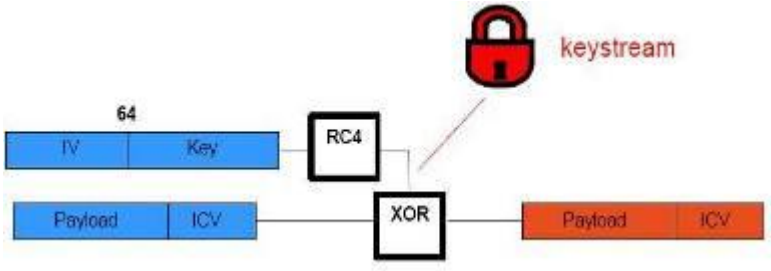


Figura No. 6: Generación de Llaves Protocolo WEP
Fuente: Átaro Wireless (http://www.matarowireless.net)

Después añadimos la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva, lista para ser enviada:

Figura No. 7: Cabecera de la Trama Llaves Protocolo WEP
Fuente: Átaro Wireless (http://www.matarowireless.net)

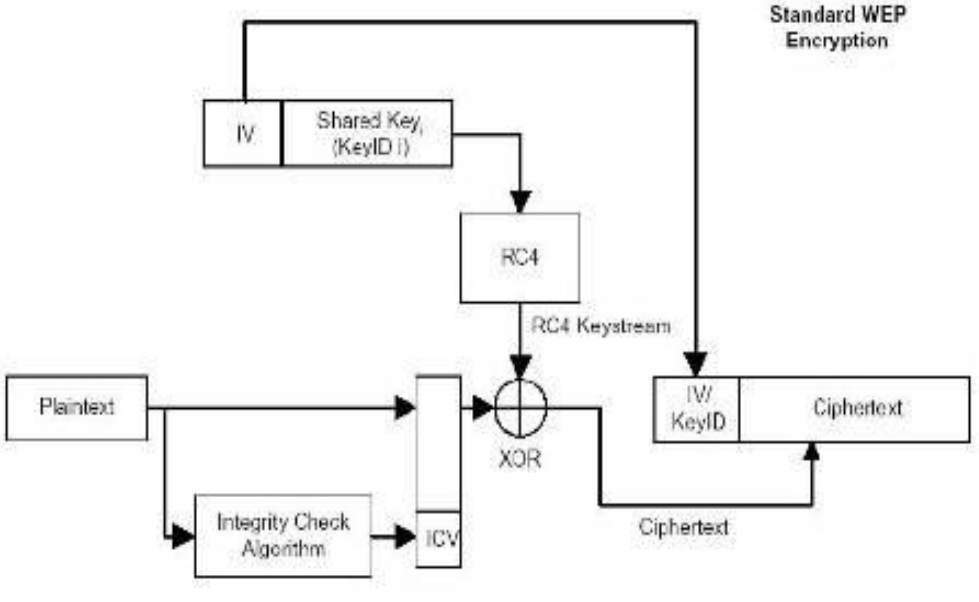


Figura No. 8: Esquema del proceso de Encriptación
Fuente: Átaro Wireless (http://www.matarowireless.net)

Proceso de Desencriptar una trama con WEP

Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama:

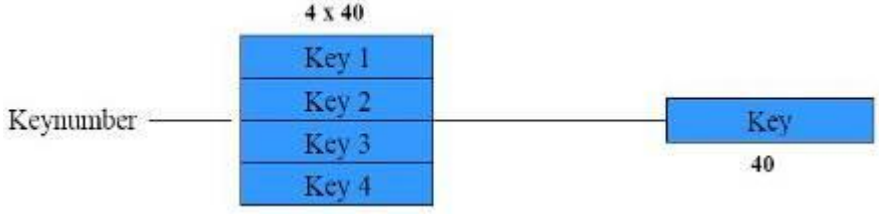


Figura No. 9: Desencriptar trama
Fuente: Átaro Wireless (http://www.matarowireless.net)

Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa. Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original.

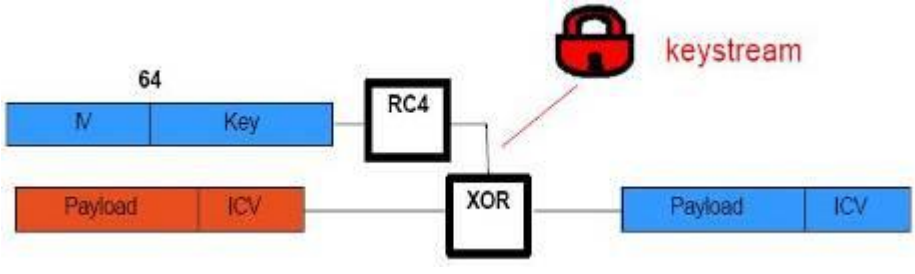


Figura No.10: Estructura trama aplicando RC4 y XOR
Fuente: Átaro Wireless (http://www.matarowireless.net)

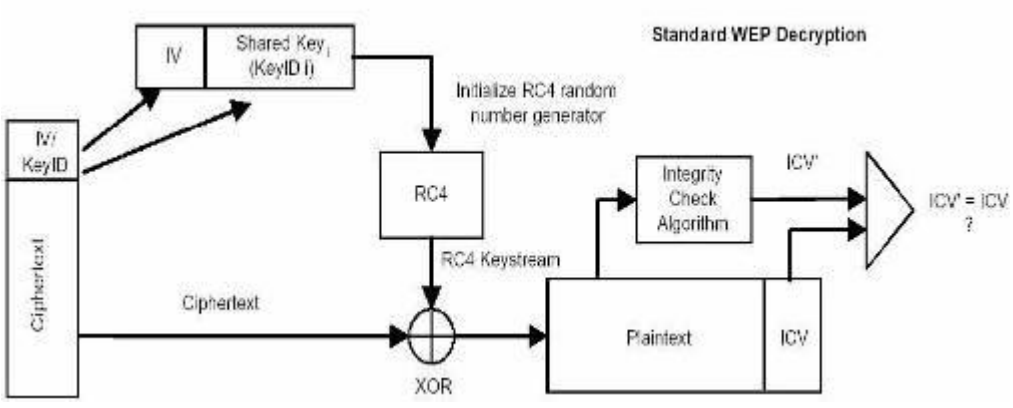


Figura No. 11: Estructura resumen del proceso de desencriptar
Fuente: Átaro Wireless (http://www.matarowireless.net)

- ✓ **Mecanismos de Autenticación**

Open System Authentication: es el protocolo de autenticación por defecto para 802.11b. Como su nombre indica, este método autentica a cualquier cliente que pide ser autenticado. Es un proceso de autenticación NULO, las tramas se mandan en texto plano aunque esté activado el cifrado WEP.

Shared Key Authentication: este mecanismo utiliza una clave secreta compartida, que conocen cliente y AP. El siguiente esquema muestra el proceso de autenticación descrito a continuación:

Figura No. 12: Esquema de autenticación

Fuente: Adtech (http://www.adtech.info)

La estación que quiere autenticarse (cliente), envía una trama AUTHENTICATION REQUEST indicando que quiere utilizar una “clave compartida”. El destinatario (AP) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente.

El texto del desafío se genera utilizando el PRNG (generador de números pseudoaleatorios de WEP) con la clave compartida y un vector de inicialización (IV) aleatorio. Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el payload de una nueva trama, que encripta con WEP utilizando la clave compartida (*passphrase*) y añade un nuevo IV (elegido por el cliente). Una vez construida esta nueva trama encriptada, el cliente la envía al AP, y éste desencripta la trama recibida y comprueba que:

- El ICV (Integrity Check Value) sea válido (CRC de 32 bits).
- El texto de desafío concuerde con el enviado en el primer mensaje.

Si la comprobación es correcta, se produce la autenticación del cliente con el AP y entonces se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el AUTHENTICATION REQUEST es el AP. De esta manera se asegura una autenticación mutua. En la siguiente figura se muestra el formato de una trama de autenticación. Este formato es utilizado para todos los mensajes de autenticación:

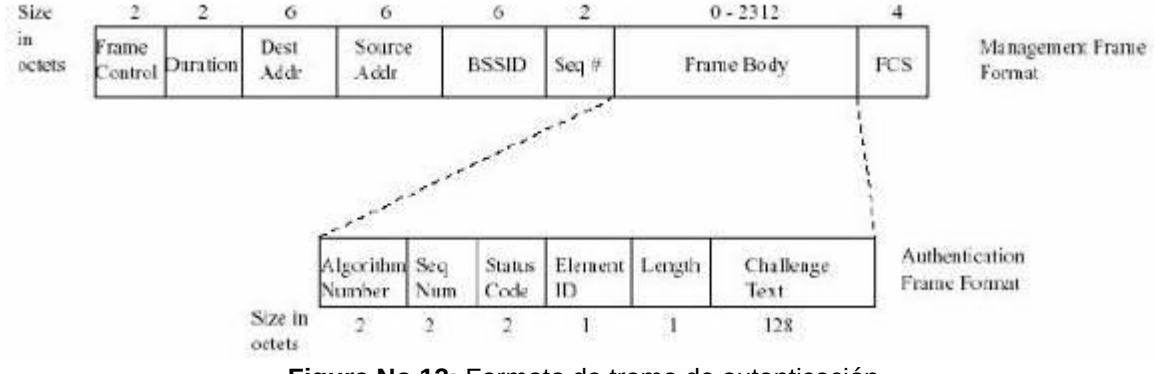


Figura No.13: Formato de trama de autenticación
Fuente: Universidad de Ibague (http://www.universidad de Ibagué)

Si el campo “Status Code” tiene valor ‘0’ indica que la autenticación ha sido realizada con éxito, si no contiene un código de error. El campo “Element identifier” indica que la trama contiene el texto de desafío. El campo “Length” indica la longitud del texto de desafío y está fijado a 128 bits. El campo “Challenge text” incluye el texto de desafío aleatorio.

- ✓ **Deficiencias en la Encriptación WEP**

- **Características lineares de CRC32:** esta vulnerabilidad fue demostrada teóricamente por Nikita Borisov, Lan Goldberg y David Wagner (Universidad de Berkeley). El campo ICV (Integrity Check Value) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje. Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

  - Los CRCs son independientes de la llave utilizada y del IV
  - Los CRCs son lineares: CRC (m Å k) = CRC(m) Å CRC(k)

Debido a que los CRCs son lineares, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es lineal y esto permite hacer el ‘*bit flipping*’. Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m’: **m’ = m Å D**

- Como el CRC-32 es lineal, puede generar un nuevo ICV’ a partir del ICV de m: **IC’ = IC Å h(D)**
- ICV’ será válido para el nuevo cyphertext c’

  c’ = c Å D = k Å (m Å D) = k Å m’

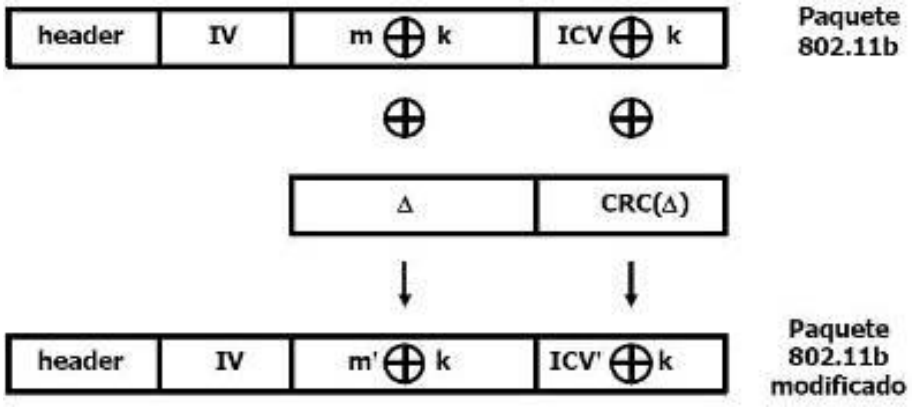


Figura No. 14: Trama paquete original vs paquete modificado
Fuente: Adtech (http://www.adtech.info)

4.4 MARCO LEGAL

Todo uso y seguimiento de uso a los recursos TI debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en la materia, incluido pero no restringido a:

- Constitución Política de Colombia, 1991.
- Ley 527 de 1999, Ley de comercio electrónico.
- NTC 27001:2006 Sistema de Gestión de Seguridad de la Información.
- Ley 1273 de 2009 de la protección de la información y de los datos**,** como ley oficial de los delitos informáticos en Colombia, sin embargo al final de la ponencia, uno de los evaluadores me indico que estaba errado porque: “En Colombia no existe una ley oficial para los delitos informáticos”.

El Ministerio de Comunicaciones de Colombia publicó la resolución con número 0689 de 21 de abril de 2004 que asigna las frecuencias para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, y se dictan otras disposiciones.

La resolución designa seis bandas como espectro no regulado y, además, establece especificaciones de modo que las redes de área local no interfieran con otros servicios de telecomunicaciones.

Las seis bandas incluyen el rango de 902-928MHz, 2.400-2.483,5MHz y cuatro bandas que van desde 5.150MHz hasta 5.850MHz.

Los proveedores de servicio no necesitan una licencia para usar el espectro, pero sí deben adquirir una concesión, como por ejemplo una licencia de servicios de valor agregado en el caso de acceso a internet.

D. Andina 351: Protección de autores / convenio antipiratería. Capítulo VII: sobre ordenador y bases de datos L 1520 medidas tecnológicas de protección y ajustes al TLC.

V. ESTUDIO DE MERCADO Y COMERCIALIZACIÓN

5.1 El producto

Es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.

El protocolo involucra tres participantes:

- ✓ Suplicante o cliente, que desea conectarse con la red.

- ✓ El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.

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

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

Para entender cómo funciona el protocolo 802.1x sigamos el siguiente esquema:

1. El cliente, que quiere conectarse a la red, envía un mensaje de inicio de EAP que da lugar al proceso de autentificación. Por ejemplo, la persona que quiere acceder al banco pediría acceso al guardia de seguridad de la puerta.

1. El punto de acceso a la red respondería con una solicitud de autentificación EAP. En el ejemplo, el guardia de seguridad respondería solicitando el nombre y el apellido del cliente, así como su huella digital. Además, antes de preguntarle, el guarda de seguridad le diría una contraseña al cliente, para que éste sepa que realmente es un guardia de seguridad.

2. El cliente responde al punto de acceso con un mensaje EAP que contendrá los datos de autentificación. 'Nuestro cliente le daría el nombre y los apellidos al guardia de seguridad además de su huella digital'.

4. El servidor de autentificación verifica los datos suministrados por el cliente mediante algoritmos, y otorga acceso a la red en caso de validarse. En nuestro caso, el sistema del banco verificaría la huella digital, y el guardia validaría que se correspondiese con el cliente.

5. El punto de acceso suministra un mensaje EAP de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo. Nuestro guardia de seguridad le abrirá la puerta o no, en función de la verificación al cliente.

6. Una vez autentificado, el servidor acepta al cliente, por lo que el punto de acceso establecerá el puerto del cliente en un estado autorizado. Nuestro cliente estará dentro del banco. La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocolo).

VI. DISEÑO – IMPLEMENTACIÓN Y DOCUMENTACIÓN

6.1 Diseño de datos

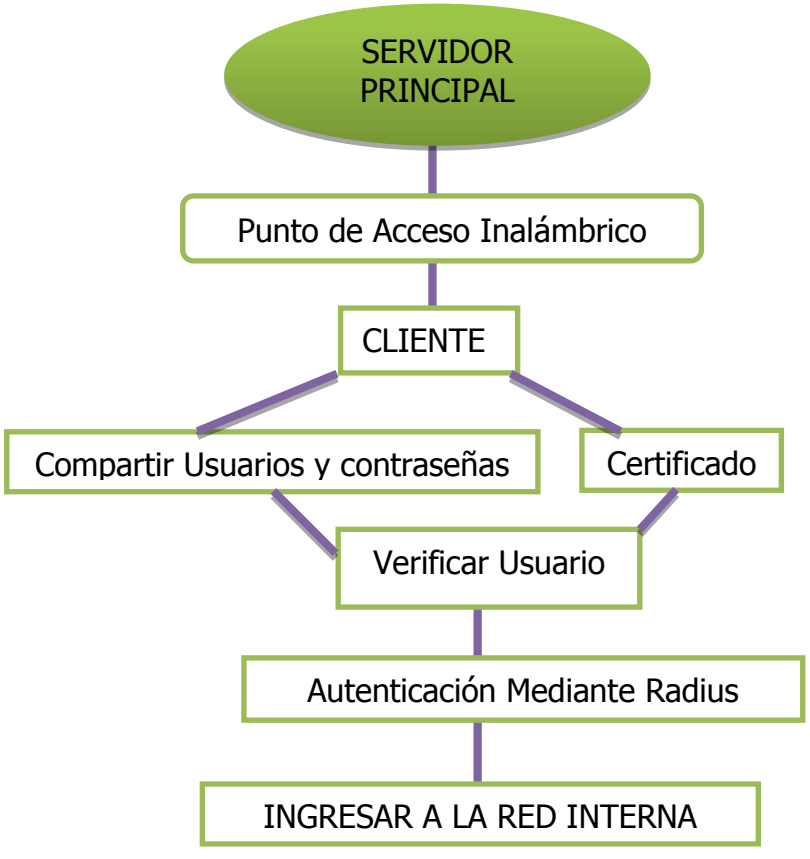


Gráfico No. 1: Diseño de datos

6.2 Diseño arquitectónico

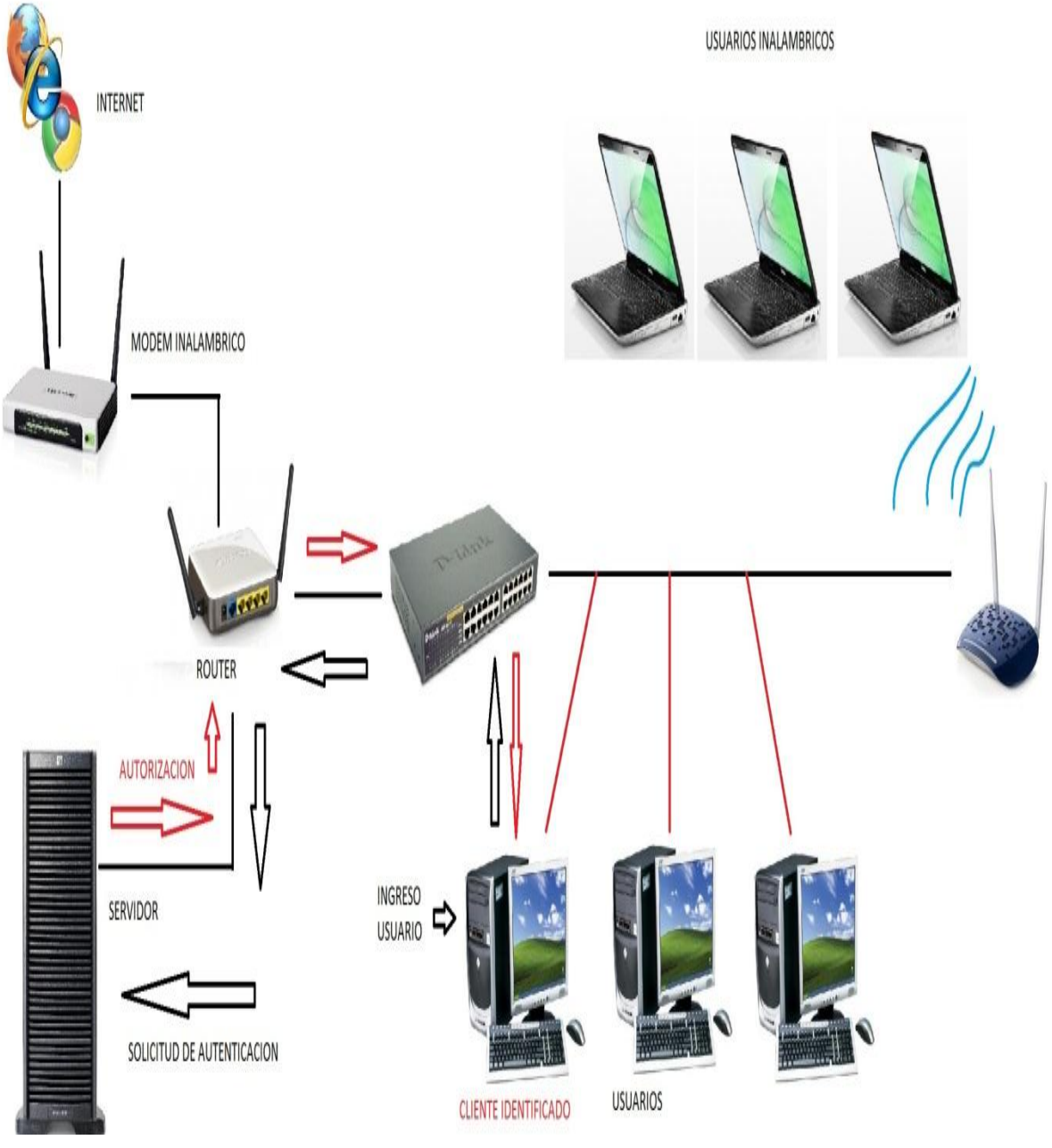


Figura No. 15: Diseño arquitectónico

6.3 Modelo funcional

6.3.1 Especificaciones de programas

RADIUS (Remote Access Dial-In User Server). Es un protocolo de autentificación, autorización y acounting de aplicaciones de acceso a la red o movilidad IP.

Cuando se hace una conexión con ISP mediante modem, DSL, Ethernet o WIFI, se envía una información que normalmente es el nombre de usuario y una contraseña.

La información recibida, se transfiere a un Servidor de Acceso sobre el protocolo PPP, quien administra la petición a un servidor RADIUS sobre el protocolo RADIUS, el servidor comprueba que la información es correcta utilizando métodos de autentificación como PAP, CHAP o EAP, si es aceptado, el servidor autorizará el acceso al sistema y le asigna los recursos de red como una dirección IP.

El protocolo RADIUS tiene la capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así al cliente se le podrá hacer seguimiento en la utilización de los recursos.

WINDOWS SERVER 2008. Es un sistema operativo predecesor de Windows server 2003, mejorando la capacidad de compartir en redes los documentos he información que los usuarios compartan mediante la conexión de una servidor o varios computadores en RED.

BACKTRACK. Es un programa diseñado por GNU/Linux para la auditoria de seguridad en redes, el cual será utilizado para comprobar la seguridad en redes de las empresas interesadas en adquirir la nuestra método de seguridad inalámbrica en redes informáticas.

MICROSOFT OFFICE. Es una suite de oficina que abarca e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos Microsoft Windows y Mac OS X, los cuales se utilizaran para la escritura y registro de todos los datos que se necesitan para la entrega del proyecto final[3].

6.3.2 Diseño de interfaz de usuario

1. El cliente inalámbrico debe establecer credenciales con el servicio de autenticación antes de que se establezca el acceso a la red inalámbrica. (Esto podría realizarse con algunos medios fuera de banda como, por ejemplo, mediante un intercambio de disquetes, o bien podría realizarse en una red segura por cable o de otro tipo.)

2. Cuando se encuentra al alcance del punto de acceso inalámbrico, el equipo cliente intenta conectarse a la WLAN activa en el punto de acceso. Para su identificación, la WLAN cuenta con un identificador del conjunto de servicios (SSID, Service Set Identifier). El cliente detecta el SSID de la WLAN y lo usa para determinar la configuración correcta y el tipo de credencial que debe utilizarse para esta WLAN específica.

3. El punto de acceso inalámbrico se configura para permitir únicamente conexiones seguras (autenticadas de 802.1X). Cuando el cliente intenta conectarse a él, el punto de acceso envía un desafío al cliente. A continuación, el punto de acceso configura un canal restringido que permite al cliente comunicarse sólo con el servidor RADIUS. Este canal bloquea el acceso al resto de la red. El servidor RADIUS solamente aceptará una conexión de un punto de acceso inalámbrico de confianza o de uno que haya sido configurado como cliente RADIUS en el servicio de autenticación de Internet (IAS, Internet Authentication

[3] MICROSOFT OFFICE. Disponible en línea URL: http://es.wikipedia.org/wiki/Microsoft_office

Service) de Microsoft y que proporcione el secreto compartido para dicho cliente RADIUS.

4. El cliente intenta realizar la autenticación con el servidor RADIUS a través del canal restringido por medio de 802.1X. Como parte de la negociación EAP-TLS, el cliente establece una sesión de seguridad de la capa de transporte (TLS, Transport Layer Security) con el servidor RADIUS. El uso de una sesión de TLS tiene las finalidades siguientes:

- Permite al cliente llevar a cabo la autenticación del servidor RADIUS, lo que significa que el cliente solamente establecerá la sesión con un servidor que cuente con un certificado de confianza.
- Permite al cliente suministrar sus credenciales de certificado al servidor RADIUS.
- Protege el intercambio de autenticación frente a intrusiones contra paquetes.
- La negociación de la sesión de TLS genera una clave que el cliente y el servidor RADIUS pueden utilizar para establecer claves maestras comunes. Estas claves se usan para derivar las claves utilizadas en el cifrado de tráfico de WLAN.

Durante este intercambio, solamente el cliente y el servidor RADIUS pueden ver el tráfico en el túnel de TLS y no queda nunca expuesto al punto de acceso inalámbrico.

5. El servidor RADIUS valida las credenciales de cliente con el directorio. Si la autenticación del cliente se lleva a cabo de forma satisfactoria, el servidor RADIUS reunirá la información que le permitirá decidir si debe autorizarse el uso de la WLAN al cliente. Utiliza información del directorio (por ejemplo, sobre la pertenencia a grupos) y las restricciones definidas en su directiva de acceso (por ejemplo, los períodos de tiempo en que se permite el acceso a la WLAN) para

conceder o denegar el acceso del cliente. Seguidamente, el servidor RADIUS transmite la decisión al punto de acceso.

6. Si se concede acceso al cliente, RADIUS transmitirá la clave maestra del cliente al punto de acceso inalámbrico. Con ello, el cliente y el punto de acceso comparten información de clave común que pueden utilizar para cifrar y descifrar el tráfico de WLAN que se desplaza entre ellos.

7. A continuación, el punto de acceso establece la conexión de WLAN del cliente con la LAN interna, lo que ofrece al cliente un acceso sin restricciones a los sistemas de la red interna. Ahora, el tráfico transmitido entre el cliente y el punto de acceso está cifrado.

8. Si el cliente requiere una dirección IP, puede solicitar una concesión del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) de un servidor en la LAN. Tras la asignación de la dirección IP, el cliente puede empezar a intercambiar información con los sistemas en el resto de la red de forma normal.

La figura siguiente muestra este proceso en más detalle.

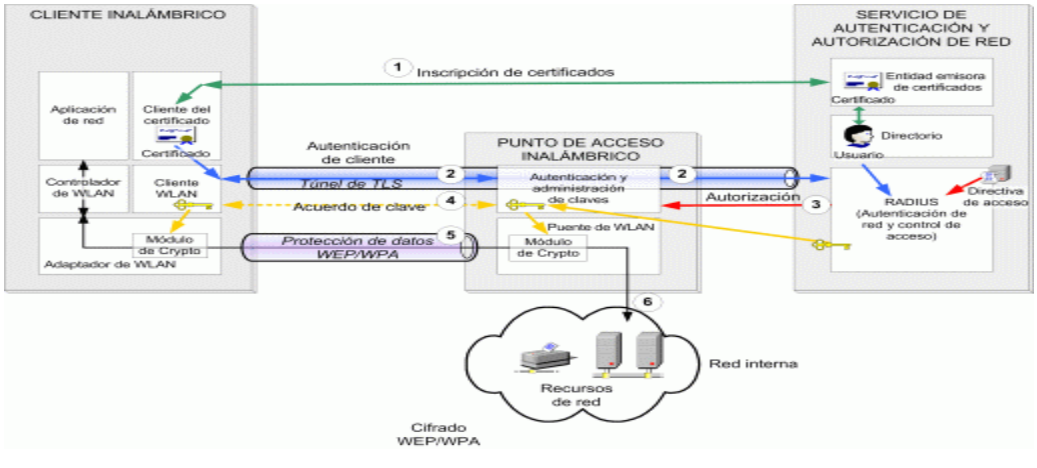


Figura No. 16: Acceso de 802.1X EAP-TLS

El diagrama anterior tomado de www.technet.microsoft.com/es-es/library muestra los componentes individuales de forma más detallada. Este diagrama da explicaciones con más claros sobre diferentes aspectos del mismo. En el proyecto tendremos en cuenta los subcomponentes del servicio de autenticación: la entidad emisora de certificados (CA), el directorio y el servidor RADIUS. Si bien conceptualmente estos subcomponentes llevan a cabo un conjunto de tareas relativamente simples, para hacerlo de manera segura, escalable, administrable y fiable, necesitan una infraestructura auxiliar muy sofisticada.

VII. DISEÑO FISICO

7.1 Diseño de seguridad y permisos

Montaje y puesta en marcha

Configuración para hacer funcional el protocolo RADIUS.

A continuación se hace explicación: Se usara Windows Server 2008 por la configuraciónlas pautas para la configuración de servidor RADIUS en el Sistema operativo Windows Server 2008.

Prerrequisitos necesarios:

- ✓ Una máquina de Windows Server 2008 ejecuta AD DS (Active Directory Domain Services)

- ✓ Una máquina de Windows Server 2008 que ejecuta NPS (Servicio de protección de red) y AD CS (Active Directory Certificate Services)

- ✓ Un WAP54G Linksys inalámbrico que soporte RADIUS

Configuración del Active Directory Domain Services

En primer lugar se hará la instalación y configuración del Directorio activo con un servidor DNS, además se creará un usuario en el dominio y que este usuario pueda arrancar desde un Windows 7.

Después de instalado el Server 2008 es cambiarle al nombre del equipo que en mi casi será SERVIDOR y se reinicia el equipo para que tome los cambios.

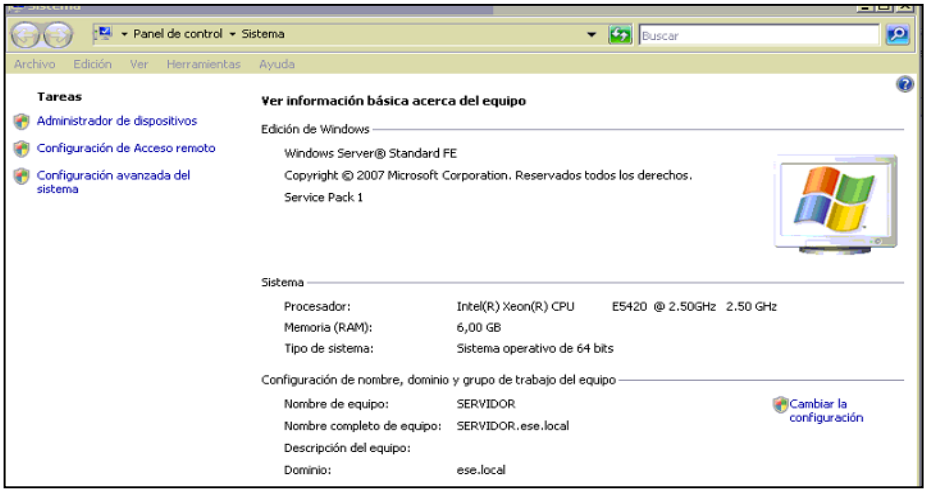


Figura 17: Propiedades del equipo

Después de reiniciado el equipo, procedemos a la instalación del active directory.

Enuncio los pasos para su instalación.

1. Administración del servidor
2. Funciones
3. Agregar Funciones
4. Elegimos servicios de dominio de Active Directory

Figura No. 18: Activación de funciones

Después de instalado el Active Directory ponemos una IP a la tarjeta de red, seleccionamos red.

Colocamos una IP que corresponda al rango que tenemos dentro del Modem, que para el caso nuestro es 190.69.88.50 y una máscara255.255.255.248 asignados por el proveedor de ISP Telefónica que es la que nos presta el servicio en nuestra entidad como IP pública. Hay que tener en cuenta que en el DNS de ir la misma dirección IP porque nuestro servidor será servidor.

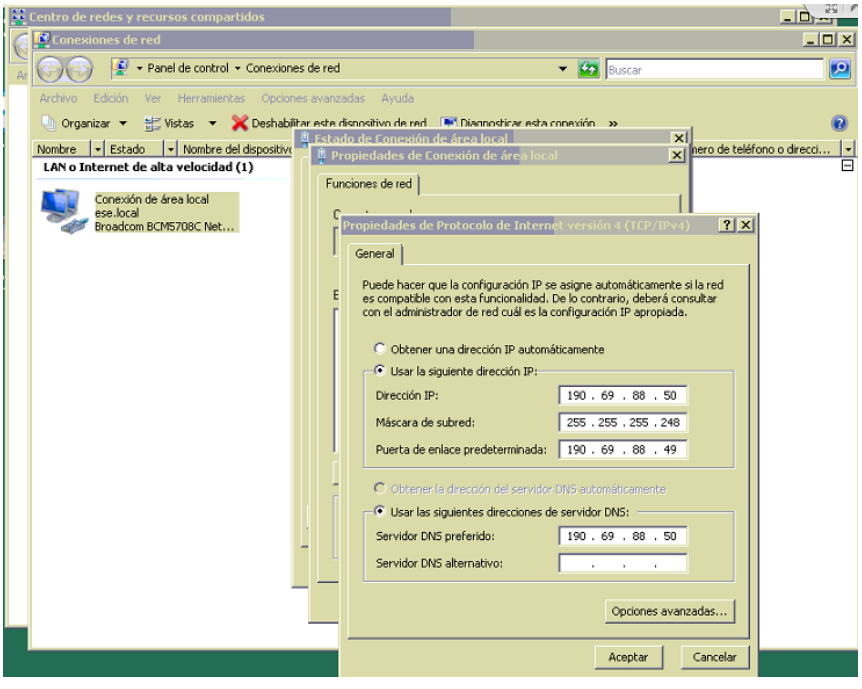


Figura No. 19: Configuración de funcionalidad de ip y dns

Damos aceptar y vamos al inicio de Windows y colocamos dcpromo y lo ejecutamos y nos aparece el asistente de instalación.

Figura No. 20: Inicio de configuración del dominio

Seleccionamos crear un dominio nuevo

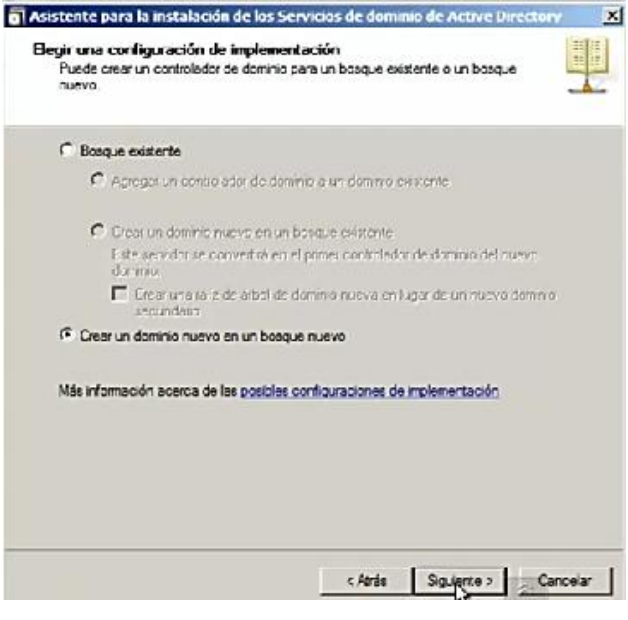


Figura No. 21: Creación de dominio

Antes de instalar la función de Active Directory Domain Server en un servidor y promoverlo a servidor de dominio, tenemos que planear la infraestructura de Active Directory.

Se debe tener decidido el nombre del dominio y de DNS que en nuestro caso será ese. local

El dominio a crear solo va a contener controladores de Windows server 2008, donde se requiere a futuro la configuración correcta del nivel funcional para beneficiarnos de todas la características de esta versión del Windows.

La configuración IP para el controlador de dominio debe ser IP estática y los valores de la máscara subred. También deberemos configurar los servidores DNS para que lleve a cabo resolución de nombres.

Se debe asignar contraseña de una cuenta al administrador. La contraseña debe existir y cuanto más compleja, mejor.

Comenzaremos desde el “administrador del servidor”, sabemos que Windows 2008 nos facilita la configuración basada en funciones, instalando solo los componentes que son indispensables para las funciones que ejecutará el servidor.

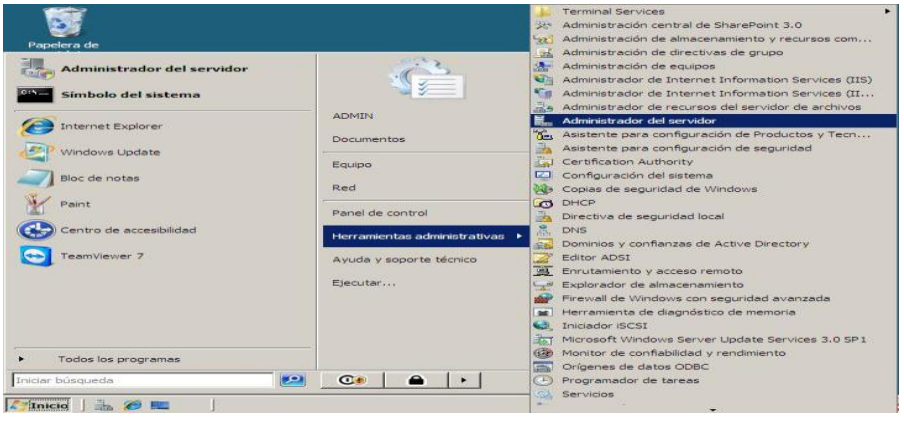


Figura No. 22: Inicio para agregar funciones

Ubicados en el link de “Funciones” hacemos click en “adicionar funciones”.

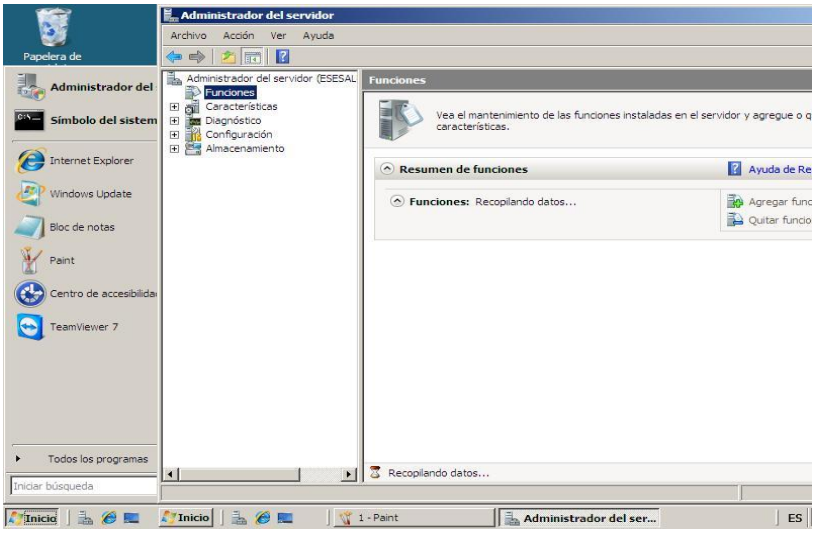


Figura No. 23: Adición de funciones

Pulsamos en “nuevo”.

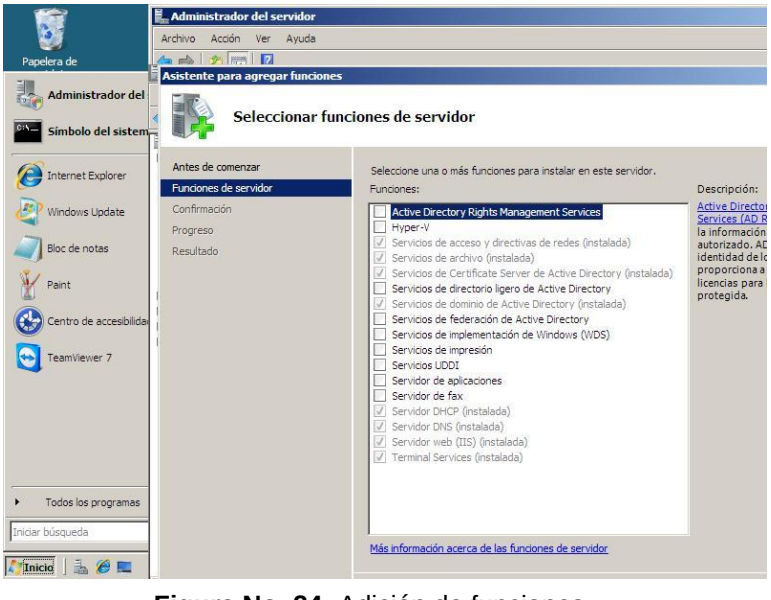


Figura No. 24: Adición de funciones

A continuación tenemos una lista de las funciones que le podemos añadir al servidor.

- ✓ Activamos la casilla de Servicios de dominio de Active Directory.
- ✓ Podemos leer lo que nos muestra para entenderlo un poco mejor.
- ✓ Después de pulsar en Instalar, comienza la instalación de AD DS.
- ✓ Al finalizar, nos muestra un resumen de la instalación que ha realizado.

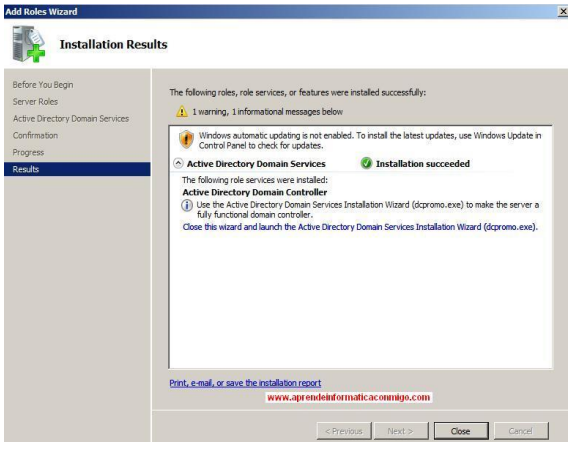


Figura No. 25: Resultado de la adición de funciones

Volvemos al administrador del servidor y ahora podemos ver que función se encuentra instalada.

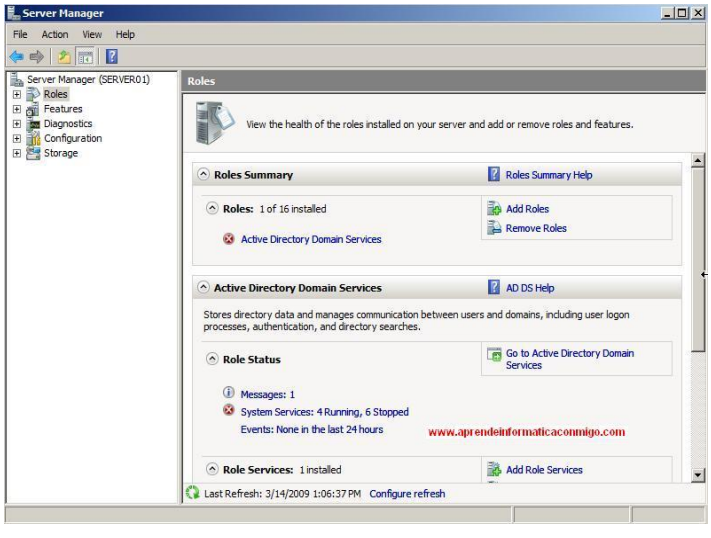


Figura No. 26: Pantalla donde se muestra la función instalada

En la parte izquierda, expandimos Funciones y seleccionamos “Active Directory y Domain Services” para que nos muestre las características del mismo:

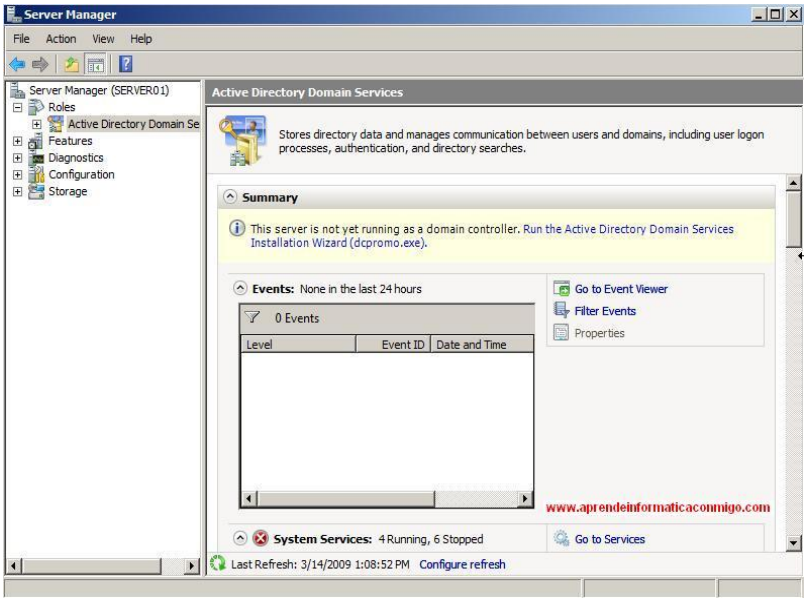


Figura No. 27: Servicios de dominio instalados

Ya tenemos instalados los Servicios de Dominio del Directorio Activo.

Configuración del sistema de autentificación con RADIUS

A continuación hago explicación de las pautas para la configuración de servidor RADIUS en el Sistema operativo Windows Server 2008.

1. En el siguiente paso, configuramos un cliente de RADIUS, así que hacemos clic en el botón agregar.

2. El cliente RADIUS será su punto de acceso inalámbrico, así que para el tipo de nombre en algo agradable para identificar el punto de acceso (para mi caso lo llamare el ClienteAP), a continuación, proporcione la dirección IP o entrada DNS para el punto de acceso.

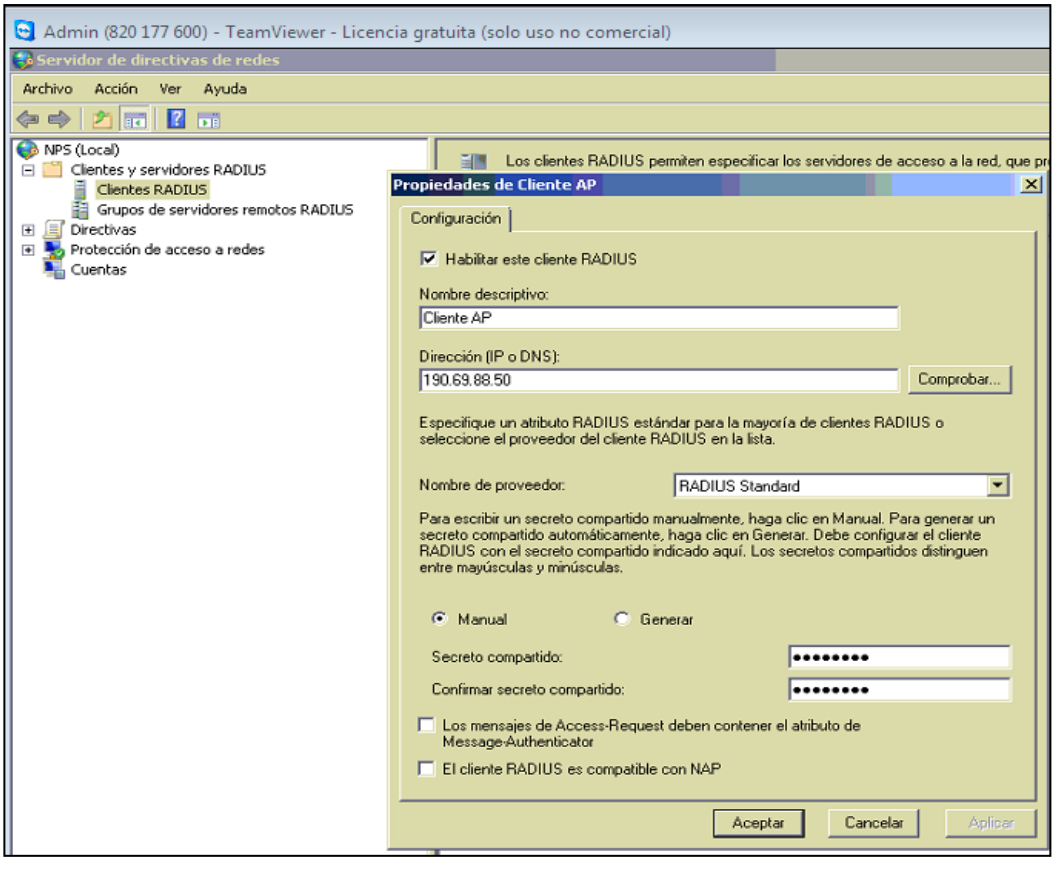


Figura No. 28: Configuración RADIUS

3. Hacemos clic en el botón Generar y, a continuación, hacemos clic en el botón manual para insertar el secreto compartido.

4. Hacemos clic en Siguiente y, a continuación, elija Microsoft: EAP protegido (PEAP) y haga clic en el botón Configurar.

5. Nos aseguramos que el certificado expedido en el cuadro desplegable tiene el certificado.

6. Hacemos clic en Siguiente y a continuación hacemos clic en el botón agregar con el fin de utilizar un grupo del Active Directory, además se debe asegurar la red inalámbrica por lo cual se debe añadir tanto las cuentas de equipo

y cuentas de usuario a este grupo para que la máquina pueda autenticar en la red inalámbrica antes de que el usuario inicia la sesión.

7. En el siguiente paso del asistente, se puede configurar la información de VLAN, de lo contrario sólo aceptan valores predeterminados para completar; Reiniciamos el servicio Servidor de directivas de redes.

Se expande l nodo Directivas ahora, veremos que el asistente ha creado una directiva de solicitud de conexión y una directiva de red que contiene los ajustes apropiados para autenticar la conexión inalámbrica.

Estas políticas individuales, obviamente, se pueden crear manualmente, pero el asistente es una manera más fácil.

También puede eliminar las opciones de autenticación menos seguro, y aumentar los métodos de cifrado en la directiva de red si así lo desea.

Con el servidor NPS configurado para aceptar peticiones de su punto de acceso inalámbrico, que ahora tendrá que configurar el punto de acceso para comunicarse con terminales. Estas instrucciones son para mi WAP54G Linksys, pero será similar a la mayoría de los puntos de acceso que soporte RADIUS.

1. Wireless En la interfaz web del punto de acceso, haga clic en la ficha Wireless y asignar un SSID apropiado;

2. Security Mode WPA-Enterprise Hacemos clic en la sub-pestaña de Seguridad y establezca el modo de seguridad WPA-Enterprise (si el punto de acceso compatible con WPA2-Enterprise, utilice esto en su lugar).

3. Encryption AES RADIUS Server Shared Secret Establecer el cifrado AES, y luego proporcionar la IP del servidor NPS como servidor RADIUS y el secreto compartido.

4. Guardar la configuración y reiniciar el punto de acceso.

Ahora el punto de acceso debe estar configurado para hablar con el servidor, por lo que todo lo que queda es configurar los clientes para conectarse.

Para configurar un cliente de Windows 7, que está unido al dominio, lo primero que debe hacerse es generar los certificados de autentificación para ello hay que activar los servicios de creación de certificados en el servidor y a su vez generarlos en cada equipo terminal.

Configuración de CA

Abrir Administrador de Servidor

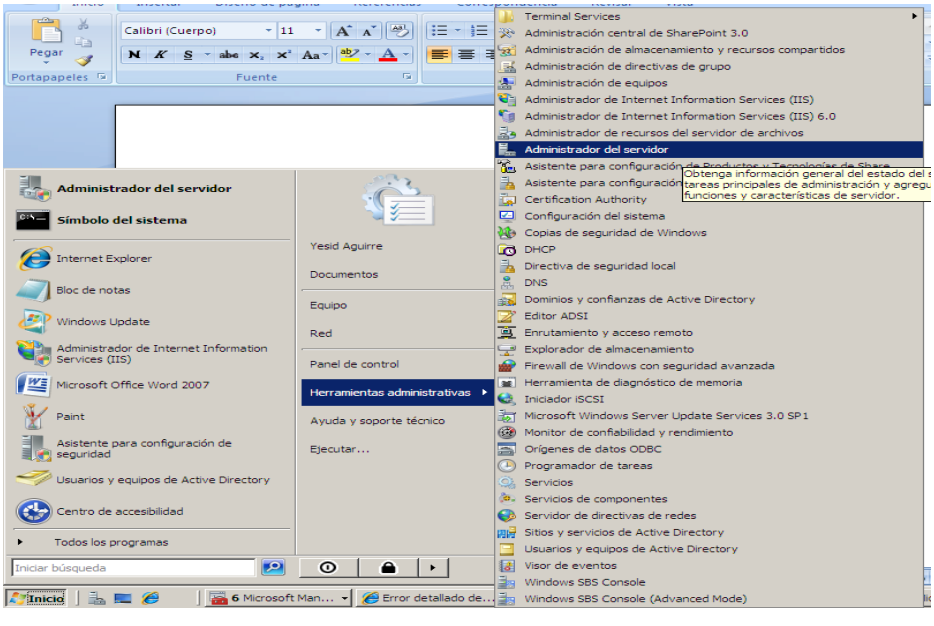


Figura No. 29: Administrador para activar certificados

Funciones -> Servicios de Certificate Server de Active Directory e instalar Servicio de publicación de World Wide Web e Inscripción web de de entidad de certificación.

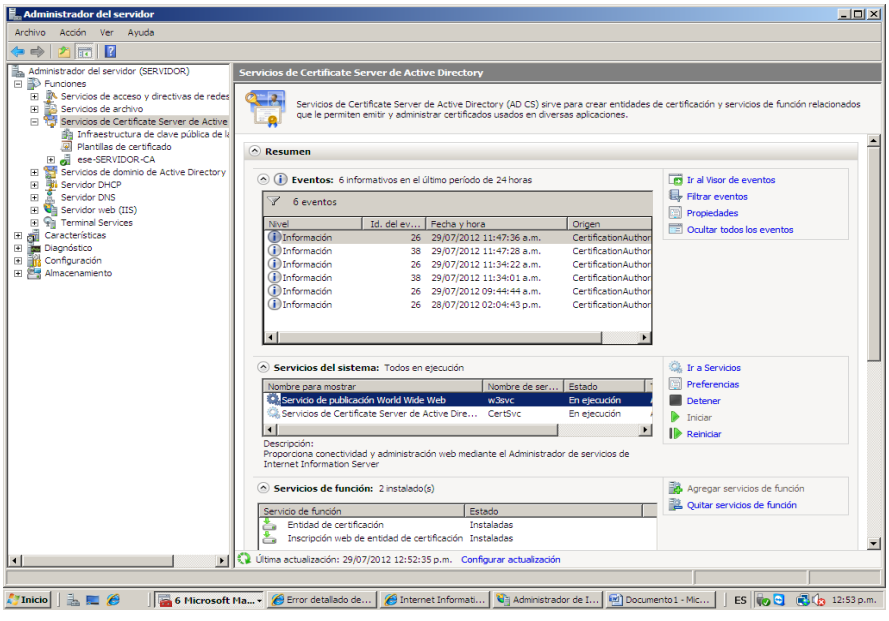


Figura No. 30: Servicio de publicación en ejecución

Activar HTTPS en el sitio web de certificados

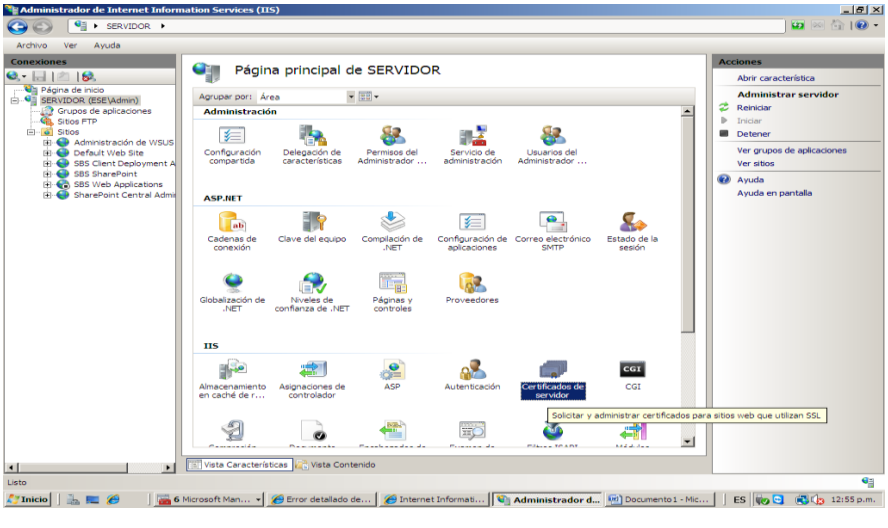


Figura No. 31: Inicio para la generación de certificados

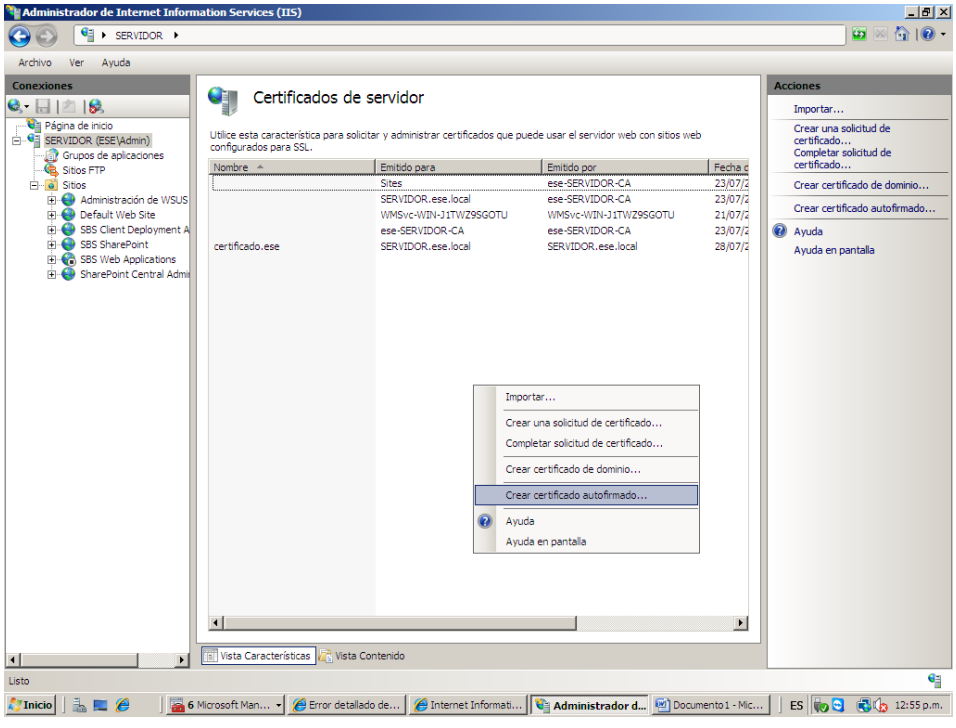


Figura No. 32: Creación de certificado nuevo

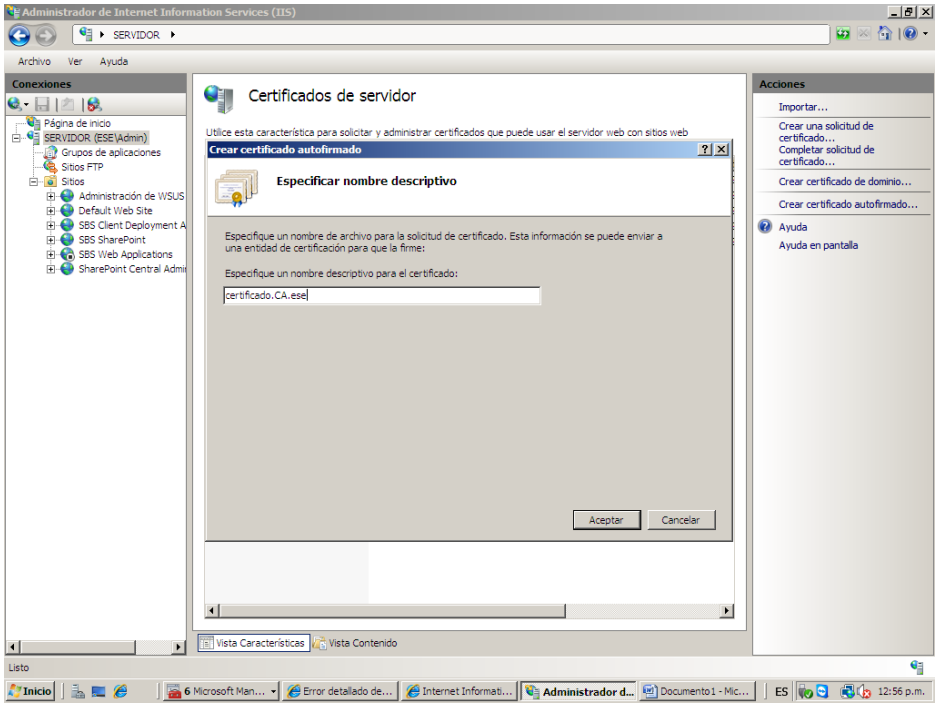


Figura No. 33: Nombre que se le da al certificado a crear

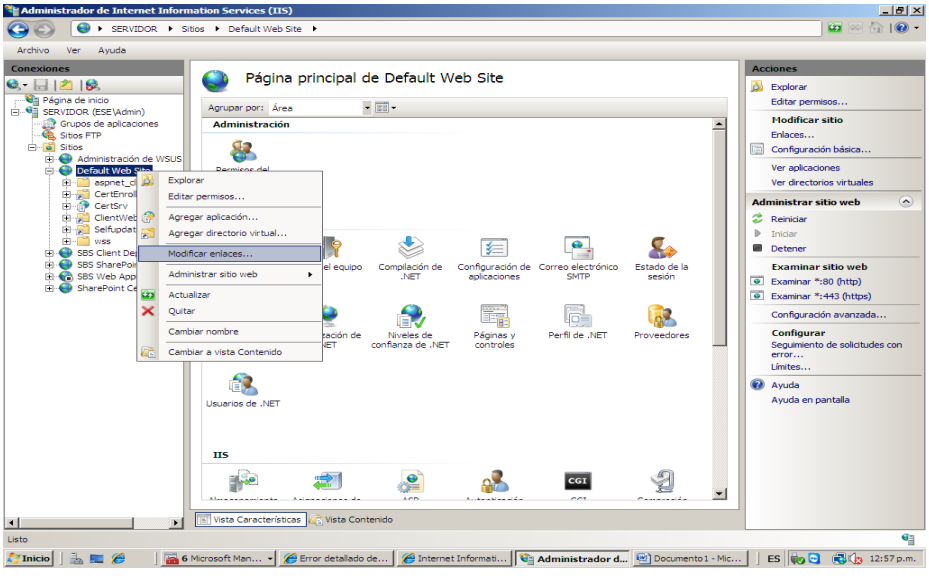


Figura No. 34: Modificación de enlaces

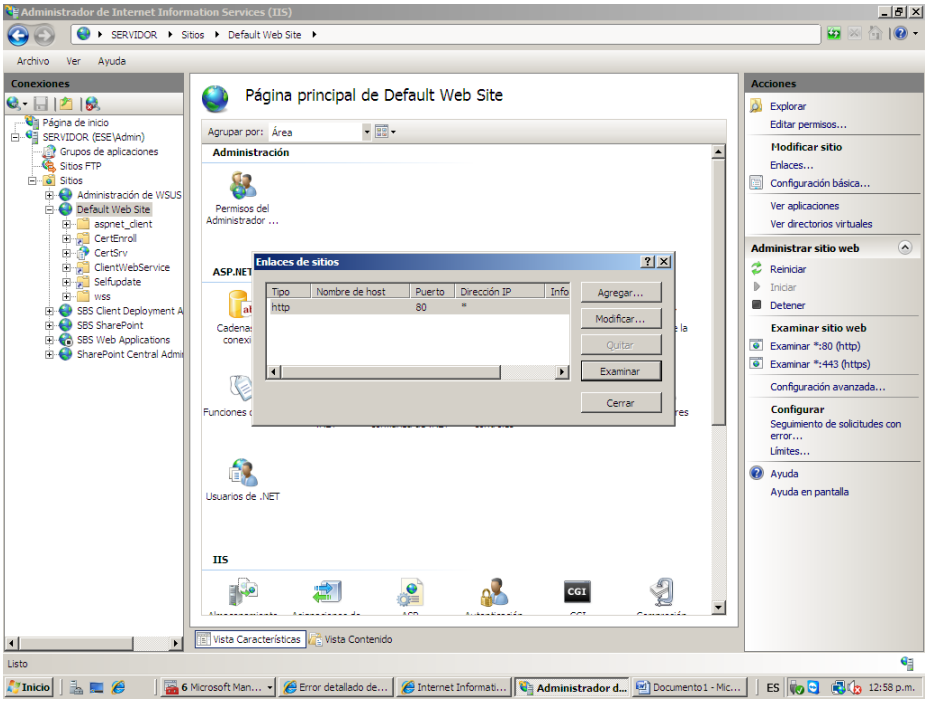


Figura No. 35: Creando los enlaces para el sitio

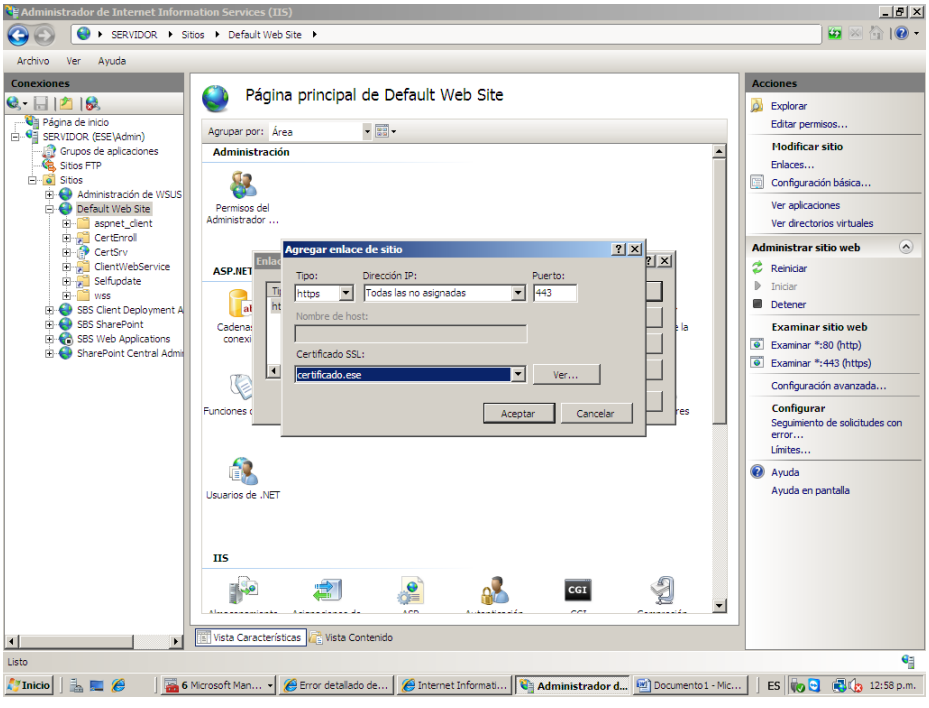


Figura No. 36: Enlazando el puerto con el nombre del certificado

Reiniciar sitio web

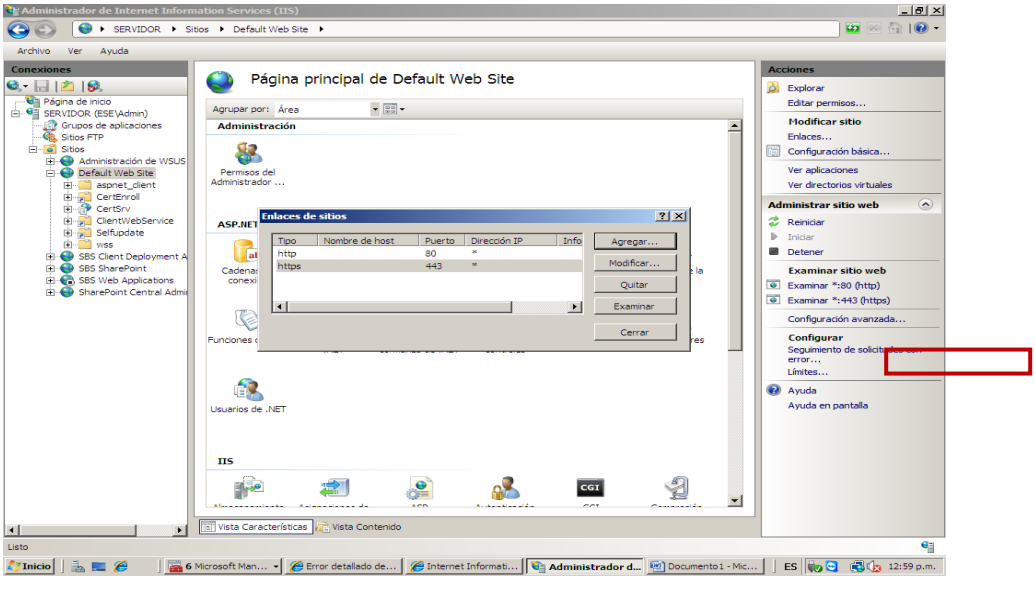


Figura No. 37: Certificado enlazado

Generar certificado para usuario a través de la web

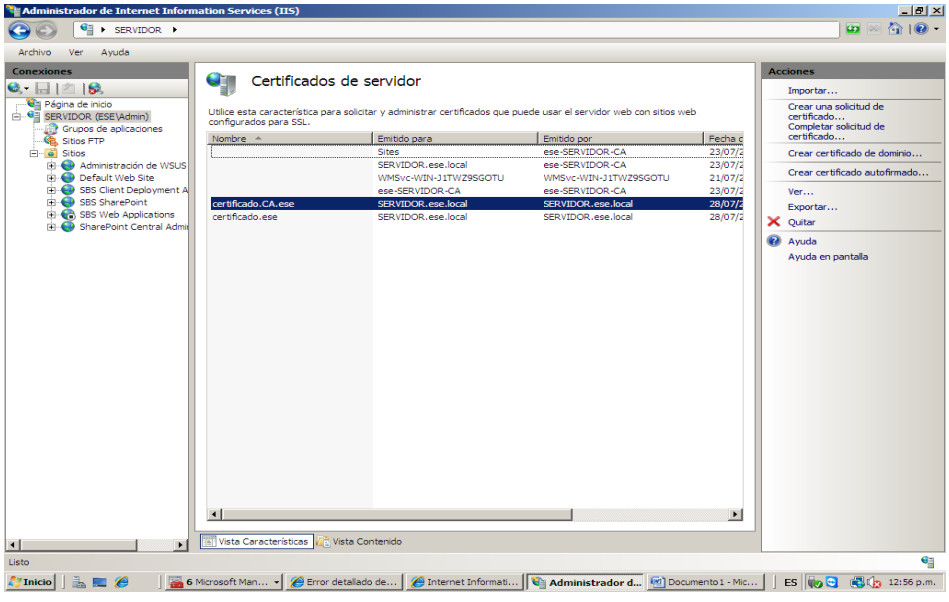


Figura No. 38: Certificado propio del servidor

Generar certificado para usuario a través del módulo web del CA.

Iniciar sesión desde un equipo conectado al dominio, abrir el navegador e ir a la IP del servidor utilizando https y apuntando al sitio web del CA. (https://190.69.88.50/certsrv/)

Figura No. 39: Módulo web del CA

Seleccionar Solicitar certificado y a continuación seleccionamos certificado de usuario.

Luego permitir operación

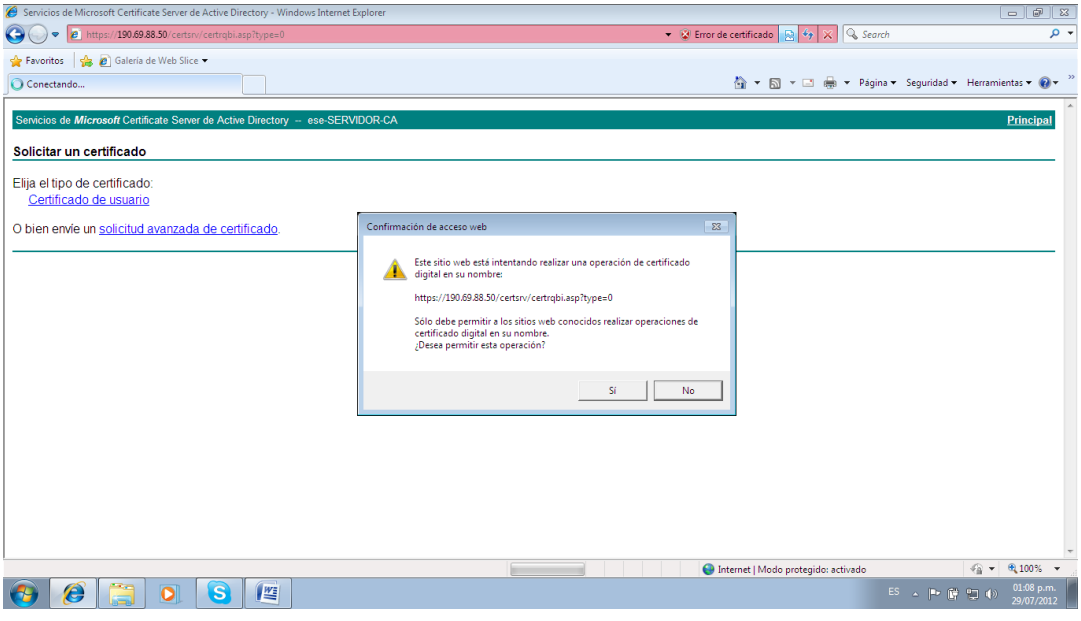


Figura No. 40: Creación de certificado digital

Clic en Enviar, permitir operación, la entidad CA genera el certificado y aparece la opción de instalar el certificado.

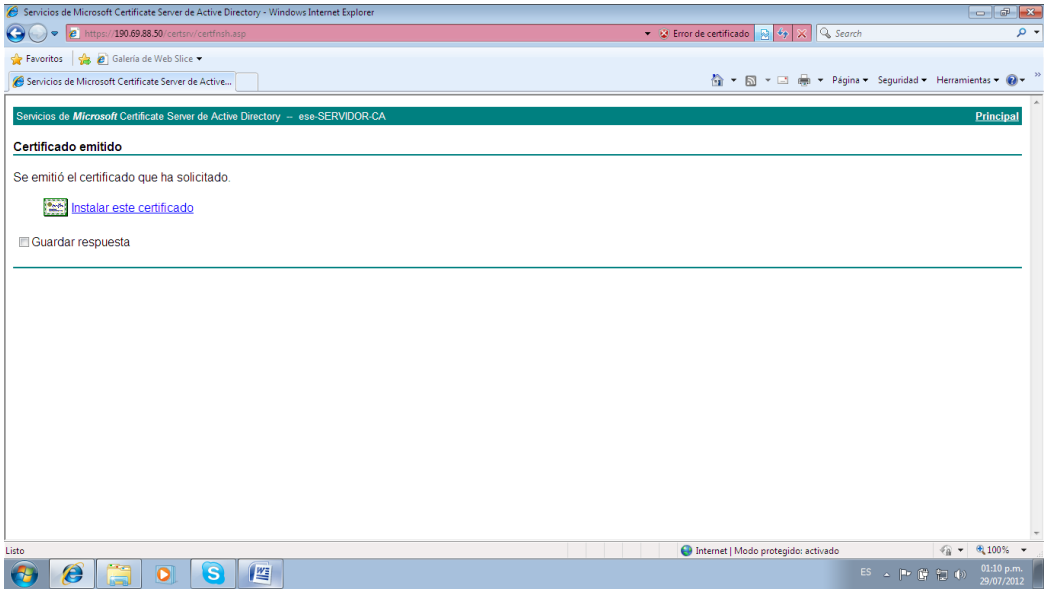


Figura No. 41: Certificado generado para el equipo terminal

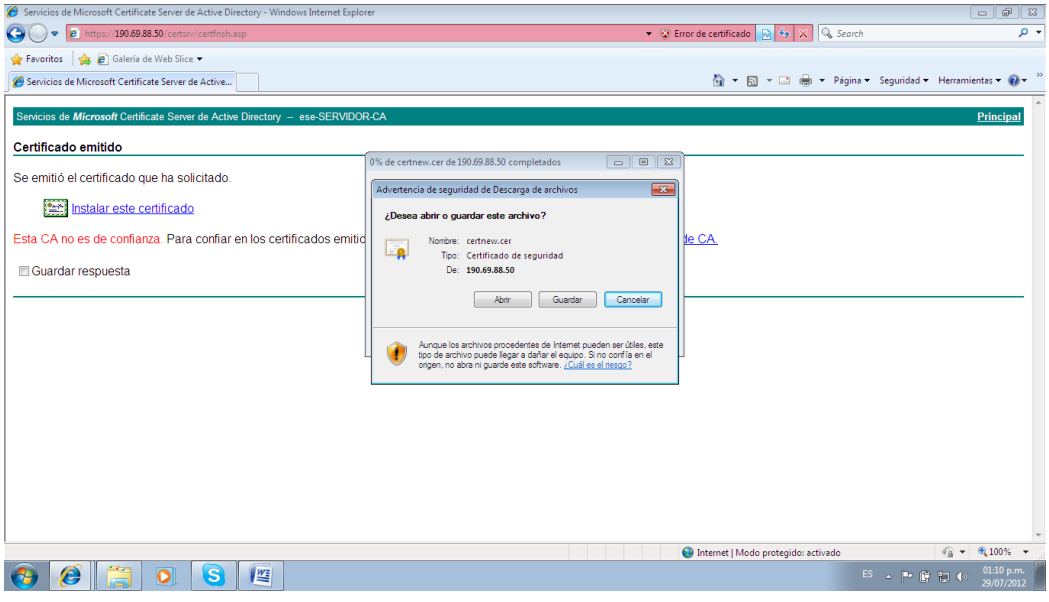


Figura No. 42: Guardado y ejecución del certificado

Guardar el certificado

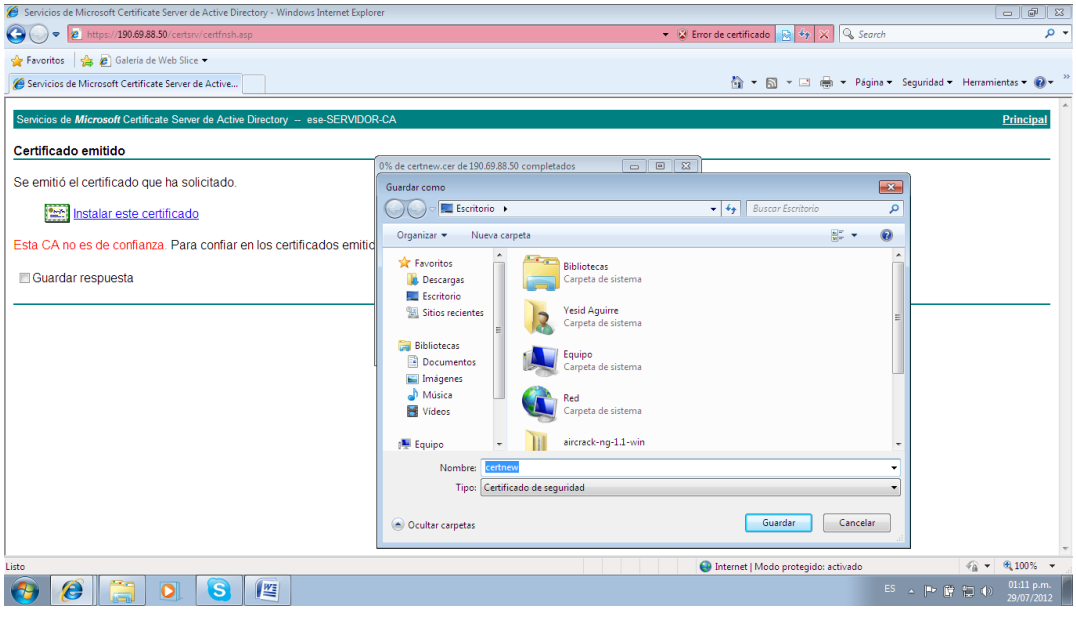


Figura No. 43: Ubicación donde quedará el certificado

Abrir el certificado e instalarlo

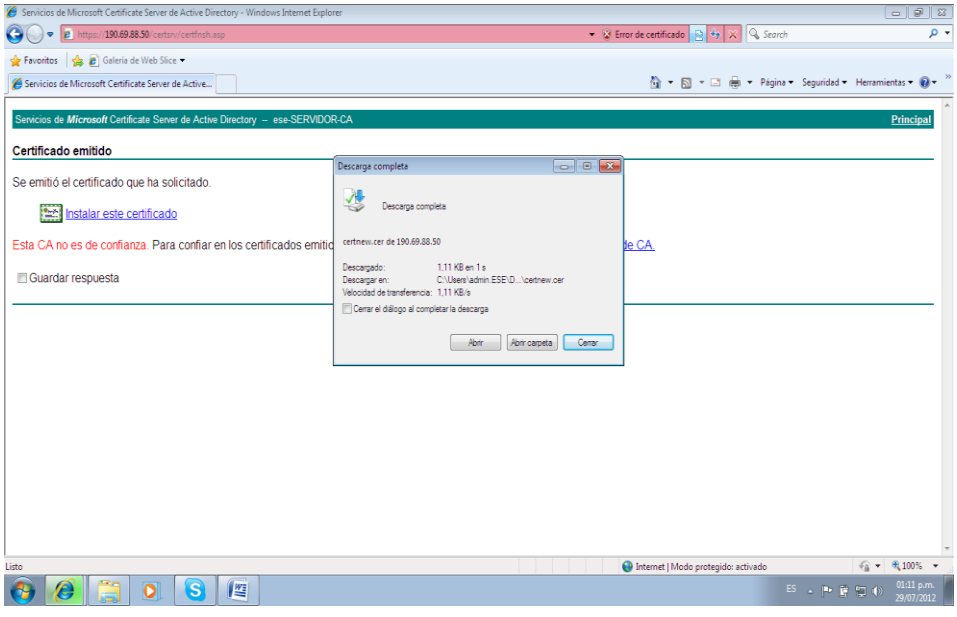


Figura No. 44: Instalación en el equipo terminal

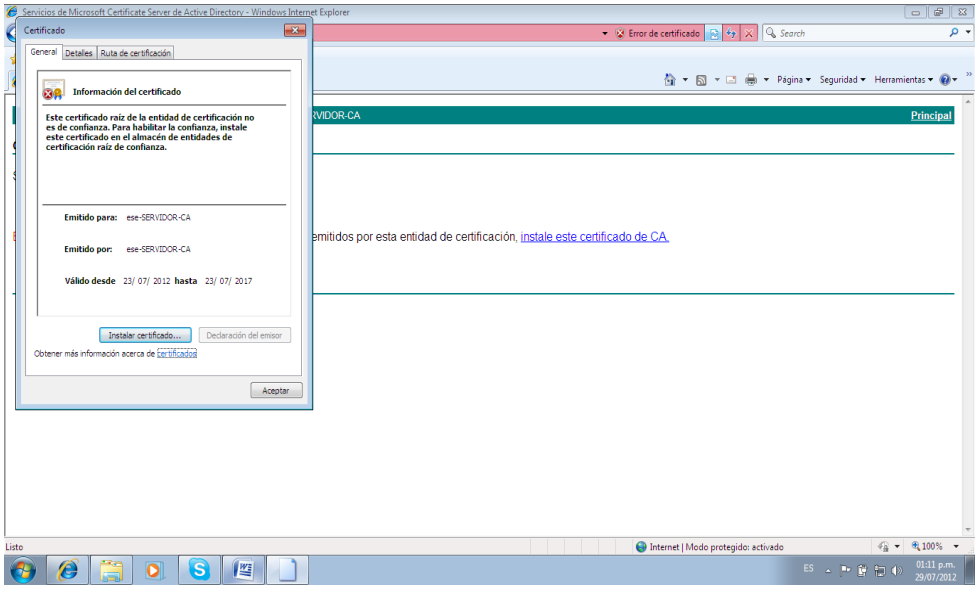


Figura No. 45: Instalación

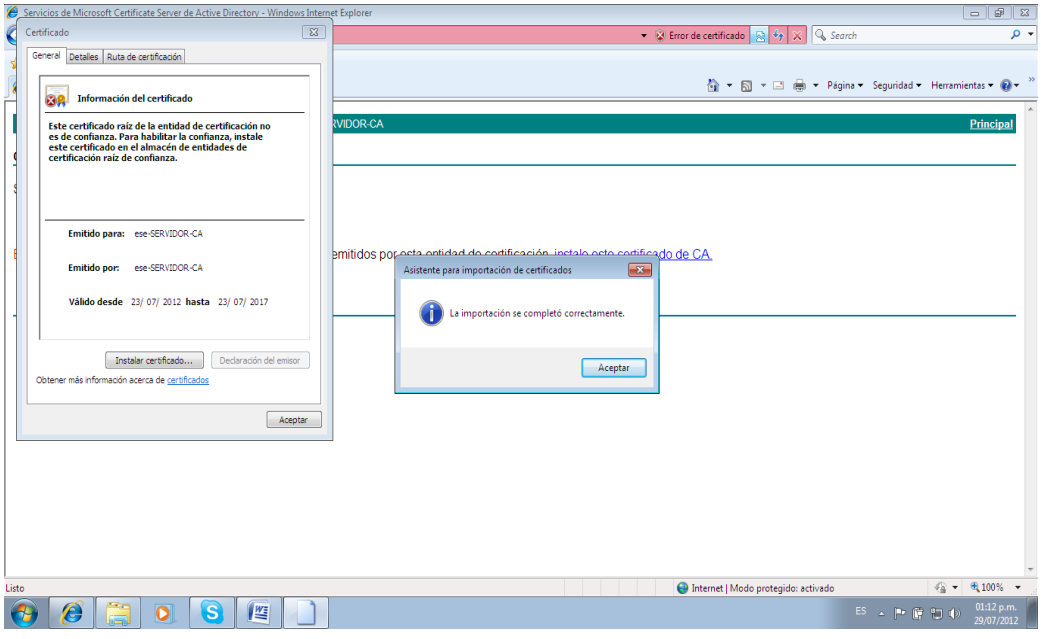


Figura No. 46: Certificado ejecutado

Así se concluye con la configuración de todas las funciones, para que sea posible la conexión segura entre dispositivos inalámbricos por medio de generación de certificados.

7.2 Aplicación del Proyecto de Desarrollo Empresarial

7.2.1 Descripción del sistema actual

Antes que todo, cabe mencionar que la organización “Alliance” es la entidad encargada de certificar a los fabricantes para que cumplan con las especificaciones para su uso comercial, basados en los estándares IEEEE (Instituto de Ingenieros eléctricos y electrónicos).

Según *IEEE* (Instituto de Ingenieros Eléctricos y Electrónicos) recuperado el (15 de abril de 2013) de su página web http://www.ieee.org/index.html CSMA/CA es el protocolo original para el control de paquetes más utilizado, evitando así la colisión

en las redes inalámbricas, ya que estas no cuentan con la facilidad de transmitir y recibir simultáneamente.

Estos son los principales estándares utilizados en las empresas de Puerto Berrio 802.11 que se mencionan a continuación:

802.11a

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, según Arias Aragues “opera en la banda de 5 Ghz y utiliza 52 subportadoras ortogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s”, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 Ghz tiene gran uso, según Arias Aragüés “al utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso”; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

La transmisión para exteriores con un valor máximo a 30 metros 54 Mbps, valor mínimo a 300 metros 6 Mbps, interiores valor máximo a 12 metros 54 Mbps y valor mínimo a 90 metros 6 Mbps.

OFDM es la técnica de modulación FDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio. OFDM divide la señal de radio en muchas sub-señales que son transmitidas simultáneamente hacia el receptor en diferentes frecuencias. OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal).

802.11b

El estándar 802.11b según Arias Aragüés “tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original”. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

Los productos de la 802.11b aparecieron en el mercado muy rápido debido a que la 802.11b es una extensión directa de la técnica de modulación DSSS definida en el estándar original. Por lo tanto los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b. El dramático incremento en el uso del 802.11b junto con sustanciales reducciones de precios causó una rápida aceptación del 802.11b como la tecnología Wireless LAN definitiva.

802.11b es usualmente usada en configuraciones punto y multipunto como en el caso de los AP que se comunican con una antena omnidireccional con uno o más clientes que se encuentran ubicados en un área de cobertura alrededor del AP. El rango típico en interiores es de 32 metros a 11 Mbit/s y 90 metros a 1 Mbit/s. Con antenas de alta ganancia externas el protocolo puede ser utilizado en arreglos fijos punto a punto típicamente rangos superiores a 8 Km incluso en algunos casos de 80 a 120 km siempre que haya línea de visión. Esto se hace usualmente para reemplazar el costoso equipo de líneas o el uso de quipos de comunicaciones de microondas.

La tarjetas de 802.11b pueden operar a 11 Mbit/s pero pueden reducirse hasta 5.5, 2 o 1 Mbit/s en el caso de que la calidad de la señal se convierta en un problema. Dado que las tasas bajas de transferencia de información usan algoritmos menos complejos y más redundantes para proteger los datos, a la vez son menos susceptible a la corrupción debido a la atenuación o interferencia de la señal. Sean han hecho extensiones del protocolo 802.11b para incrementar su velocidad a 22, 33, 44 Mbit/s pero estas no han sido ratificadas por la IEEE. Muchas compañías llaman a estas versiones mejoradas 802.11b+. Estas extensiones han sido ampliamente obviadas por los desarrolladores del 802.11g que tiene tasas de transferencia a 54 Mbit/s y es compatible con 802.11b.

El protocolo DSSS es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan en el estándar 802.11b[4].

802.11g.

Según Arias Aragüés “el estandar802.11g utiliza la banda de 2.4 Ghz, operando a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11ª”. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

El mayor rango de los dispositivos 802.11g es ligeramente mayor que en los del 802.11b pero el rango que el cliente puede alcanzar 54 Mbit/s es mucho más corto que en el caso del 802.11b.

[4] Protocolo DSSS. Disponible en línea desde la URL: http://ieeestandards.galeon.com/aficiones1573579.html, Recuperado el día 16/04/2013

Los dispositivos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de ser aprobado por el IEEE. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Muchos de los productos de banda dual 802.11a/b se convirtieron de banda dual a modo triple soportando a (a, b y g) en un solo adaptador móvil o AP. A pesar de su mayor aceptación 802.11g sufre de la misma interferencia de 802.11b en el rango ya saturado de 2.4 GHz por dispositivos como hornos microondas, dispositivos bluetooth y teléfonos inalámbricos. Recuperado el día 16/04/2013 en http://ieeestandards.galeon.com/aficiones1573579.html

802.11n. Según El IEEE (Institute of Electrical and ElectronicsEngineers), recuperado el (20 de abril de 2013) de su página web http://www.ieee.org/index.html aprobó finalmente el estándar Wi-Fi de alto rendimiento 802.11n. Este nuevo estándar para redes inalámbricas, donde se ofrece velocidades de más de 300 Mbps.

Los inicios de la versión del proyecto 802.11n fue presentado por primera vez hace siete años, y han tenido que ser presentadas hasta una docena de versiones, para que finalmente sea aprobado el proyecto.
Según Bruce Kraemer, quien estuvo mucho tiempo como presidente del Grupo de Tareas del 802.11n, publico en su blog la aprobación final del estándar.

Esta nueva modificación de la norma 802.11, ha sido diseñada para resolver una necesidad actual de la industria de la comunicación frente a la creciente demanda que hay en los hogares, empresas y WLANs públicas, con el aumento de las transferencias de pesados archivos que llegan con esta próxima generación de aplicaciones multimedia.

El estándar 802.11n, permitirá unas redes WLAN con un mejor rendimiento, un mejor despliegue de redes WLAN escalables, y una perfecta coexistencia con los sistemas e implementaciones de seguridad.

7.2.2 Diagnostico de la situación actual

Actualmente las redes inalámbricas y los sistemas informáticos, se vuelven cada vez más vulnerables a un ataque externo, que ocasione retrasos en los procesos y hasta perdida de información. La vulnerabilidad en los sistemas está ligada al desconocimiento múltiples herramientas que ayuden a la protección de la información, por tanto es necesario utilizar nuevos métodos que ayuden a reforzar la seguridad implementada en las redes internas de las empresas.

Un alto porcentaje de las empresas, y hasta en los mismos hogares se tienen redes inalámbricas con un nivel de seguridad muy bajo que fácilmente permiten el ingreso, de usuarios no deseados que alteran la información a conveniencia de ellos generando así problemas para el hogar o la empresa.

7.2.3 Metodologías para el análisis

7.2.3.1 Análisis estructurado. Descripción para determinar quienes harán uso de la red inalámbrica, los posibles usuarios que tendrán acceso a la red.

Administración segura de las claves de cifrado.
Configuración adecuada que asegure el tráfico de la red.
Vulnerabilidad a posibles ataques a la denegación del servicio (DoS).

La figura siguiente muestra un diagrama conceptual de la solución (autenticación de 802.1X EAP-TLS).

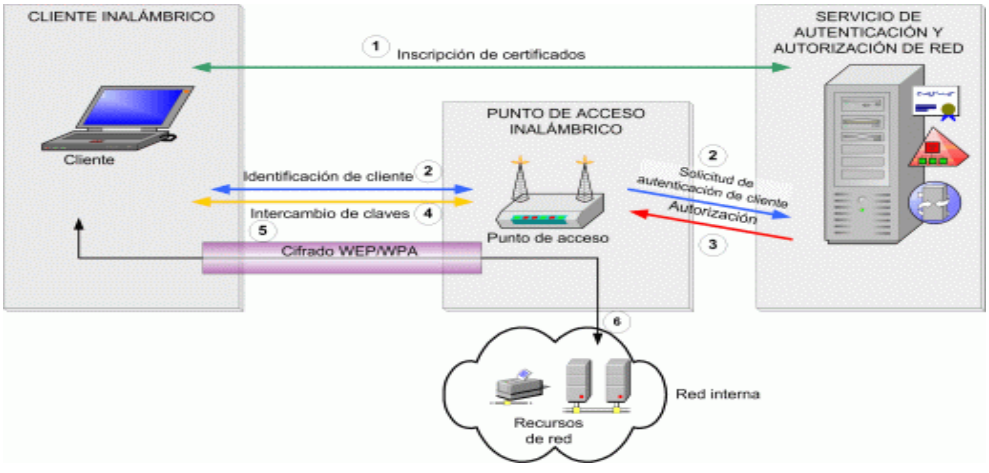


Figura No. 47: Autenticación de 802.1X EAP-TLS

7.2.3.2 Análisis orientado a objetos

El diseño de red lógico / físico simplificado de esta organización podría ser similar al definido en el diagrama siguiente:

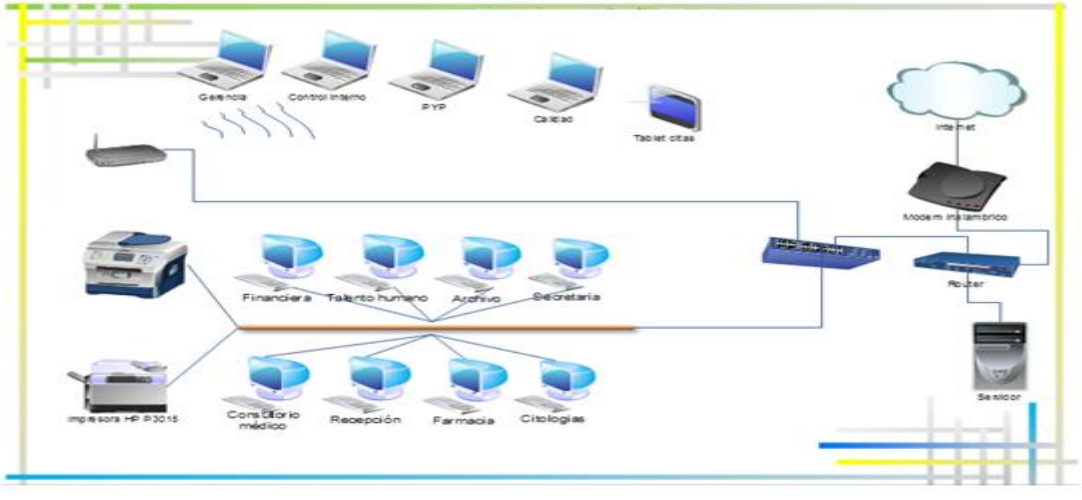


Figura No. 48: Diseño de red lógico / físico

7.3 El Consumidor

Los consumidores son el pilar fundamental de cualquier empresa; por esta razón nuestros consumidores potenciales serán todas aquellas empresas públicas y privadas, escuelas, colegios y personas naturales que requieran el servicio de implementación de sistemas de seguridad que garanticen el correcto funcionamiento de las redes de transmisión de datos, estas empresas están ubicadas en el municipio de Puerto Berrio y alguna de ellas son:

Empresas:
Sibelco, Soportuaria, Coregan, Gases de Antioquia, MotoAntioquia,

Escuelas y Colegios:
Colegio la inmaculada, Normal Superior, Antonio Nariño, Colegio la bombona, Colegio Alfonso Lopez

Persona natural:
Todos y cada uno de los habitantes del municipio de Puerto Berrio, teniendo en cuenta que este municipio cuenta con 43.000 habitantes aproximadamente.

Adicional exploraremos el escenario actual, donde la mayor parte de los actores se han puesto de acuerdo en optimizar el tráfico de sus redes con los servicios de datos, los fabricantes de equipos industriales, en los cuales ya está encabezando líneas de producto, cada vez con mayor peso específico, las ingenierías, integradores y desarrolladores que ven en este sistema un estándar de comunicaciones potente y práctico, y, finalmente, los usuarios que siempre están a la espera de la evolución, estandarización y comercialización de un sistema competitivo en precio y prestaciones.

El Wi-Fi proviene del sector de las comunicaciones de datos, un subproducto de la industria informática. Los servicios provistos por los equipos son gratis para los

dueños de los equipos. Para los clientes, el equipo representa un bien de capital que se deprecia.

En general, el servicio que se proveerá a la comunidad cerrada de usuarios: empresas, estudiantes, etc., tendrá el acceso wireless, comienzan a ofrecerse servicios de acceso prácticamente ubicuos.

En este contexto, cabe destacar que la tecnología Wi-Fi es la única que permite, configurar el grado de seguridad en función del criterio de los usuarios. Los terminales de acceso son uno de los eslabones más importantes a la hora de establecer medidas de seguridad al trabajar con tecnologías inalámbricas.

La seguridad abarca muchos más aspectos que la mera tecnología, siendo necesario aplicar otras medidas asociadas a las tecnologías y/o buenas prácticas generales asociadas a la auditoría y uso responsable de las mismas.

7.4 Delimitación y descripción del mercado

7.4.1 Localización

El Municipio de Puerto Berrio, se encuentra localizado sobre la margen del Magdalena Medio al Oriente del Departamento de Antioquia, con una extensión de 1.184 Km^2, altura de 125 m.s.n.m., su altura sobre el nivel del mar es de 178 metros, con una temperatura 29° C (promedio), latitud Norte 6º29’35’’ y Longitud Este 74º24’26’’.

7.4.2 Límites del municipio:

Norte: Remedios y Yondó
Nor – Occidente: Yolombó
Occidente: Maceo y Caracolí

Sur: Puerto Nare

Oriente: Río Magdalena, Departamento de Santander y Boyacá.

7.5 Comportamiento de la demanda del producto

El servicio está dirigido a empresas agrícolas, ganaderas, industriales y financieras del Municipio de Puerto Berrio, Antioquia. Estas son:

✓ **Sibelco.** Sibelco Colombia, es una empresa procesadora de carbonato de calcio con participación a nivel nacional e internacional, con sede principal en puerto Berrio, planta segundaria en Cali, oficina corporativa en Bogotá y oficina virtual en Medellín; la empresa cuenta con 163 empleados.

✓ **Soportuaria.** Sociedad Administradora portuaria, es la encargada de administrar el muelle multimodal del municipio de Puerto Berrio, facilita el desplazamiento de carga pesada entre terrestre y marítimo con conexión directa con el puerto de barranquilla.

✓ **Gramalote.** Gramalote Colombia Límite, es una empresa del sector minero que tiene el proyecto más ambicioso de explotación de oro a cielo abierto, esta empresa cuenta con su departamento operativo y administrativo con contacto directo con la sede gerencial en la ciudad de Bogotá.

✓ **MotoAntioquia.** Empresa comercializadora de motocicletas de marcha Yamaha de toda clase de cilindraje, tiene conexión con los diferentes sedes en municipios de Antioquia.

✓ **Coregan.** Comité Regional de Ganaderos de Puerto Berrio, es la encargada de agrupar el gremio de ganadero, buscando fortalecerlo e impulsarlo con los diferentes enlaces de ganaderos del país.

7.6 Comportamiento de la oferta del producto

En el municipio de Puerto Berrio existen personas que tienen conocimientos técnicos para implementar sistemas de seguridad, pero no están constituidos como empresa legal y no pueden prestar el servicio a empresas que requieran factura.

Adicional podemos resaltar que en otras regiones de Colombia existen empresas que prestan el servicio las cuales son: Telypc Soluciones integrales de telecomunicaciones y Mooib en Bogotá. Tenemos presente que las diferentes empresas que venden computadores tienen el conocimiento pero no profundizan en la implementación de sistemas de seguridad de redes inalámbricas.

7.7 Estudio de Demanda

Puerto Berrio, es un municipio que está en constante desarrollo y crecimiento; aumentando la dinámica operativa y flujo de procesos que busca cada vez mas innovar en los métodos productivos.

Podemos resaltar que según el DANE el número de habitantes para el 2010 era de 42.178, para el 2011 43.617 y para 2012 44.431; reflejando un crecimiento significativo de habitantes en Puerto Berrío. Así como los habitantes crecen, las empresas que se constituyen van en crecimiento y es este nuestro pilar fundamental para basarnos en que puerto Berrío hay empresas que se catalogan como clientes potenciales en el presente y a futuro.

Actualmente las empresas existentes acuden a ciudades cercanas para contactar personal capacitado que pueda asesorar en la configuración de seguridad de redes en especial redes inalámbricas, y es esta nuestra ventaja de suplir la necesidad que tienen las empresas en la implementación de seguridad en sus redes inalámbricas.

7.8 Población y muestra

La encuesta está dirigida a todas las empresas potenciales ubicadas en Puerto Berrio interesadas en la seguridad informática y aquellas que quieran implementar desde su inicio este sistema, para mantener protegida la información.

7.8.1 Instrumentos

Se utilizarán en la realización del proyecto los siguientes instrumentos.

7.8.1.1. Encuesta: Aplicación de una encuesta dirigida a las empresas del sector con el fin de indagar las ventajas y beneficios del uso de un sistemas de redes al fin de controlar a nivel de seguridad informática los archivos de datos e información que cada una de las empresas, la encuesta consta de 8 preguntas y se aplicara al personal de la seguridad informática (anexo No. 1 Encuesta seguridad informática).

7.8.1.2 ANALISIS Y RESULTADOS

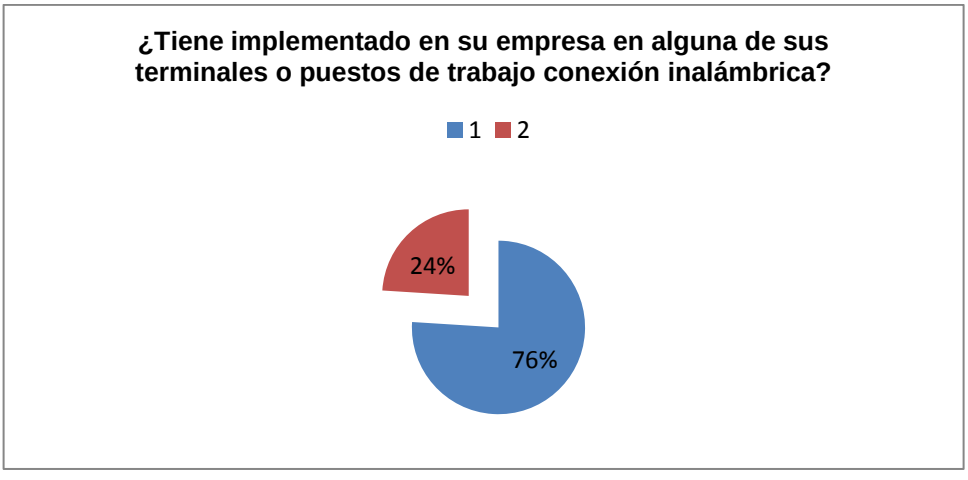
Para efecto de determinar la necesidad de nuestro servicio en esta población se aplicó la siguiente encuesta que arrojó los resultados descritos a continuación:

No.	ITEMS	FRECUENCIA (Fr.)		PORCENTAJES (%)		TOTAL (%)
		SI	NO	SI	NO	
1	¿Tiene implementado en su empresa en alguna de sus terminales o puestos de trabajo conexión inalámbrica? SI ( ) NO ( ) Si su respuesta es no, no responda las preguntas de la cuarta en adelante.	38	12	76	24	100%
2	¿Estaría dispuesto a implementar un tipo de configuración que mantenga salvaguardada la					

	información de su empresa? Total acuerdo Desacuerdo No sabe Acuerdo	27 11 10 2	54 22 20 4			100%
3	¿Conoce usted los tipos de ataques fraudulentos y los daños posibles que se pueden ocasionar al no tener protegida su red inalámbrica? SI ( ) NO ( )	45	5	90	10	100%
4	¿Qué protocolo de seguridad utiliza en su red inalámbrica actualmente? WPA ( ) WAP2 ( ) COMPARTIDO ( ) ABIERTA ( ) CCKM ( ) 802.1X ( )	22 3 3 2 10 5 3 2	- - - -	44 6 6 4 20 10 6 4	0 0 0 0	100%
5	¿Existe algún tipo de monitoreo referente al acceso a la red local y de la utilización de recursos que se hacen internamente en su empresa? SI ( ) NO ( )		50	-	100%	100%
6	¿Tiene confianza en la seguridad inalámbrica implementada en su empresa? SI ( ) NO ( )	23	27	46	54	100%
7	¿Está interesado en recibir asesoría sobre la seguridad en redes inalámbricas? SI ( ) NO ( )	50	-	-	100	100%
8	¿Dado los beneficios que trae implementar y configurar la red inalámbrica de forma adecuada, ¿cambiaría el sistema estándar por un sistema de configuración avanzada? SI ( ) NO ( )	40	10	80	20	100%
	TOTAL					100%

RESULTADOS:

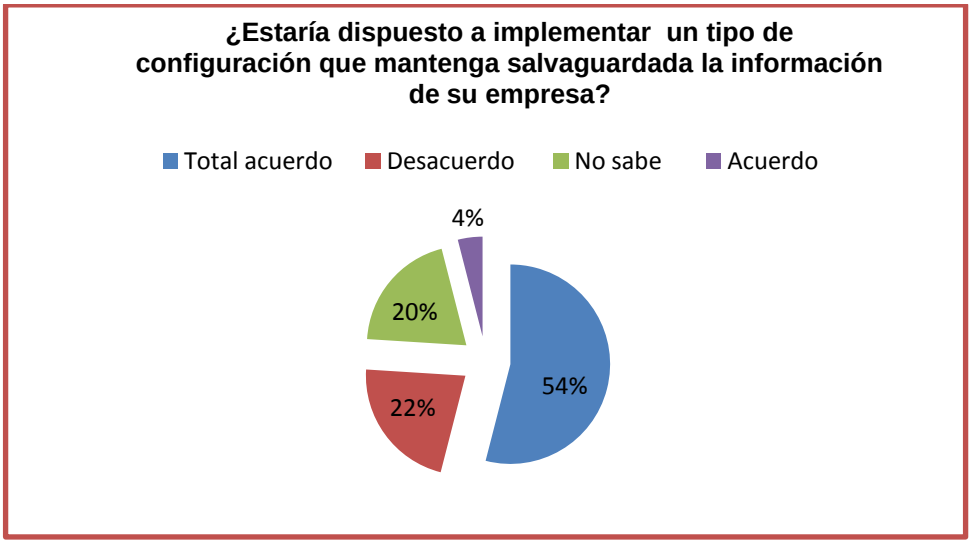
ITEM 1: ¿Tiene implementado en su empresa en alguna de sus terminales o puestos de trabajo conexión inalámbrica?



Fuente. Sanabria, *et. al*, 2013

En la figura anterior se puede observar que el 76% tienen implementado conexión inalámbrica, seguido de un 24% que dice que no tienen implementada esta tecnología ya que no saben usar los recursos informáticos, entre ellos Internet.

ITEM 2: ¿Estaría dispuesto a implementar un tipo de configuración que mantenga salvaguardada la información de su empresa?

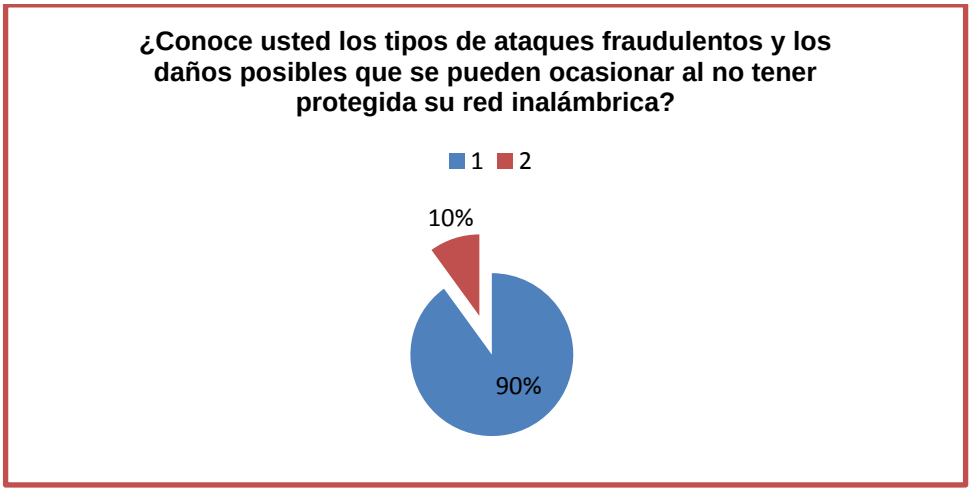


Fuente. Sanabria, *et. al*, 2013

La información es un recurso necesario para la organización y para la continuidad de las operaciones, ya que provee de una imagen de su ambiente actual, su pasado y su futuro.

El 24% dijo estar de acuerdo con contar con un sistema de seguridad informática, el 22% dijo no estar de acuerdo, el 20% no sabe o no conoce nada de sistemas informáticos, solo el 4% desea contar con un buen sistema de seguridad para salvaguardar la información.

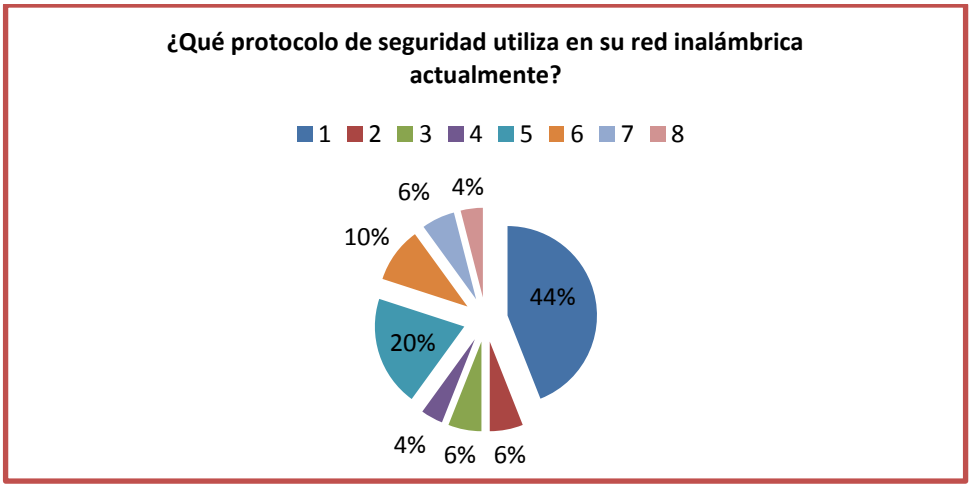
ITEM 3: ¿Conoce usted los tipos de ataques fraudulentos y los daños posibles que se pueden ocasionar al no tener protegida su red inalámbrica?



Fuente. Sanabria, *et. al*, 2013

El 90% dijo conocer los tipos de ataques fraudulentos a los que se exponen los sistemas informáticos, solo un 10% dijo no conocer y no tener protegida su red inalámbrica.

ITEM 4: ¿Qué protocolo de seguridad utiliza en su red inalámbrica actualmente?

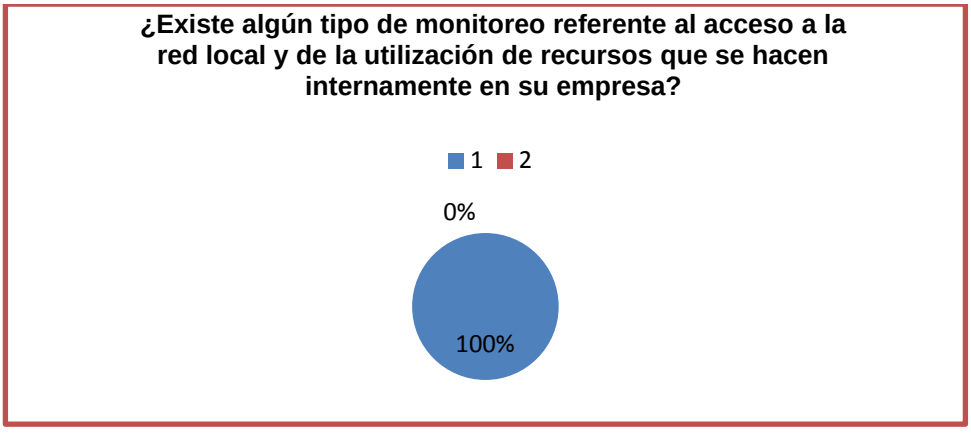


Fuente. Sanabria, *et. al*, 2013

El 22% utiliza en su red inalámbrica WPA, el 6% utiliza el WPA2, el 4% utiliza el sistema compartido; abierto solo el 20%, CCKM solo el 6% y el 802.1X solo el

4%. Se observa que el protocolo 802.1X es casi desconocido en la región de Puerto Berrio.

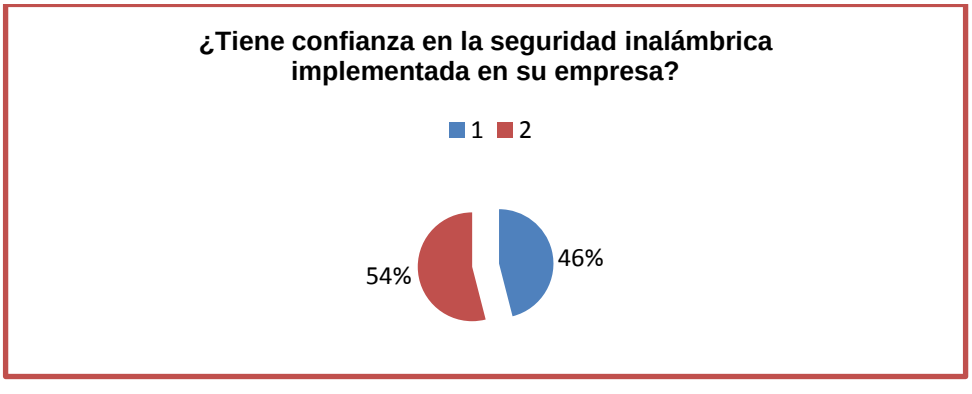
ITEM 5: ¿Existe algún tipo de monitoreo referente al acceso a la red local y de la utilización de recursos que se hacen internamente en su empresa?



Fuente. Sanabria, *et. al*, 2013

Según se observa en la gráfica, el 100% desconocen el tipo de monitoreo referente al acceso de la red local, consideran que es vital la seguridad informática, ya que se evitarían los problemas informáticos en las empresas en cuanto al amparo de la información de estas.

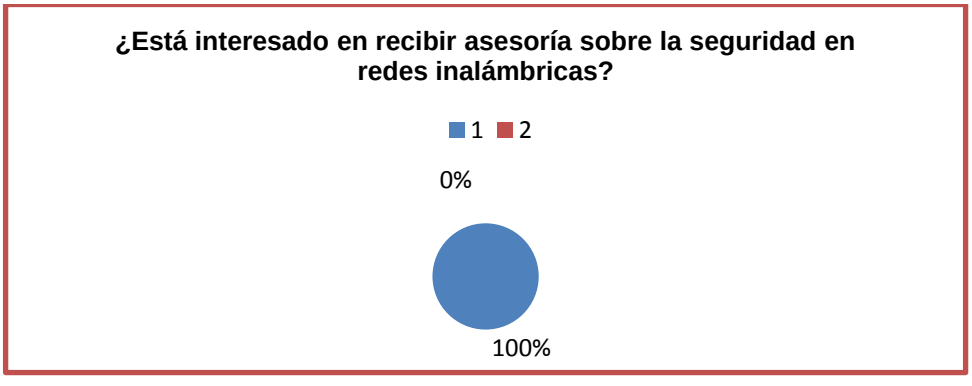
ITEM 6: ¿Tiene confianza en la seguridad inalámbrica implementada en su empresa?



Fuente. Sanabria, *et. al*, 2013

El 46% de los encuestados consideran que la red de seguridad que emplean es confiable, solo el 54% no creen contar con seguridad inalámbrica en su empresa, porque han tenido problemas de jaqueo.

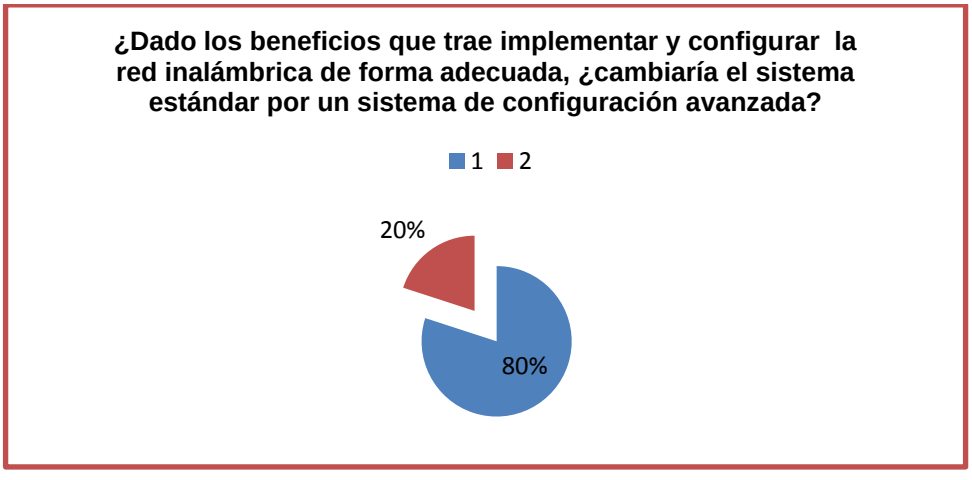
ITEM 7: ¿Está interesado en recibir asesoría sobre la seguridad en redes inalámbricas?



Fuente. Sanabria, *et. al*, 2013

El 100% de los encuestados dijo estar interesado en recibir asesorías, para contar con una buena información sobre redes inalámbricas, solo asi evitarían actos fraudulentos en su red.

ITEM 8: ¿Dado los beneficios que trae implementar y configurar la red inalámbrica de forma adecuada, ¿cambiaría el sistema estándar por un sistema de configuración avanzada?



Fuente. Sanabria, *et. al*, 2013

Según lo muestra la gráfica, el 80% de los encuestados consideran cambiar el sistema estándar por un sistema de configuración avanzada, solo 20% dijo no la cambiaria.

Con esta encuesta podemos ver reflejado la necesidad que se tiene de brindar soporte en implementación de métodos de seguridad en redes especialmente redes inalámbricas; sabiendo que del total de personas encuestadas y sumando quienes respondieron a la segunda pregunta "¿Estaría dispuesto a implementar un tipo de configuración que mantenga salvaguardada la información de su empresa?" con las que no sabe, de acuerdo y totalmente de acuerdo suma un 96% que podrían ser clientes potenciales.

7.9 Diseño metodológico

El diseño metodológico corresponde a un proyecto de desarrollo empresarial en empresas de la Ciudad de Puerto Berrio, utilizando una metodología técnica que permite determinar factores precisos de costos y gastos y de proyección de ingresos para la verificación de su viabilidad como unidad de negocio. Dentro de la línea de investigación en redes de la ECBTI.

7.10 Variables

Como variable independiente se considera la “seguridad en las redes inalámbricas implementadas en las empresas de Puerto Berrio” por cuanto esto será una implementación segura, cual es el resultado que se pretende lograr y sobre el cual se manipulan una serie de procedimientos. Del mismo modo como variables dependiente se analiza:

Calidad de la señal de actual vs la calidad de la señal de la configuración propuesta. Calidad de la seguridad en la configuración actual vs la calidad de la seguridad en la configuración propuesta.

VIII. ESTUDIO TECNICO Y ADMINISTRATIVO

En este aparte se describen los requerimientos técnicos para realizar el proceso de configuración de la red inalámbrica y mantener estable la señal. Para ello se tiene en cuenta los requerimientos de hardware y software necesarios para transmitir señal desde un punto de acceso y del sistema en relación para que exista confiabilidad entre los dispositivos y usuarios.

Software necesario:

- ✓ Windows server 2008
- ✓ Sistemas operativos (Windows xp, Windows Vistas, Windows 7 y Windows Mobile)
- ✓ Software administrativo de cada AP.

8.1 Localización

La empresa piensa atender a empresarios del Municipio de Puerto Berrio y posteriormente a algunos sectores del Oriente Antioqueño.

8.2 Obras físicas y distribución en planta

Estará ubicada en el municipio de Puerto Berrio, en un lugar amplio (Unos 20 mts. Cuadrados aproximadamente) en el cual no se tendrán muchos requerimientos en cuanto a infraestructura y equipos necesarios para la prestación del servicio.

8.3 Microlocalización

Estaremos ubicados en el municipio de Puerto Berrio, Antioquia; en la calle 49 no. 9-54, barrio san francisco. Un punto estratégico con una ubicación central de fácil

acceso y con alto volumen de transeúntes que ayudan da dar reconocimiento de nuestra ubicación.

IX. ESTUDIO ECONOMICO Y FINANCIERO

Permite mostrar los recursos económicos y financieros necesarios para desarrollar o llevar a cabo las actividades o procesos y/o para obtener los recursos básicos que se deben considerar como son el costo del tiempo, el costo de la realización y el costo de adquirir nuevos recursos.

En esta fase se compara la relación de costos de lo existente al propuesto para su implementación. Este aplica en esta propuesta, ya que las empresas no cuenta con los requerimientos técnicos necesarios para establecer los mecanismos de Seguridad en la red inalámbrica como se explica en el apartado de Factibilidad Técnica.

Lo que si es necesario es la cantidad de tiempo disponible para realizar las nuevas configuraciones, y esta se debe establecer según acuerdos con el personal de Seguridad de Información y sus proyectos internos, que solo son manejados por las empresas y no se pueden exponer en este documento.

9.1 Determinación de inversiones y costos a partir de las variables técnicas.

9.1.1 Presupuesto de inversiones

- ✓ **Inversiones fijas**

Para la puesta en marcha del proyecto se requiere una inversión inicial fija activos tangibles.

Producto	Valor
1 Equipo servidor DELL PowerEdge T110 II	$ 2. 378.000
1 Equipo Portatil	$ 1.000.000
1 Access Point D-link Dwl-8500ap Wireless	$ 943.000

Switching	
Router	$ 500.000
Switch	$ 350.000
Total Equipos	**$ 5.171.000**

- ✓ **Inversión activos intangibles**

Matricula Mercantil	$ 26.000
Sociedad	$ 127.000
Total	$ 153.000

9.1.2 Capital de trabajo

Para la puesta en marcha del proyecto es necesaria $ 10.000.000, los cuales serán necesarios para que el negocio inicie la operación y se sostenga en el mercado por 3 meses donde podremos comprar equipos, pagar empleado, servicios públicos, impuestos, arriendo, publicidad

9.2 Gastos de operación

Internet	180.000
Energía	150.000
Empleados	$ 4.000.000
Total	**$ 4.330.000**

Mes 1	1	$ 4.330.000
Mes 2	1	$ 4.330.000
Mes 3	1	$ 4.330.000

9.2.1 Gastos de ventas

Los gastos de operación que influyen en nuestra operación son los siguientes:

Papelería y tarjetas de presentación	60.000
Transporte	40.000

9.2.2 Ingresos

Según lo proyectado se tiene previsto que de 50 empresas en la región de Puerto Berrio, 5 tomarán el servicio según lo contratado.

Ingresos por montaje completo del servicio Radius

Instalación Sistema Radius	5	$ 20.000.000
Instalación Seguridad Sencilla	150	$ 12.000.000
Soporte de Seguridad	150	$ 1.000.000
Total		**$ 33.000.000**

9.3 Punto de equilibrio

Actividades	A	B	
Participación	40%	60%	
Precio de Venta	4,000,000.00	800,000.00	
Costos Variables	2,340,000	508,500	
Margen de contribución	1,660,000.00	291,500.00	
Costos Fijos	14994916		
MCPP	996,000.00	116,600.00	1,112,600.00

x		13.48		
A		5.39		
B		8.09		

Descripción	**A**	**B**		
Ventas	21,563,783.57	6,469,135.07		
Costos Variales	2,574,753			
Margen Contribución	18,989,030.87	6,469,135.07		
Total Ventas			28,032,918.64	
Total Costo Variables			2,574,753	
Total Margen de contribución			25,458,165.94	
Costos Fijos			25,459,031	
Utilidad			865	

Con la anterior tabla podemos resaltar que la inversión inicial, más los gastos de operación del primer mes, nuestro punto de equilibrio se resalta en el mes 2, cubriendo el saldo negativo del mes 1. Y cumpliendo con una venta de 13 servicios de los cuales 5 son de configuración de sistema RADIUS y 8 configuraciones sencillas que no requieren servidor.

9.4 ESTADO DE RESULTADOS

ESTADO DE RESULTADOS
1 ENERO AL 31 DE DICIEMBRE DE 2012

		49,700,00
Ventas		0
Costo de producción		0
		49,700,00
Utilidad bruta en ventas		0
Gastos de administración	22,279,031	
Gastos de ventas	3,180,000	
TOTAL GASTOS		25,459,03
OPERACIONALES		1
		24,240,96
Utilidad operacional		9
Gastos financieros		0
		24,240,96
Utilidad antes de impuestos		9
Provisión para impuestos		0
		24,240,96
UTILIDAD NETA		9

T.I.O	i+f+if		Inflación	4%		
T.I.O	i+f+if=15%		Incremento	15%		
T.I.O	0.196					
V.P.N	17,392,249	70,660,894	73,291,460	75,922,026	78,552,592	
	(1+0,196)1	(1+0,196)2	(1+0,196)3	(1+0,196)4	(1+0,196)5	
	17,392,249	70,660,894	73,291,460	75,922,026	78,552,592	
	1.196	1.430416	1.710777536	2.046089933	2.44712356	
						Sumatoria
	14,542,014	49,398,842	42,841,023	37,105,909	32,099,970	175,987,758

$$\frac{5478333=}{(1+0,196)1} \quad 5,478,333 \quad \text{Suma egresos}$$

V.P.N	(i=0,196)=	175,987,758	5,478,333	170,509,425
V.P.N	(i=0,196)=	170,509,425		

TIR

AÑOS	1	2	3	4	5
F=	17,392,249	70,660,894	73,291,460	75,922,026	78,552,592
I=	46%	1.46			
N=	# de años				
POTENCIA=	1.46	2.1316	3.112136	4.54371856	6.633829098
-28033783.7	11,912,499	33,149,228	23,550,211	16,709,227	11,841,214

TIR **65%**

X. ANALISIS AMBIENTAL

El impacto ambiental que se espera generar en el presente proyecto sobre el área de influencia es nulo, porque el diseño propuesto se ajusta a las condiciones y necesidades ambientales sugeridas en este documento y tomando medidas adecuadas durante la fase de ejecución, implementando un plan de prevención y mitigación.

No se presentan riesgos en el proyecto por agentes externos, ni por efectos de implementación del proyecto.

- ✓ **Recurso del Aire.** La contaminación del aire o atmosfera no existe.

- ✓ **Recurso paisaje.** Para la construcción del proyecto no se modificará el paisaje.

XI. ANALISIS SOCIAL

El imparto social que se espera generar con el presente proyecto en el municipio de Puerto Berrío, es general empleo directo e indirecto, que ayuden a mejorar la calidad de vida de las personas.

Adicional brindaremos seguridad a las personas de que su información personal estará blindad aliviando la presión de ser atacadas por intrusos que sabotean los equipos y la información queda expuesta.

XII. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

✓ Entre las publicaciones tecnológicas, todas las grandes consultoras coinciden en señalar el desarrollo de las tecnologías Wi-Fi como una de las que presentan mayor potencial de crecimiento. Las ventas de aparatos con conexión inalámbrica se incrementarán gracias a factores como la extensión de los estándares, el aumento de la interoperabilidad, la creciente demanda de aparatos portátiles o la aparición de nuevas aplicaciones.

✓ Por el lado de la oferta, la intensa competencia en un mercado en el que todavía no existen claros dominadores conduce a un progresivo abaratamiento de los precios. Por su parte, la instalación de una red inalámbrica en el hogar o en las empresas de la ciudad de Puerto Berrio, podría ser más barata.

✓ Por otro lado, y haciendo referencia a las comunicaciones inalámbricas, se advierte que Wi-Fi se erigirá como una de las tecnologías más fuerte, alternativa que generará un alto volumen de negocio durante el presente año. Según esto, se señala que serán las redes WLAN privadas o semiprivadas, tales como las de empresas o universidades, las que registren un mayor aumento, el cual vendrá favorecido por la calidad de servicio y la seguridad.

✓ Con la elaboración de este proyecto se logra evidenciar que es viable, rentable y sostenible ponerlo en marcha; resaltando con las encuestas que hay personas que requieren del servicio y están dispuestos a invertir por ello.

✓ Podemos destacar los impactos positivos que tiene este proyecto, adicional a la rentabilidad que genera, la sostenibilidad y trayectoria que puede tener en el mercado visionando expandir sus servicios a otras regiones.

RECOMENDACIONES

✓ Los departamentos encargados de velar por el cumplimiento de políticas de seguridad (Gerencia General, Unidad Central de Riesgos de los Sistemas de Información, Auditoría de Sistemas, Área de Tecnología) deben considerar las siguientes recomendaciones a fin de garantizar el eficaz funcionamiento de las políticas, normativas, procedimientos y monitoreo de las configuraciones de accesos a la información implementados en la red inalámbrica.

✓ Establecer revisiones constantes a los mecanismos de seguridad implementados, a fin de determinar rango de acción, eficacia y operatividad del plan adoptado. Una medida idónea es realizar pruebas de penetración (*Penetration Testing*) a la red de la institución, determinando los niveles de seguridad actuales.

✓ Contemplar la unificación de plataformas operativas en la institución e instalar las actualizaciones de estas plataformas operativas (*Windows*), principalmente a las herramientas de seguridad (*ISA Server 2000*) y a los servidores de la empresa (*Windows 2000 Server*).

✓ Tomar en consideración el diseño de red propuesto, el cual contempla modificaciones relevantes a la configuración de la red, eliminando ciertas debilidades en cuanto al desaprovechamiento de características o cualidades que poseen algunos enlaces y conexiones en la infraestructura de red actual.

XIII. BIBLIOGRAFIA

Kendall, K. y Kendall, J. (1997). *Análisis y Diseño de Sistemas*. México: Prentice Hall.

Sheldon, T. (1997). "*Planes de Seguridad y Administración", en Seguridad en Windows NT*. Osborne: McGraw Hill.

Stephen, R. y De Cenzo, D. (1996). *Fundamentos de Administración*. México: Prentice Hall.

Tamayo, B. y Tamayo, M. (2002). *Proceso de Investigación Científica.* México: Limusa.

Universidad Pedagógica Experimental Libertador. (1998). *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas: FEDUPEL.

Zacker, C. (2002). *Redes Manual de Referencia*. España: McGraw Hill

Lee, Thomas; Davies, Joseph, (aut.). Microsoft Windows Server 2008 Protocolos y servicios. McGraw-Hill

Thomsom, Carlos. (2005). Redes 1: Transporte de información y telecomunicación. Universidad Manuela Beltrán

Biblioteca TechNet. Configuración de clientes Radius. http://technet.microsoft.com/es-es/library/cc786863(v=ws.10)

Arias, Araguez: Internet y Redes Inalámbricas. Clanar Internacional.

Villa, Daniel. López, Jorge. Lamadrid, Alain. Olivera, Jesús. (2007). Internet: Servicios Avanzados. Recuperado el 16 Agosto de 2012 en http://site.ebrary.com/

ANEXO A: ENCUESTA

Estimado Empresario y/o Usuario:

Solicito su valiosa colaboración al revisar el cuestionario que le suministro a continuación. En consecuencia le agradezco emita un juicio relacionado con la investigación titulada: “IMPLEMENTACIÓN DE SEGURIDAD EN REDES 802.11X (WIFI) EN EMPRESAS DE PUERTO BERRIO”, presentada como requisito para optar al título *de Tecnólogo en Ingeniería de Sistemas de la Unad.*

Ítems:

1. ¿Tiene implementado en su empresa en alguna de sus terminales o puestos de trabajo conexión inalámbrica?

   SI ( ) NO ( )

   Si su respuesta es no, no responda las preguntas de la cuarta en adelante.

2. ¿Estaría dispuesto a implementar un tipo de configuración que mantenga salvaguardada la información de su empresa?

   TOTAL ACUERDO ( )
   DESACUERDO ( )
   NO SABE ( )
   ACUERDO ( )

3. ¿Conoce usted los tipos de ataques fraudulentos y los daños posibles que se pueden ocasionar al no tener protegida su red inalámbrica?

   SI ( ) NO ( )

4. ¿Qué protocolo de seguridad utiliza en su red inalámbrica actualmente?
   WPA ( )
   WAP2 ( )
   COMPARTIDO ( )
   ABIERTA ( )
   CCKM ( )
   802.1X ( )

5. ¿Existe algún tipo de monitoreo referente al acceso a la red local y de la utilización de recursos que se hacen internamente en su empresa?

   SI ( ) NO ( )

6. ¿Tiene confianza en la seguridad inalámbrica implementada en su empresa?

   SI ( ) NO ( )

7. ¿Está interesado en recibir asesoría sobre la seguridad en redes inalámbricas?

   SI ( ) NO ( )

8. ¿Dado los beneficios que trae implementar y configurar la red inalámbrica de forma adecuada, ¿cambiaría el sistema estándar por un sistema de configuración avanzada?

   SI ( ) NO ( )

Gracias por su colaboración.

ANEXO B. CRONOGRAMA DE ACTIVIDADES

Fase del proyecto	Actividades	Desarrollo de actividades	Tiempo en semanas			
			Enero	Febrero –Abril	Mayo-Julio	Agosto-Noviembre
Fase1: Estudio	Estudio técnico	Investigar sobre configuración radius en Windows server 2008 y método de autentificación				
	Estudio operativo	Se determina los componentes necesarios para llevar a cabo el tipo de configuración				
	Estudio económico	Se debe plantear en términos económicos el costo para implementar el proyecto.				
Fase2: Diseño del proyecto	Diseño de la configuración	Se diseña la configuración entre los diferentes dispositivos y se crea conexión entre los mismos.				
Fase 3: Puesta en marcha	Muestra real mediante prototipo	Se implementa el proyecto inicialmente y hacen las pruebas pertinentes para evaluar su resultado.				