
# UNIVERSIDAD TECNICA DE BABAHOYO

**FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA**

**ESCUELA DE SISTEMAS**

# TESIS DE GRADO

**Previa a la Obtención del Título de:**

## INGENIERA DE SISTEMAS

## TEMA:

**"INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA "DR. RAFAEL HERNANDEZ TROYA""**

## AUTORA:

***MARIA FERNANDA HERNANDEZ MENDEZ.***

***GABRIELA SIOMAR PARRALES HIGUERA.***

## DIRECTOR:

**ING. ANGEL ESPAÑA**

**BABAHOYO – LOS RIOS- ECUADOR**

**2011**

# UNIVERSIDAD TECNICA DE BABAHOYO

**FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA**
**ESCUELA DE SISTEMAS**

**Tesis previa a la obtención del título de:**

# INGENIERA DE SISTEMAS

## "INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA "DR. RAFAEL HERNANDEZ TROYA""

**Proponente:**

***MARIA FERNANDA HERNANDEZ MENDEZ.***

***GABRIELA SIOMAR PARRALES HIGUERA.***

# UNIVERSIDAD TECNICA DE BABAHOYO


**FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA**

## ESCUELA DE SISTEMAS

## MEMORIA DE TESIS

**“INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA “DR. RAFAEL HERNANDEZ TROYA””**

**Previa a la obtención del título de:**

## INGENIERA DE SISTEMAS

***MARIA FERNANDA HERNANDEZ MENDEZ.***

***GABRIELA SIOMAR PARRALES HIGUERA.***

***BABAHOYO***

***2011***

# UNIVERSIDAD TECNICA DE BABAHOYO

## ESCUELA DE SISTEMAS

# MEMORIA DE TESIS

**“INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA “DR. RAFAEL HERNANDEZ TROYA””**

**PRESENTADA AL TRIBUNAL EXAMINADOR COMO REQUISITO PARA OBTENER EL TITULO DE:**

## INGENIERA DE SISTEMAS

## TRIBUNAL EXAMINADOR

**PRESIDENTE DEL TRIBUNAL**

**…….....**

**DIRECTOR DEL TRIBUNAL**

**…….....**

**LECTOR DE TESIS**

**…….....**

**MIEMBRO DEL TRIBUNAL**

**…….....**

# UNIVERSIDAD TECNICA DE BABAHOYO

## ESCUELA DE SISTEMAS

# MEMORIA DE TESIS

## “INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA “DR. RAFAEL HERNANDEZ TROYA””

**AREA:** **SISTEMAS**

**AUTORA:** **MARIA FERNANDA HERNANDEZ MENDEZ**

***GABRIELA SIOMAR PARRALES HIGUERA.***

**DIRECTOR:** **ING. ANGEL ESPAÑA**

**LECTOR:** **ING. OMAR MONTECE MORENO**

# TITULO:

**“Instalación Y Seguridad de las Redes Inalámbricas en la Clínica “Dr. Rafael Hernández Troya””**

# DEDICATORIA

Dedico este trabajo de investigación para aquellos seres que han sido el apoyo fundamental en mi vida, que siempre inculcaron en mí la Constancia y Perseverancia para mi superación:

A mis Padres **Fanny** y **Fernando** por su apoyo incondicional durante el transcurso de mi vida estudiantil.

A mi esposo por su comprensión;

A mis adorados hijos Jeremy y Ashley por el sacrificio realizado al no estar con ellos el tiempo requerido.

A mis hermanos Fernando y Katty por la ayuda brindada cuando los necesite;

A mis queridas sobrinas Dani y Nanda, y a todas aquellas personas que me han apoyado en este largo camino para cumplir mis ideales sin escatimar esfuerzo y sacrificio, especialmente a **Dios** quien siempre ha sido mi guía principal.

Gracias a todos por la confianza que pusieron en mi!!!!!

**Mafer Hernández Méndez**

# DEDICATORIA

A mi Señor Jesús, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo.

A mis padres, Betty y Jorge quienes me enseñaron desde pequeña a luchar para alcanzar mis metas. Mi triunfo es de ustedes los amo.

A mis queridos hermanos Mariella y Joffre les agradezco, sin ustedes no hubiese podido hacer realidad este sueño.

A mi esposo Guillermo Javier quien me brindo su amor, cariño, estimulo, y su apoyo constante, comprensión y paciente espera para que pudiera terminar la tesis son evidencia de su gran amor ¡Gracias!.

A mi adorado hijo Ian Javier quien me prestó el tiempo que le pertenecía para terminar la tesis ¡Gracias Bebe Te Amo!

A mis amados sobrinos Jetita y Robert Williams que con su tierna alegría motivaron a terminar este trabajo

A mi segundo padre Ab. Ausberto Colina quien siempre motivo a seguir adelante y a quien prometí que terminaría mis estudios. ¡Promesa cumplida! .

A los que nunca dudaron que lograría este triunfo. A mi cuñada Mariuxi, a mi cuñado Roberto, a mis amigos Dani, Carlos, Romina, Esaut, Fercho, Diego, Geovanny, David, Mafer, Zoila.

**Gabriela Parrales Higuera**

# AGRADECIMIENTO

A Dios por ser el pilar principal en nuestras vidas, por la inteligencia y salud dada para poder llegar a cumplir esta meta.

A nuestros amados padres, hermanos y esposo por darnos siempre el apoyo requerido durante nuestra preparación académica.

A nuestros adorados hijos por el sacrificio hecho durante este largo recorrido, para alcanzar esta meta.

Al Dr. Rafael Hernández Troya, por el apoyo y confianza brindada para la realización de este proyecto

A todos nuestros profesores, en especial a los ingenieros Omar Montece y Angel España, por el empeño y dedicación que siempre pusieron durante mi formación en las aulas.

A nuestros amigos, en especial al Ab. Ausberto Colina, por el apoyo incondicional que siempre nos ha brindado durante estos ciclos de estudios.

# INTRODUCCIÓN

La irrupción de la nueva tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas de futuros para el desarrollo de sistemas de comunicación, así como nuevos riesgos.

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho, que la utilización de estas redes se hayan incrementado desde el año 2002 siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

Pero como todas las nuevas tecnologías en evolución, presenta riesgos debidos al optimismo inicial y en la adopción de la nueva tecnología sin observar los riesgos inherentes a la utilización de un medio de transmisión tan 'observable' como son las ondas de radio.

El presente trabajo pretende dar una visión global del estado actual de la seguridad en las redes inalámbricas, desde los riesgos existentes en las implementaciones de los estándares actuales, hasta las mejores propuestas para subsanar, para evitar la filtración de la información, hemos realizado un trabajo de investigación que coadyuva a solucionar los problemas de seguridad de las redes inalámbricas.

Por último, debemos manifestar que han aparecido nuevas vulnerabilidades de diversos protocolos. Por lo tanto, con el deseo de que esta memoria no quede obsoleta, por lo anteriormente expuesto, nuestros objetivos so, que este trabajo de investigación sirva, para colaborar con la labor social que realizan las instituciones benéficas, y particularmente con la Fundación Teolinda Troya Escobar, de esta ciudad que funciona en la Clínica “Dr. Rafael Hernández Troya”

# CAPITULO I

## 1.1. El Problema

### 1.1.1. Contexto Problemático

La Fundación Teolinda Troya, es una corporación, **sin fines de lucro**, con finalidad social, autónoma y funciona mediante acuerdo ministerial N. 01742, domiciliada en la ciudad de Babahoyo cuya acción se constituye para trabajar con sectores de nuestra comunidad con una proyección Cantonal y Provincial.

- **Visión**

Promover y ejecutar, servicios de calidad, con criterio de integralidad y universalidad para la satisfacción del ejercicio pleno de los derechos de los niños, niñas, adolescentes y sus familias enfatizando temas de Salud.

- **Misión**

Contribuir al mejoramiento de la salud de los niños, niñas, adolescentes y sus familias, haciendo efectivo el "Derecho a la Salud", y, potenciar el desarrollo comunitario con la participación de la sociedad y la familia.

- **Nuestros Valores**

- Vocación, compromiso y dedicación con el usuario.
- El paciente es el centro de referencia y actuación de nuestra Fundación.
- Profesionalismo en la atención.
- Asistencia humanizada.
- Seriedad, fiabilidad y credibilidad.
- Respeto mutuo, trabajo en equipo y sentido de pertenencia.

## 1.2. Situación Problemática

El envío y recepción de los datos en la Clínica Dr. Rafael Hernández Troya , se lo realizaba en forma manual, lo cual generaba congestionamiento en la tramitación

de dichos eventos, para poder solucionar esta situación creímos que era necesario la implementación de una red inalámbrica, la misma que nos permitió solucionar el problema de la transmisión de datos, ya que obtuvimos mayor agilidad al momento de enviar o recibir información de los pacientes tanto de consulta externa, como de los casos de intervenciones quirúrgicas, entre las diferentes áreas de la clínica.

## 1.3. **Problema de Investigación**

Con lo anteriormente expuesto, consideramos que es necesario apoyar y dar solución a este problema de la inexistencia de RED INALAMBRICA, a continuación enunciamos el problema:

**“Como debe ser una red inalámbrica que optimice los recursos de información en la Clínica Dr. Rafael Hernández Troya, donde funciona la Fundación Teolinda Troya Escobar?”**

### 1.3.1.Delimitación de la Investigación

- **Temporal:**

Para realizar el presente trabajo de investigación se requerirá un tiempo de seis meses a partir de la aprobación de este proyecto.

- **Espacial:**

La investigación se desarrollará en la Clínica Dr. Rafael Hernández Troya, ubicada en el edificio de Herederos Hernández Troya, localizado en las calles García Moreno 720, entre Eloy Alfaro y Sucre de esta ciudad.

## 1.4. Justificación

✓ Se justifico porque a través de la implementación de la red inalámbrica, pudimos demostrar los conocimientos adquiridos como estudiante de la Universidad Técnica de Babahoyo en la Facultad de Administración Finanzas e Informática.

✓ Se justifico porque en la clínica Dr. Rafael Hernández Troya no contaba con la implementación de ningún tipo de red.

✓ El presente trabajo de investigación se justifico realizarlo, por cuanto se dio mayor agilidad al envío y recepción de la información desde cada área de la Clínica Dr. Rafael Hernández Troya.

## 1.5. Objetivos

### 1.5.1. Objetivo General

Diseñar una Red Inalámbrica Segura en la Clínica Dr. Rafael Hernández Troya, como solución para recibir y enviar información de un terminal a las diferentes áreas de la clínica

### 1.5.2. Objetivos Específicos

✓ Mantener información actualizada respecto de los pacientes de las diferentes áreas de la Clínica Dr. Rafael Hernández Troya, para uso tanto de consulta externa como para los casos de intervenciones quirúrgicas.

✓ Almacenar información histórica de los pacientes para uso posterior y permitir el acceso solo a personal autorizado.

# CAPITULO II

## 2. MARCO TEORICO DE LA INVESTIGACION

### 2.1. Fundamentación Teórica

Para establecer la fundamentación teórica del presente trabajo de investigación, hemos considerado los criterios o planteamientos de diversos autores y profesionales respecto al tema, nos identificamos con sus criterios sobre el uso e instalaciones de las redes inalámbricas.

### 2.1.1. ¿Qué es una red inalámbrica?

Es una red que permite a sus usuarios conectarse a una red local o a Internet sin estar conectado físicamente, sus datos (paquetes de información) se transmiten por el aire. (1)

Al montar una red inalámbrica hay que contar con un PC que sea un “Punto de Acceso” y los demás son “dispositivos de control”, todo esta infraestructura puede variar dependiendo que tipo de red queremos montar en tamaño y en la distancias de alcance de la misma. Según gráfico # 1

**GRÁFICO # 1**

### 2.1.2. Riesgos de las Redes Inalámbricas

Aunque este trabajo vaya dirigido a los aspectos de seguridad de la red inalámbrica, no podemos pasar por alto los elementos que componen la red inalámbrica.

Existen 4 tipos de redes inalámbricas, la basada en tecnología Blue Tooth, la IrDa (Infrared Data Association), la HomeRF y la WECA (Wi – Fi). La primara de ellas no permite la transmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizada por los dispositivos de ondas infrarrojas, debe permitir la visión directa entre los dos elementos comunicantes. Las tecnologías HomeRF y Wi – Fi están basados en las especificaciones 802.11 (Ethernet Inlambricas) y son la que utilizan actualmente las tarjetas de red inalámbricas.

### 2.1.3. Mecanismos de Seguridad

### 2.1.3. WEP (Wired Equivalent Protocol)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

La vulnerabilidad de WEP reside en la superficie longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

### 2.1.3.2. OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las particiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

### 2.1.3.3. ACL (Access Control List)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

### 2.1.3.4. CNAC (Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

## 2.1.4. Diseño Recomendado

Podemos hacer varias recomendaciones para diseñar una red inalámbrica e impedir lo máximo posible el ataque de cualquier intruso.

Como primera medida, se debe separar la red de la organización en un dominio público y otro privado. Los usuarios que proceden del dominio público (los usuarios de la red inalámbrica) pueden estar tratados como cualquier usuario de Internet (externo a la organización). Así mismo, instalar cortafuegos y mecanismos de autentificación entre la red inalámbrica y la red clásica, situando los puntos de acceso delante de los cortafuegos y utilizando VPN a nivel de cortafuegos para la encriptación del tráfico en la red inalámbrica.

Los clientes de la red inalámbrica deben acceder a la red utilizando SSH, VPN o IPSec y mecanismos de autorización, autenticación y encriptación del tráfico (SSL). Lo ideal sería aplicar un nivel de seguridad distinto según que usuario accede a una determinada aplicación.

La utilización de VPNs nos impediría la movilidad de las estaciones cliente entre puntos de acceso, ya que estos últimos necesitarían intercambiar información sobre los usuarios conectados a ellos sin reiniciar la conexión o la aplicación en curso, cosa no soportada cuando utilizamos VPN.

Como contradicción, es recomendable no utilizar excesivas normas de seguridad por que podría reducir la rapidez y la utilidad de la red inalámbrica. La conectividad entre estaciones cliente y PA es FCFS, es decir, la primera estación cliente que accede es la primera en ser servida, además el ancho de banda es compartido, motivo por el cual tenemos que asegurar un número adecuado de puntos de acceso para atender a los usuarios.

También se podrían adoptar medidas extraordinarias para impedir la intrusión, como utilizar receivers (Signal Leakage Detection System) situados a lo largo del perímetro del edificio para detectar señales anómalas hacía el edificio además de utilizar estaciones de monitorización pasivas para detectar direcciones MAC no registradas o clonadas y el aumento de tramas de reautentificación.

Por último también podrían ser adoptadas medidas físicas en la construcción del edificio o en la utilización de ciertos materiales atenuantes en el perímetro exterior del edificio, debilitando lo máximo posible las señales emitidas hacia el exterior. Algunas de estas recomendaciones podrían ser, aún a riesgo de resultar extremadas:

- Utilizar cobertura metálica en las paredes exteriores.
- Vidrio aislante térmico (atenúa las señales de radiofrecuencia)
- Persianas venecianas de metal, en vez de plásticas.
- Poner dispositivos WLAN lejos de las paredes exteriores.
- Revestir los closets (rosetas) de la red con un revestimiento de aluminio.
- Utilizar pintura metálica.
- Limitar el poder de una señal cambiando la atenuación del transmisor.

### 2.1.5. Políticas de Seguridad

A parte de las medidas que se tomen en el diseño de la red inalámbrica, debemos aplicar ciertas normas y políticas de seguridad que nos ayudarían a mantener una red más segura:

- Utilizar WEP, aunque sea rompible con herramientas como AirSnort o WEPCrack, como un mínimo de seguridad.

- Utilizar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales.

- Inhabilitar DHCP para la red inalámbrica. Las IPs deben ser fijas.

- Actualizar el Firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones wireless.

- Proporcionar un entorno físicamente seguro a los puntos de acceso y desactivarlos cuando se pretenda un período de inactividad largo.

- Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos. El SSID es una identificación configurable que permite la comunicación de los clientes con un determinado punto de acceso. Actúa como password compartido entre la estación cliente y el punto de acceso.

- Inhabilitar la emisión broadcast del SSID.

- Reducir la propagación de las ondas de radio fuera del edificio.

- Utilizar IPSec, VPN, firewalls y monitorizar los accesos a los puntos de acceso.

### 2.1.6. Tipos de Inseguridades

Si una red inalámbrica está bien configurada nos podemos ahorrar muchos disgustos y estar más tranquilos.

- ✓ Las inseguridades de las redes inalámbricas radica en:

- Configuración del propio “servidor” (puntos de accesos).

- La “escucha” (pinchar la comunicación del envió de paquetes).

- “Portadoras” o pisarnos nuestro radio de onda (NO MUY COMÚN), mandan paquetes al aire, pero esta posibilidad es real.

- Nuestro sistema de encriptación (WEP, Wirelles Equivalent Privacy , el mas usado es de 128 Bits, pero depende el uso que le demos a nuestra red.

### 2.1.7. Consejos de Seguridad

Para que un intruso se pueda meter un nuestra red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar nuestra transmisión.

Por ello presentamos los siguientes consejos:

1. Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.

2. Control de acceso seguro con autentificación bidireccional.

3. Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.

4. Configuración WEP (muy importante), la seguridad del cifrado de paquetes que se transmiten es fundamental en las redes inalámbricas, la codificación puede ser

más o menos segura dependiendo del tamaño de la clave creada y su nivel, la más recomendable es de 128 Bits.

5. Crear varias claves WEP, para el punto de acceso y los clientes y que varíen cada día.

6. Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto más de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.

7. Radio de transmisión o extensión de cobertura, éste punto no es muy común en todo los modelos, resulta más caro, pero si se puede controlar el radio de transmisión al círculo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

## 2.1.8. CLASES DE REDES

A lo largo de la historia y como ha venido evolucionando la tecnología y que el mundo necesita estar en constante comunicación, se observa un gran avance en cuanto a las tecnología de redes, y sus diferentes tipos de configuraciones y los modos como se trasmite información y la constante comunicación de las personas mediante voz, audio y video,

### 2.1.8.1. Redes de Área Local (LAN)

Son privadas y se usan para conectar computadores personales y estaciones de trabajo de una oficina, fábricas, otro objetivo intercambian información.

Las LAN están restringidas en tamaño porque el tiempo de transmisión está limitado, opera a una velocidad de 10 a 100 mega bites por segundo

El material para una conexión puede ser cable coaxial un cable de dos hilos, fibra óptica o cable U T P, se pueden efectuar conexiones inalámbricas empleando transmisiones de infrarrojos.

Las redes emplean protocolos o reglas para intercambiar información, impidiendo una colisión de datos, se emplean protocolos como ethernet o token Ring

## 2.1.8.2. Redes de Área Amplia (WAN)

Es extensa geográficamente en un país o continente, utiliza maquinas Hosts conectadas por una subred de comunicaciones para conducir mensajes de una hosts a otra, en redes amplias la subred tiene dos componentes las líneas de transmisión y los elementos de conmutación que son computadoras especializadas que conectan dos o mas líneas de transmisión.

Las WAN contienen numerosos cables y hacen uso de enrutadores, en el caso de no compartir cables y desean comunicarse lo hacen por medio de otros enrutadores intermedios hasta que la línea de salida este libre y se reenvía y una subred basado en este principio se llama punto a punto.

Algunas posibles topologías diseñadas de interconexión de enrutador tienen topologías irregulares como son de anillo, árbol, completa, intersección de anillos, irregular, estrella.

### 2.1.8.3. Red de Área Metropolitana (MAN)

Para extenderse a lo largo de una ciudad se puede conectar un cierto número de LAN en una red mayor de manera que se puedan compartir recursos de una LAN a otra haciendo uso de una MAN se conectan todas las LAN de oficinas dispersas.

### 2.1.8.4. Redes punto a punto

Conexiones directas entre terminales y computadoras, tienen alta velocidad de transmisión, seguras, inconveniente costo, proporciona más flexibilidad que una red con servidor ya que permite que cualquier computadora comparta sus recursos.

### 2.1.8.5. Redes de difusión

Poseen un solo canal de comunicaciones compartido por todas las maquinas de la red, cuando el mensaje es enviado se recibe por todas las demás verifican el campo de dirección si es para ella se procesa de lo contrario se ignora. Pero este tipo de red permite mediante un código la posibilidad de dirigir un paquete a todos los destinos permitiendo que todas las maquinas lo reciban y procesen.

### 2.1.8.6. Redes conmutadas

Los datos provienen de dispositivos finales que desean comunicarse conmutando de nodo a nodo objetivo facilitar la comunicación.

## 2.1.9. PROTOCOLO Y ARQUITECTURAS DE RED

**PROTOCOLOS**: conjunto de reglas o convenios para llevar a cabo una tarea. Define qué se comunica, cómo se comunica y cuándo se comunica. Los elementos claves del protocolo son:

- Sintaxis, formato de los datos orden en el cual se presentan.
- Semántica, significado de cada sección de bits.
- Temporizador, define cuando se envía y con qué rapidez.

## 2.1.10. FUNCIONES DE LOS PROTOCOLOS

- **Se agrupan en las siguientes categorías**

**Segmentación y ensamblado:** envían mensajes en una secuencia continua, se dividen los datos en bloques de menor tamaño y se denominan (P D U) Protocol Data Unit, intercambiándose entre dos entidades a través de un protocolo.

**Encapsulado:** cada P D U consta no solo de datos sino también de información de control, cuando solo tienen de control se clasifican en Dirección, Código, Control.

**Control de conexión:** al transmitir datos cada PDU se trata independientemente de las PDU anteriores, se conoce como transferencia de datos no orientadas a conexión.

**Envío ordenado:** cuando las PDU no reciben en el mismo orden porque siguen diferentes caminos a través de la red se necesita que se mantenga un orden de las PDU para que la información llegue tal como se envió.

**Control de flujo:** limitar la cantidad o tasa de datos que envía la entidad emisora se hace uso de un procedimiento de parada y espera (stop-and-wait) en que cada PDU debe ser confirmada antes de ser enviada.

**Control de errores:** se incluyen detección de errores basadas en el uso de secuencia de comprobación de trama y de transmisión de PDU.

## Direccionamiento:

**Múltiplexación:** relacionado con el concepto de direccionamiento

**Servicios de transmisión:** un protocolo ofrece una gran variedad de servicios adicionales a las entidades que hagan uso de el.

## 2.1.11. PROTOCOLO TCP / IP

Protocolo de control de transmisiones / protocolo de Internet usados para el control de la transmisión en Internet permite que diferentes tipos de ordenadores se comuniquen a través de redes heterogéneas.

Una Internet bajo TCP / IP opera como una única red que conecta muchas computadoras de cualquier tamaño y forma

El protocolo TCP fue desarrollado antes que el modelo OSI por lo tanto TCP / IP no coinciden con los modelos O S I, T C P / I P consta de cinco niveles físico, enlace de datos, de red, de transporte y de aplicación.

**Físico:** soporta protocolos estándar (LAN) (MAN) (WAN)

**Transporte:** define TCP y (UDP)

**TCP / IP:** protocolo jerárquico compuesto por módulos interactivos que proporcionan funcionalidad específica.

## 2.1.12. ARQUITECTURA DE REDES

### 2.1.12.1. Conmutación de circuitos

Crea una línea directa entre dos dispositivos como teléfonos y computadoras, un conmutador es un dispositivo con N entradas y M salidas que crea una conexión temporal entre un enlace de entrada y otro de salida.

Conmutador plegado n por n conectar n líneas en modo full-duplex

**2.1.12.2. Conmutación de paquetes:**

Datos transmitidos en unidades discretas formados por bloques de longitud. La red establece la longitud máxima del paquete.

**2.1.12.3. Conmutación de paquetes en datagramas:**

Cada paquete es tratado en forma independiente de los otros

**2.1.12.4. Conmutación de paquetes en circuitos virtuales:**

Se mantiene la relación que existe entre todos los paquetes que pertenecen a un mismo mensaje, se implementan de dos formas

Circuitos virtuales conmutados (SVC)

Circuitos virtuales permanentes (PVC)

Proyecto 802 para definir estándares que permitan la intercomunicación entre equipos de distintos fabricantes, el modelo 802 no busca remplazar nada del modelo OSI busca especificaciones del nivel físico, el nivel de enlace de datos y en menos extensión el nivel de red permitiendo conectividad en protocolos LAN y WAN

El LLC no especifico para cada arquitectura, es el mismo para todas las LAN definidas por la IEEE

El proyecto 802 está en modularidad y se subdivide para la gestión de la LAN

802.1 dedicada a los aspectos de comunicación entre redes LAN y WAN aunque no está completo trata de resolver las incompatibilidades entre arquitectura de redes.

802.2 (LLC) toma la estructura de una trama HDLC control de enlace de datos de alto nivel, el LLC es la capa superior del nivel de enlace de datos del IEEE 802 común en todos los protocolos LAN

IEEE 802.3 ETHERNET define banda base y banda ancha

Método Acceso CSMD / CD siempre que múltiples usuarios tienen acceso incontrolado a una única línea existe el peligro de que las señales se solapen y se destruyan entre si. La solución se denomina acceso múltiple con detección de colisiones (CSMD) estandarizado en el IEEE 802.3

IEEE 802.4 Bus con paso de testigo: combina la característica de la ethernet y red de anillo con paso de testigo es un bus físico que opera como un anillo lógico usando testigos.

IEEE 802.5 red anillo con paso testigo: exige a las estaciones que envíen los datos por turnos, envía solo una trama en cada turno coordinado por el paso de testigo. Un testigo es una trama contenedor sencilla que se pasa de estación en estación alrededor del anillo.

LA X – 25: por costos elevados de líneas alquiladas se introdujeron las redes de paquetes conmutados donde las líneas compartidas reducen el costo. El primer grupo fue el grupo de protocolo X. 25 con baja tasa de bits y que puede ser conmutada. Poseen canales preestablecidos proporcionando un PVC (Circuito Virtual Permanente)

Resulta económico ya que las tarifas se basan en la cantidad de datos entregados y no en el tiempo de conexión.

FRAME RELAY: es una tecnología de conmutación rápida de tramas basada en estándares internacionales y que se utilizan como protocolo de transporte y de acceso a redes públicas. Ha evolucionado proporcionando la integración de una única línea de los distintos tipos de tráfico de datos y voz y transporte por una única red. Se adoptó estándares como:

ATM (Modo de Transferencia Asincronomo) protocolo de retransmisión de celdas capaz de transferir voz, video y datos a través de redes privadas y publicas basada en una arquitectura de celdas ya que son adecuadas para transportar voz y video porque es intolerante con el retardo

## 2.1.13. Clases de red A, B y C como identificarlas por su dirección Ip y máscara de subred

### Que es la dirección IP?

La dirección IP es un número único que identifica a una computadora o dispositivo conectado a una red que se comunica a través del protocolo de redes TCP (Transmission Control Protocol).

Para que entendamos mejor el IP debemos conocer primero el TCP. Un protocolo de red es como un idioma, si dos personas están conversando en idiomas diferentes ninguna entenderá lo que la otra quiere decir. Con las computadoras ocurre una cosa similar, dos computadoras que están conectadas físicamente por una red deben "hablar" el mismo idioma para que una entienda los requisitos de la otra. El protocolo TCP standariza el cambio de información entre las computadoras y hace posible la comunicación entre ellas. Es el protocolo más conocido actualmente pues es el protocolo standard de Internet.

El protocolo TCP contiene las bases para la comunicación de computadoras dentro de una red, pero así como nosotros cuando queremos hablar con una persona tenemos que encontrarla e identificarla, las computadoras de una red también tienen que ser localizadas e identificadas. En este punto entra la dirección IP. La dirección IP identifica a una computadora en una determinada red. A través de la dirección IP sabemos en que red está la computadora y cual es la computadora. Es decir verificado a través de un número único para aquella computadora en aquella red específica.

La dirección IP consiste en un número de 32 bits que en la práctica vemos siempre segmentado en cuatro grupos de 8 bits cada uno (xxx.xxx.xxx.xxx). Cada segmento de 8 bits varía de 0-255 y están separados por un punto.

Esta división del número IP en segmentos posibilita la clasificación de las direcciones IPs en 5 clases: A, B, C, D e Y.
Cada clase de dirección permite un cierto número de redes y de computadoras dentro de estas redes.
En las redes de clase A los primeros 8 bits de la dirección son usados para

identificar la red, mientras los otros tres segmentos de 8 bits cada uno son usados para identificar a las computadoras.

Una dirección IP de clase A permite la existencia de 126 redes y 16.777.214 computadoras por red. Esto pasa porque para las redes de clase A fueron reservados por la IANA (Internet Assigned Numbers Authority) los IDs de "0" hasta "126".

Los tipos de redes utilizados normalmente son A, B y C aunque existen los de tipo D y E que están destinados a otros usos.

## ➢ Redes de clase A

Las redes de clase A tienen como número en su primer segmento uno comprendido entre el 1 y 126 ambos incluidos, vamos con unos ejemplos:

La dirección Ip **80**.85.23.164 es de clase A
La dirección Ip **186**.23.54.69 no es de clase A
La dirección Ip **126**.36.76.65 es de clase A

Y por último queda la identificación por su máscara de subred que va a ser **255.0.0.0**

## ➢ Redes de clase B

Las redes de clase B tienen en su primer segmento números comprendidos entre el 128 y el 191 ambos incluidos vamos a verlo:

La dirección Ip **149**.34.127.143 es de clase B
La dirección Ip **42**.169.221.86 no es de clase B
La dirección Ip **129**.3.45.131 es de clase B

En este caso la máscara de subred va a ser **255.255.0.0**

- **Redes de clase C**

Y para terminar las de clase C, son la que utizamos nosotros y en las que su primer segmento se encuentra entre el 192 y 223 ambos incluidos y vamos a verlo con unos ejemplos:

La dirección Ip **192**.78.91.97 es de clase C
La dirección Ip **97**.142.174.162 no es de clase C
La dirección Ip **201**.121.41.63 es de clase C

Esta es la más conocida como sabemos la máscara de subred es la conocida 255.255.255.0 y es para redes de tipo LAN (Local Area Network).

## Direcciones privadas

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten a través del protocolo NAT. Las direcciones privadas son:

**Clase A:** 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).

**Clase B:** 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.

**Clase C:** 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C contiguas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para estas circunstancias. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

## Máscara de subred

La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP. Dada la dirección de clase A 10.2.1.2 sabemos que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma. La máscara se forma poniendo a 1 los bits que identifican la red y a 0 los bits que identifican el host. De esta forma una dirección de clase A tendrá como máscara 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0.

Los dispositivos de red realizan un AND entre la dirección IP y la máscara para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo un router necesita saber cuál es la red a la que pertenece la dirección IP del datagrama destino para poder consultar la tabla de encaminamiento y poder enviar el datagrama por la interfaz de salida. Para esto se necesita tener cables directos.

## Creación de subredes

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Un ejemplo de uso es cuando necesitamos agrupar todos los empleados pertenecientes a un departamento de una empresa. En este caso crearíamos una subred que englobara las direcciones IP de éstos. Para conseguirlo hay que reservar bits del campo host para identificar la subred estableciendo a uno los bits de red-subred en la máscara. Por ejemplo la dirección 172.16.1.1 con máscara 255.255.255.0 nos indica que los dos primeros octetos identifican la red (por ser una dirección de clase B), el tercer octeto identifica la subred (a 1 los bits en la máscara) y el cuarto identifica el host (a 0 los bits correspondientes dentro de la máscara). Hay dos direcciones de cada subred que quedan reservadas: aquella que identifica la subred (campo host a 0) y la dirección para realizar broadcast en la subred (todos los bits del campo host en 1).

## IP dinámica

Una **dirección IP dinámica** es una IP asignada mediante un servidor DHCP (**Dynamic Host Configuration Protocol**) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC 2131 especifica la última definición de DHCP (marzo de 1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. Éstas suelen cambiar cada vez que el usuario reconecta por cualquier causa.

## ***Ventajas***

- Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
- Reduce la cantidad de IP asignadas (de forma fija) inactivas.

## ***Desventajas***

- Obliga a depender de servicios que redirigen un host a una IP.

## ***Asignación de direcciones IP***

Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

✓ **manualmente**, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creada manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.

✓ **automáticamente**, donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.

✓ **dinámicamente**, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

## IP fija

Una **dirección IP fija** es una IP asignada por el usuario de manera manual. Mucha gente confunde IP Fija con IP Pública e IP Dinámica con IP Privada.

Una IP puede ser Privada ya sea dinámica o fija como puede ser IP Pública Dinámica o Fija.

Una IP Pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie por eso siempre la IP Pública se la configura de manera Fija y no Dinámica, aunque si se podría.

En el caso de la IP Privada generalmente es dinámica asignada por un servidor DHCP, pero en algunos casos se configura IP Privada Fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del

número de IP que tenemos, si esta cambiara (fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

Las **IP Públicas fijas** actualmente en el mercado de acceso a Internet tienen un costo adicional mensual. Estas IP son asignadas por el usuario después de haber recibido la información del proveedor o bien asignadas por el proveedor en el momento de la primera conexión.

Esto permite al usuario montar servidores web, correo, FTP, etc. y dirigir un nombre de dominio a esta IP sin tener que mantener actualizado el servidor DNS cada vez que cambie la IP como ocurre con las IP Públicas dinámicas.

## Direcciones IPv6

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la tierra tenga asignada varios millones de IPs, ya que puede implementarse con $2^{128}$ ($3.4\times10^{38}$ hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas de notación acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales, como en IPv4, se pueden obviar.

Ejemplo: *2001:0123:0004:00ab:0cde:3403:0001:0063* -> ***2001:123:4:ab:cde:3403:1:63***

- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer **una** vez.

Ejemplo: *2001:0:0:0:0:0:0:4* -> ***2001::4***.

Ejemplo no válido: *2001:0:0:0:2:0:0:1* -> *2001::2::1* (debería ser *2001::2:0:0:1* ó *2001:0:0:0:2::1*).

## 2.1.14. Packet Tracer

**Packet Tracer** es la herramienta de aprendizaje y simulación de redes interactiva Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

Este producto tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando – línea de los dispositivos de Cisco para práctica y aprender por descubrimiento.

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego clickando en ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco IOS e incluso funciona el "tab completion". Una vez completada la configuración física y lógica de la red. También se puede hacer simulaciones de conectividad (pings, traceroutes, etc) todo ello desde las propias consolas incluidas.

**Principales funcionalidades**

Entre las mejoras del Packet Tracer 5 encontramos:

- Soporte para Windows (2000, XP, Vista) y Linux (Ubuntu y Fedora).

- Permite configuraciones multiusuario y colaborativas en tiempo real.

- Soporte para IPv6, OSPF multiárea, redistribución de rutas, RSTP, SSH y Switchs multicapa.

**Soporta los siguientes protocolos:**

- HTTP, Telnet, SSH, TFTP, DHCP y DNS.

- TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6.

- RIP, EIGRP, OSPF Multiárea, enrutamiento estático y redistribución de rutas.

- Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP.

- ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP, Polly Mkt.

## Nuevos recursos, actividades y demostraciones:

- OSPF, IPv6, SSH, RSTP, Frame Relay, VLAN's, Spanning Tree,Mike mkt etc.

# Interfaces y Escenario del Packet Tracer


Para una mejor comprensión y detalle dividí las diferentes interfaces. En cada una van a encontrar el detalle y uso de cada item. Comencemos.

## A) Interfaz Standard


**1)** Nuevo / Abrir / Guardar / Imprimir / Asistente para actividades.

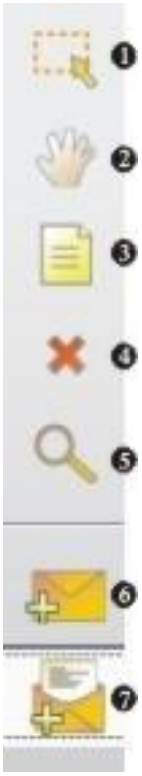
**2)** Copiar / Pegar / Deshacer.

**3)** Aumentar Zoom / Tamaño original / Reducir Zoom.

**4)** Dibujar figuras (cuadrados, círculos y líneas).

**5)** Panel de Dispositivos Personalizados: Sirve para agregar o quitar dispositivos personalizados.

## B) Herramientas




**1)** Puntero. Sirve para seleccionar cualquier item o área en el escenario.

**2)** Sirve para mover el escenario.

**3)** Sirve para hacer anotaciones en el escenario.

**4)** Borrar del escenario un item.

**5)** Muestra las tablas del dispositivo (enrutamiento, NAT, ARP, MAC, etc.).

**6)** Inyecta tráfico simple (ping) de dispositivo a dispositivo.

**7)** Inyecta tráfico complejo (IP destino, TTL, intervalos, HTTP, Telnet, SNMP).

## C) Dispositivos


**1) Routers:** Muestra en el panel **9)** los modelos de routers disponibles.

**2) Switchs:** Muestra en el panel **9)** los modelos de switchs disponibles.

**3) Hubs:** Muestra en el panel **9)** los modelos de hubs disponibles.

**4) Dispositivos Wireless:** Muestra en el panel **9)** los modelos de dispositivos Wireless disponibles.

**5) Medios:** Muestra en el panel **9)** los medios (serial, fibra, consola, etc) disponibles.

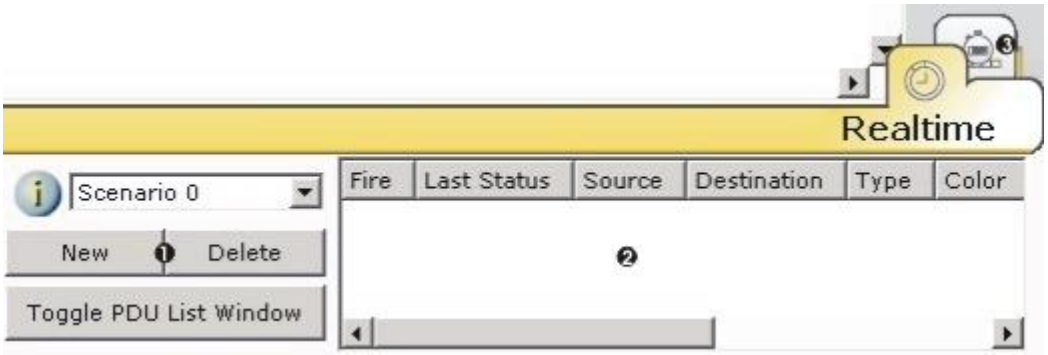
**6) Dispositivos Finales:** Muestra en el panel **9)** los dispositivos finales (impresora, host, server, etc.) disponibles.

**7) Emulación WAN:** Muestra en el panel **9)** las diferentes emulaciones WAN (DSL, módem, cable, etc.) disponibles.

**8) Dispositivos Personalizados:** Muestra en el panel **9)** los diferentes dispositivos personalizados disponibles.

**9) Panel de Dispositivos Seleccionados:** Muestra los dispositivos disponibles según nuestra selección para utilizar en la topología. Se hace click en el dispositivo que deseamos utilizar y luego click en la parte del escenario que queremos ubicar nuestro dispositivo.

## D) Tráfico




**1)** Crea escenarios para las diferentes PDU.

**2)** Muestra los resultados de las diferentes PDU.

**3)** Abre una ventana que muestra las transacciones de diferentes PDU en tiempo real.

# 2.1.15. AutoCAD

**AutoCAD** es un programa de diseño asistido por ordenador para dibujo en 2D y 3D. Actualmente es desarrollado y comercializado por la empresa Autodesk.

La primera versión de este software fue lanzada en noviembre de 1982 y la última versión es la 2008, lanzada hace unos cuantos meses.

AutoCAD gestiona una base de datos de entidades geométricas (puntos, líneas, arcos, etc.) con la que se puede operar a través de una pantalla gráfica en la que se muestran éstas, el llamado editor de dibujo. **La interacción del usuario se realiza a través de comandos**, de edición o dibujo, desde la línea de órdenes, a la que el programa está fundamentalmente orientado. Las versiones modernas del

programa permiten la introducción de éstas mediante una interfaz gráfica de usuario.

Como todos los programas de diseño asistido por computadora, procesa imágenes de tipo vectorial, aunque admite incorporar archivos de tipo fotográfico o mapa de bits, donde se dibujan figuras básicas o primitivas (líneas, arcos, rectángulos, textos, etc.), y mediante herramientas de edición se crean gráficos más complejos.

Parte del programa AutoCAD está orientado a la producción de planos, empleando para ello los recursos tradicionales de grafismo en el dibujo, como color, grosor de líneas y texturas tramadas. AutoCAD, a partir de la versión 11, utiliza el concepto de espacio modelo y espacio papel para separar las fases de diseño y dibujo en 2D y 3D, de las específicas para obtener planos trazados en papel a su correspondiente escala.

Las aplicaciones del programa son múltiples, desde proyectos y presentaciones de ingeniería, hasta diseño de planos o maquetas de arquitectura.

# CAPITULO III

## 3. Recursos Metodológicos

### 3.1. Tipo de investigación

El tipo de investigación que se empleo fue experimental

### 3.2. Nivel de la investigación

Los niveles de investigación que utilizamos fueron: propositivo, prospectivo, no participativa, aplicada.

## 3.3. Métodos y Técnicas de Investigación

### 3.3.1. Métodos

Se utilizo como método general, el científico y como particular el experimental.

### 3.3.2. Técnicas

La técnica que se aplico es la observación directa para detectar los problemas de seguridad y transmisión de datos de la Clínica Dr. Rafael Hernández Troya.

### 3.3.3. Procedimientos

Los procedimientos que aplicamos fueron el analítico y descriptivo.

**Analítica**, porque nos permitió un análisis del problema, para su rectificación.

**Descriptiva**, por cuanto a través de la información obtenida, se clasifico los elementos y estructuras para caracterizar una realidad.

## 3.4. Diseño De La Investigación

### 3.4.1. Modalidad Básica de la Investigación

En la presente investigación se empleo la modalidad **documental,** por apoyarse en las referencias científicas en el área de redes.

## 3.5. Métodos de Investigación

### 3.5.1. Métodos y Técnicas de la Investigación

La metodología guardo relación directa con el marco teórico y el problema de la investigación, en consecuencia, para el presente trabajo de investigación creímos pertinente aplicar la observación directa de los participantes (dueño de clínica, profesionales de la medicina, etc), por considerarla más adecuada y a las posibilidades de involucrar a todos los estratos inmersos en la problemática, y con las opiniones de ellos planteamos alternativas de solución.

Para iniciar se delimito y selecciono el "**área estratégica" y "unidades especificas",** donde se realizo la investigación. Para nuestro caso se selecciono y delimito como área estratégica a la Clínica Dr. Rafael Hernández Troya, para lo cual enviamos una solicitud pidiendo autorización para realizar nuestro trabajo y como unidad específica al edificio de los herederos Hernández Troya, ubicado en las calles García Moreno y Eloy Alfaro.

Se trabajo siguiendo un método científico, planteado en nuestro proyecto, optado para descubrir las formas de existencias de los procesos y resultados del problema investigado **"Como debe ser una red inalámbrica que optimice los**

**recursos de información en la Clínica Dr. Rafael Hernández Troya, donde funciona la Fundación Teolinda Troya Escobar?"**

### 3.5.2. Fase Indagatoria

Se utilizaron técnicas pertinentes y se elaboraron los pasos a seguir en este trabajo de investigación para cumplir con la información empírica, para ello:

### 3.5.3. Fase Demostrativa

Después de haber revisado y realizado las técnicas y pasos respectivos sistematizamos esta información y luego, realizamos la instalación y configuración de la red inalámbrica.

- Solicitamos la autorización respectiva al dueño de la clínica para realizar nuestro proyecto de tesis.

- Luego de obtener la autorización correspondiente, realizamos un recorrido por las instalaciones de la clínica para definir el lugar en donde se encontrarían las pcs.

- Solicitamos cotizaciones de los equipos que se requerían para realizar la red inalámbrica (computadoras, tarjeta de red, Access point, etc).

- Entregamos el informe de las cotizaciones al dueño de la clínica.

- Realizamos las compras de los equipos.

- Instalamos los equipos en cada piso, y realizamos la configuración de los mismos.

- Luego realizamos la configuración de la red.

- Comprobamos que la red funcione correctamente.

### 3.5.3.1. Pasos para configurar una red inalámbrica

1. Primero revisamos en la barra de tareas el estado de la red, es decir si se encuentra desconectada o si no ha sido instalada

2. Al encontrar el icono de la red, dimos click derecho sobre él para realizar la búsqueda de la red y luego apareció un menú con varias opciones en donde escogimos **ver redes inalámbricas disponibles.**

3. En la ventana de conexiones de redes inalámbricas seleccionamos la opción **elegir una red inalámbrica,** a continuación actualizamos **la lista de redes** para poder observar las redes inalámbricas a las que podemos acceder.

4. Luego apareció una ventana en la que nos indicaba que está buscando las redes disponibles en el computador, esto tardo poco tiempo, y en la misma ventana mostro el resultado.

5. Después de haber obtenido el resultado de la búsqueda, seleccionamos la red que deseamos y si queremos podemos cambiar el nombre de la misma, y damos click en conectar.

6. A continuación, nos solicita la clave de la red para acceder, la introducimos y luego seleccionamos **conectar**.

7. Luego el asistente de conexión intentara conectar a la red que hemos seleccionado, si la clave introducida es correcta se completara la acción.

**8.** Si la red se ha conectado correctamente, aparecerá los detalles en una **ventana**

9. Luego regresamos a la barra de tareas, damos click derecho sobre el icono de la red y seleccionamos el **estado.**

**10.** En la ventana de estado de conexiones de las redes inalámbricas, nos muestra las características de la conexión: **Estado, Red, Duración, Velocidad, Intensidad de la señal**

11. Al seleccionar **\/88**, aparecerá en la misma ventana el adaptador y los tipos de componentes de la red que estamos utilizando.

12. En la opción **Redes Inalámbricas,** definimos si la conexión que creamos se conectara automáticamente, además podemos agregar o quitar conexiones, y ver sus propiedades.

13. En la pestaña **Opciones avanzadas** definimos las configuraciones de los cortafuegos o Firewall, y si la conexión será compartida.

### 3.5.3.2. Configurar un router inalámbrico D-Link

Paso 1. Enchufa un extremo del cable Ethernet en el módem DSL.

Paso 2. Luego enchufa el otro extremo en el puerto "*WAN*" en la parte posterior del router inalámbrico D-Link.

Paso 3. Conecta la PC a cualquiera de los otros puertos Ethernet del router utilizando un cable Ethernet.

#### *3.5.3.3. Cómo acceder a la pantalla de configuración D-Link*

Paso 1. Abre tu navegador web y escribe "*http://192.168.0.1*" en la barra de direcciones, y luego presiona "*Enter*".

Paso 2. Usa "*Admin*" como nombre de usuario en el cuadro de pop-up y deja la contraseña en blanco.

Paso 3. Haz clic en "*OK*". Ahora verás la pantalla de configuración D-Link.

#### *3.5.3.4. Configuración General de Seguridad (Set Up General Security)*

Paso 1. Cambia tu contraseña de administración haciendo clic en la ficha "*Tools*" y seleccionando el botón "*Admin*". Introduce una nueva contraseña en la opción "*Administrator*". Confirma y haz clic en "*Apply*".

Paso 2. Deshabilita la Red de Área Local (LAN), si no es necesaria, ya que te asegura de que nadie más será capaz de acceder a tu red.

Paso 3. Ve a la pestaña "*Home*", selecciona "*Wireless*" y selecciona la opción "*Off*".

#### *3.5.3.5. Protocolo de habilitar el cifrado inalámbrico (Enable Wireless Encryption Protocol "WEP")*

Paso 1. Busca la pestaña "*Home*" en la pantalla de configuración D-Link y haz clic en el botón "*Wireless*".

Paso 2. Utiliza la opción "*Open System*" al lado del botón "*Authentication*".

Paso 3. Selecciona el botón "*Enabled*" junto a "*WEP*" y establece la clave de cifrado en "*128 bit*".

Paso 4. Establece el "*Key Type*" a "*ASCII*" y elije una contraseña de 13 dígitos para la "*Key 1*".

Paso 5. Escribe la contraseña en un lugar seguro.

Paso 6. Haz clic en "*Apply*".

#### *3.5.3.6. Cambiar el SSID*

Paso 1. Cambia el SSID para que sea más difícil a otras personas localizar y utilizar tu red, haz clic en la pestaña "*Home*" y localiza el botón "*Wireless*".

Paso 2. Cambia el SSID por defecto a una de tu elección, a continuación, haz clic en "*Apply*".

Paso 3. Deshabilita la opción SSID broadcasting. Bajo la pestaña "*Advanced*", haz clic en "*Performance*" y marca la opción "*Disabled*". Una vez más, haz clic en "*Apply*".

### *3.5.3.7. Filtro de direcciones MAC (MAC Addresses)*

Paso 1. Haz clic en la pestaña "*Advanced*" en la pantalla de configuración de D-Link y selecciona el botón "*Filters*".

Paso 2. Elije la opción "*MAC Filters*" y haz clic en "*Only Allow Computers with MAC Address Listed Below to Connect to the Network*".

Paso 3. Escribe el nombre y la dirección MAC de las computadoras que permitirás acceder a la red, comenzando por el que actualmente estás configurando. Haz clic en "*Apply*".

# CAPITULO IV

# 4. Análisis e interpretación en relación a las hipótesis de la investigación

La información teórica construida orienta al análisis de los datos empíricos, obtenidos en la investigación. Los resultados se presentan en función de las hipótesis que orientaron nuestro trabajo de investigación.

**"INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA "DR. RAFAEL HERNANDEZ TROYA"**

Las hipótesis generales y específicas o particulares que nos planteamos como orientadores del presente trabajo de investigación, se enunciaron de la siguiente manera:

## 4.1. Hipótesis General

Si se crea una red inalámbrica segura se lograra optimizar el flujo de la información de la Clínica Dr. Rafael Hernández Troya.

## 4.2. Hipótesis Particulares

**HIP1.-** El uso de una red inalámbrica segura se lograra disponer de información actualizada de los pacientes, de cada área.

**HIP2.-** El uso de una red inalámbrica segura permitirá almacenar información histórica de los pacientes de la Clínica Dr. Rafael Hernández Troya.

**Variable HIP1.-**

- ☞ Características de la red inalámbrica segura.

**Variable HIP2.-**

- ☞ Calidad de la información

## 4.3. Operacionalización de las Hipótesis

Para efecto de una mejor comprensión de la relación horizontal que existen de las variables y categorías definidas y los correspondientes indicadores, presentamos matrices operacionales por hipótesis específicos o particulares.

## ✓ Operacionalización de las hipótesis particular

| VARIABLES | DEFINICION | INDICADORES |
|---|---|---|
| **INDEPENDIENTE:**<br><br>Red inalámbrica segura.<br><br>**DEPENDIENTE:**<br>Calidad de la información | ✓ Es aquella que no permite el acceso indebido al sistema por parte de usuarios no autorizados por el administrador.<br><br>✓ Estado de la conformidad de la información con relación a las necesidades institucionales. | ✓ Velocidad<br>✓ Seguridad<br>✓ Confiabilidad<br>✓ Accesibilidad<br><br>✓ Historial clínico actualizado de forma inmediata.<br>✓ Disponibilidad de la información cuando es requerida. |

# CAPITULO V

## 5. Recursos y Presupuestos

### 5.1. Recursos Humanos

☞ 2 Egresadas de la Facultad de Administración Finanzas e Informática.
☞ 2 digitadoras

### 5.2. Recursos Materiales

☞ 7 Computadores Multimedia
☞ 7 Tarjetas de Red inalámbrica
☞ 1 Router inalámbrico
☞ 1 Access Point
☞ 7 escritorios para computadores
☞ 7 Reguladores de Voltaje
☞ 1 Proveedor de Internet

### 5.3. Recursos Económicos

Los recursos económicos son aporte de los autores del proyecto y propietario de la clínica.

### 5.4. Presupuesto

| CANTIDAD | UNIDAD | CONCEPTO | VALOR UNITARIO | TOTAL |
|---|---|---|---|---|
| **7** | | **Computador** | **$ 699.00** | **$ 4893.00** |
| **7** | | **Tarjeta de red inalámbrica** | **24.00** | **168.00** |
| **1** | | **Router** | **55.00** | **55.00** |

| | | | | |
|---|---|---|---|---|
| | | **inalámbrico** | | |
| **1** | | **Access Point** | **70.00** | **70.00** |
| **1** | | **Digitadora** | **200.00** | **400.00** |
| **1** | | **Transporte** | **60.00** | **60.00** |
| **1** | | **Otros** | **50.00** | **50.00** |
| **TOTAL:** | | | | **$5676.00** |

# Capítulo VI

## 6. Cronograma de Actividades

| TIEMPO | OCTUBRE | | | | NOVIEMBRE | | | | DICIEMBRE | | | | MARZO | | | | ABRIL | | | | MAYO | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACTIVIDADES | I | II | III | IV | I | II | III | IV | I | II | III | IV | I | II | III | IV | I | II | III | IV | I | II | III | IV |
| PREPARACION DEL PERFIL DEL PROYECTO | X | X | | | | | | | | | | | | | | | | | | | | | | |
| REAJUSTE DEL PERFIL DEL PROYECTO | | | X | X | | | | | | | | | | | | | | | | | | | | |
| PRESENTACION DEL PROYECTO | | | | X | | | | | | | | | | | | | | | | | | | | |
| APROBACION DEL PROYECTO | | | | | X | | | | | | | | | | | | | | | | | | | |
| INCORPORACION DE OBSERVACIONES AL PERFIL DEL | | | | | | X | | | | | | | | | | | | | | | | | | |
| ELABORACION DEL BORRADOR DEL PROYECTO | | | | | | | X | | | | | | | | | | | | | | | | | |
| PRESENTACION AL DIRECTOR - ASESOR DEL PROYECTO | | | | | | | | X | | | | | | | | | | | | | | | | |
| REDACCION FINAL DEL PROYECTO | | | | | | | | | X | | | | | | | | | | | | | | | |
| ENGTREGA DEL PROYECTO | | | | | | | | | | X | | | | | | | | | | | | | | |
| ANALISIS DE LA SITUACION PROBLEMATICA | | | | | | | | | | X | X | | | | | | | | | | | | | |
| ELABORACION DE INSTRUMENTOS | | | | | | | | | | | | X | | | | | | | | | | | | |
| APLICACION DE INSTRUMENTOS | | | | | | | | | | | | X | X | | | | | | | | | | | |
| EXTRACCION DE CONCLUSIONES DE LA HIPOTESIS | | | | | | | | | | | | | | X | | | | | | | | | | |
| REDACCION DE INFORMES DE LOS RESULTADOS | | | | | | | | | | | | | | | X | | | | | | | | | |
| REDACCION DE INFORMES DE LOS RESULTADOS POR EL | | | | | | | | | | | | | | | | X | X | | | | | | | |
| REDACCION FINAL DEL INFORME DE LOS RESULTADOS | | | | | | | | | | | | | | | | | | | | | X | | | |
| ENTREGA DE INFORME | | | | | | | | | | | | | | | | | | | | | | X | X | |
| SUSTENTACION DEL INFORME | | | | | | | | | | | | | | | | | | | | | | | | X |

# Capítulo VII

# 7. Conclusiones y Recomendaciones

## 7.1. Conclusiones

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho, que la utilización de estas redes se hayan incrementado desde el año 2002 siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

El presente trabajo pretendió dar una visión global del estado actual de la seguridad de las redes inalámbricas, desde los riesgos existentes en los estándares actuales, hasta las mejores propuestas para subsanar y para evitar la filtración de la información.

El presente trabajo nos llevo a realizar una labor social, en la fundación Teolinda Troya Escobar, la misma que funciona en la Clínica Dr. Rafael Hernández Troya, ya que es una fundación que recién está empezando hacer labor social.

Por lo expuesto anteriormente nos lleva a considerar que era necesario apoyar y dar solución a este problema de la inexistencia de la red inalámbrica en el edificio donde funciona la Clínica Dr. Rafael Hernández Troya.

**Enunciando el problema:**

“Como debe ser una red inalámbrica que optimice los recursos de información en la Clínica Dr. Rafael Hernández Troya, donde funciona la Fundación Teolinda Troya Escobar?”

Se justifico porque a través de la implementación de la red inalámbrica, pudimos demostrar los conocimientos adquiridos como estudiante de la Universidad Técnica de Babahoyo en la Facultad de Administración Finanzas e Informática.

El trabajo de campo se realizo en la clínica Dr. Rafael Hernández Troya, ubicado en el edifico de los herederos Hernández Troya, localizado en las calles Eloy Alfaro y Sucre.

Se justifico porque en la clínica Dr. Rafael Hernández Troya no contaba con la implementación de ningún tipo de red.

Con el diseño de la red inalámbrica segura en la clínica Dr. Rafael Hernández se dio solución al problema del envío y recepción de la información de una terminal a las diferentes áreas de las clínicas.

Así como también se mantiene la información histórica de los pacientes almacenada y actualizada, respecto de las diferentes áreas de la Clínica Dr. Rafael Hernández Troya, para uso tanto de consulta externa como de cirugía.

Al término de este trabajo se ha podido demostrar que las hipótesis presentadas han sido comprobadas.

## 7.2. Recomendaciones

Consideramos que el crear e instalar redes inalámbricas, en los diferentes departamentos de las instituciones públicas es de gran utilidad para la agilidad de los procesos.

Consideramos que el crear e instalar redes inalámbricas, optimiza el trabajo de los empleados en las instituciones en donde existe estas instalaciones.

Y por ultimo queremos que nuestro trabajo documental y de campo sirva como lectura y apoyo para futuras investigaciones de los estudiantes y personas naturales.

# Bibliografía

## Direcciones URL de Internet


1. http://www.arturosoria.com/eprofecias/art/wireless_seguridad.asp

2. http://dns.bdat.net/seguridad_en_redes_inalambricas/

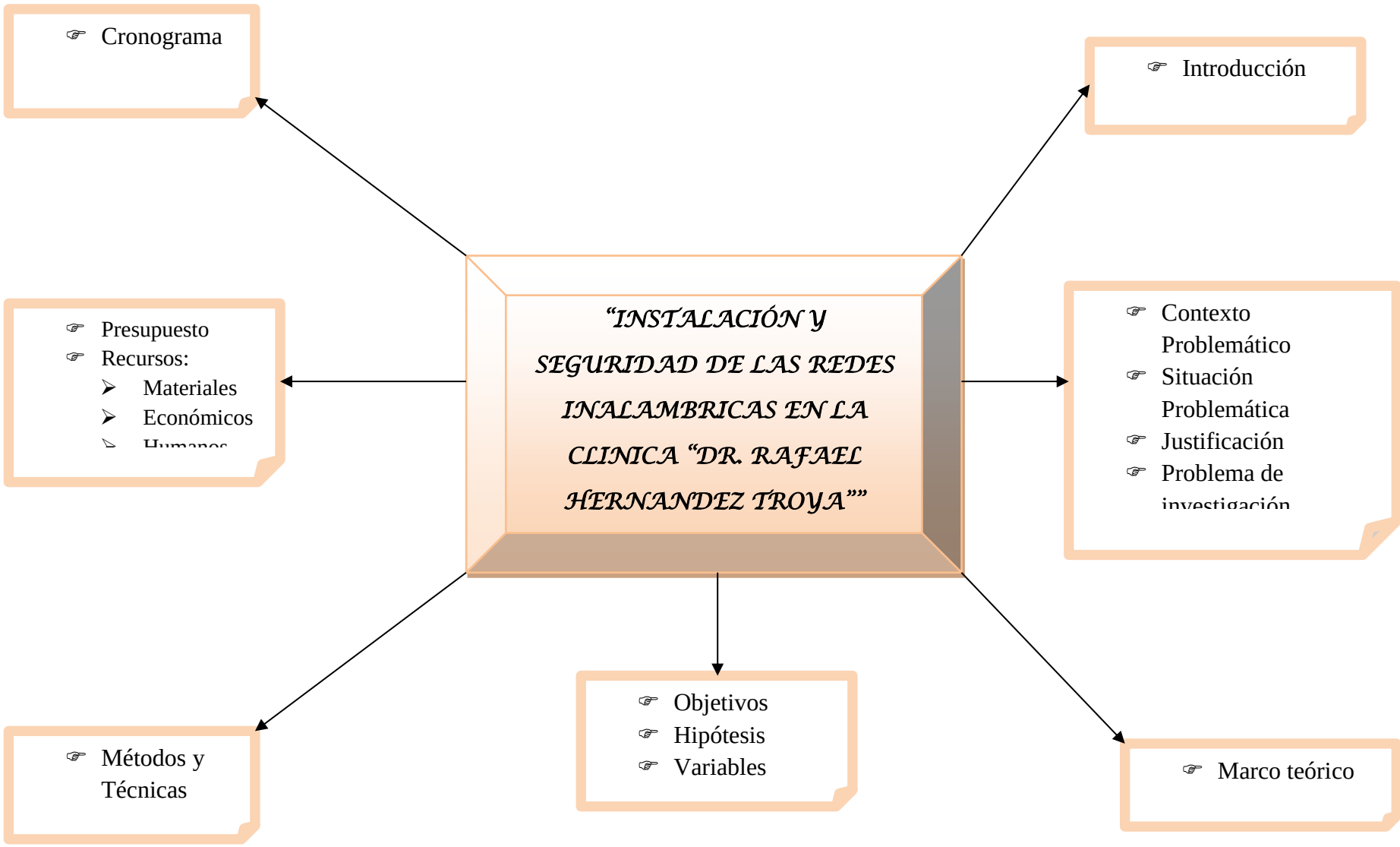
3. http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

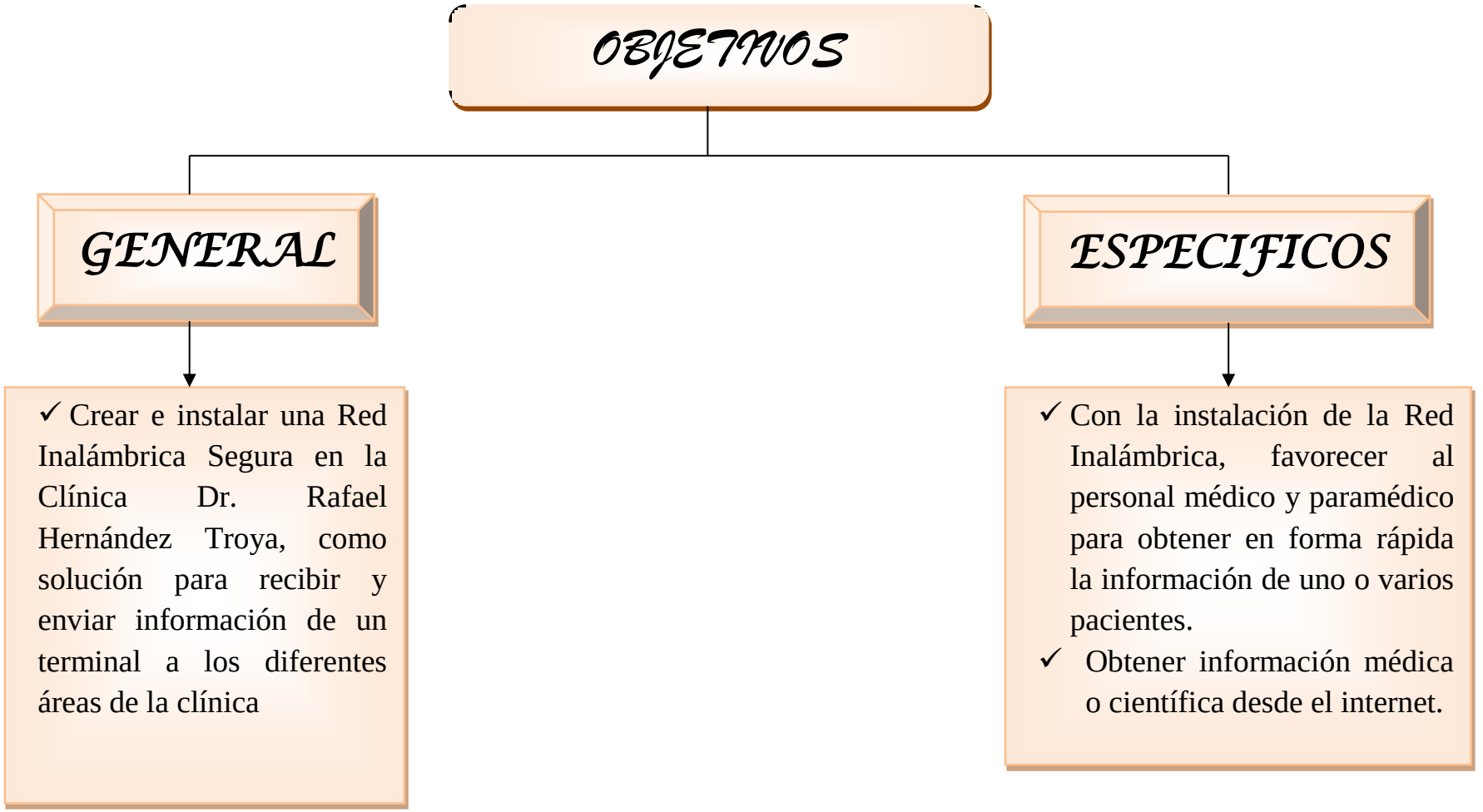
4. http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml

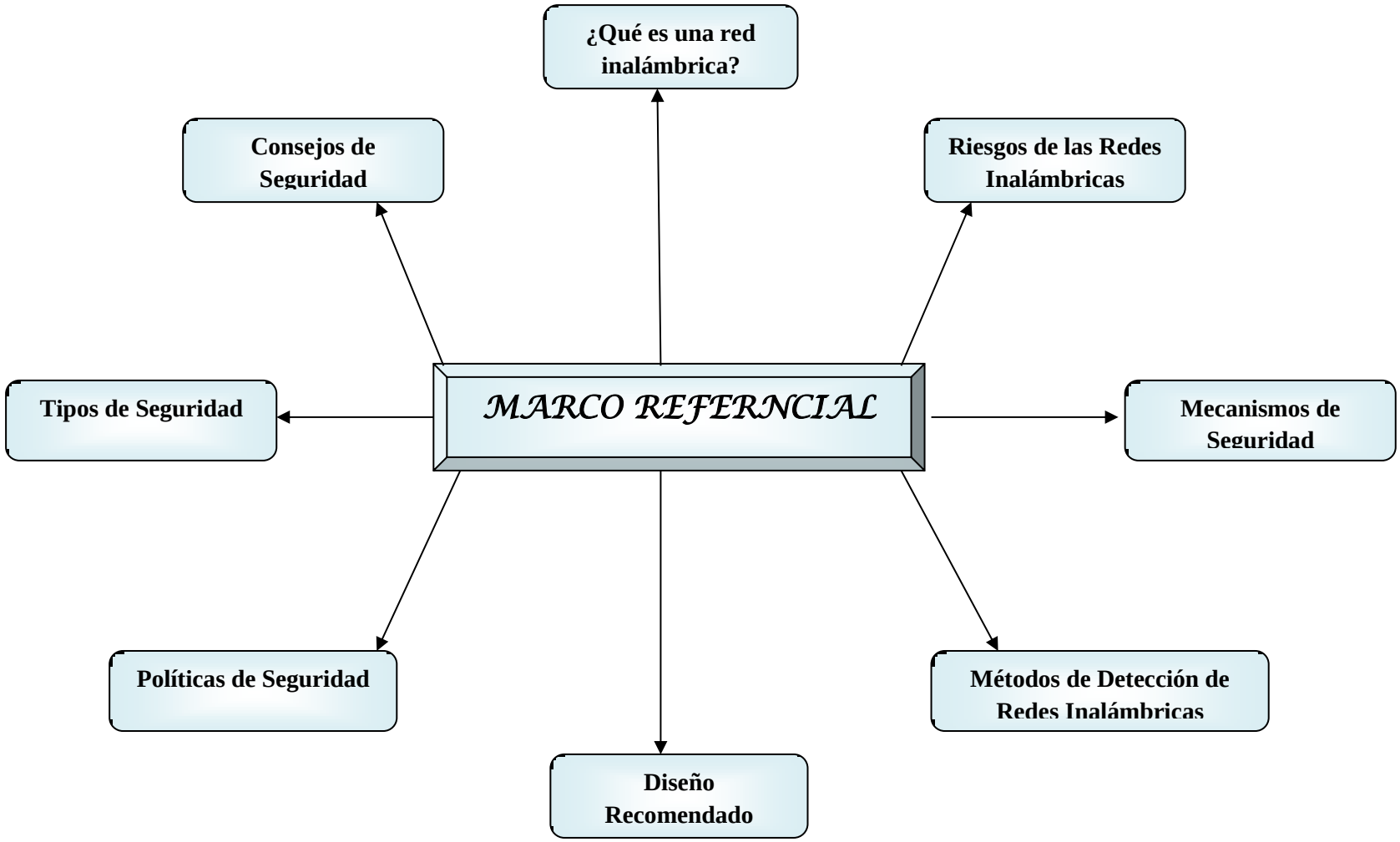
5. http://www.saulo.net/pub/inv/SegWiFi-art.htm

6. http://www.zonagratuita.com/servicios/seguridad/wireles.html

# ANEXOS


Cronograma
Introducción
Presupuesto
Recursos:
Materiales
Económicos
Humanos
"INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA "DR. RAFAEL HERNANDEZ TROYA""
Contexto Problemático
Situación Problemática
Justificación
Problema de investigación
Métodos y Técnicas
Objetivos
Hipótesis
Variables
Marco teórico


OBJETIVOS
GENERAL
ESPECIFICOS
✓ Crear e instalar una Red Inalámbrica Segura en la Clínica Dr. Rafael Hernández Troya, como solución para recibir y enviar información de un terminal a los diferentes áreas de la clínica
✓ Con la instalación de la Red Inalámbrica, favorecer al personal médico y paramédico para obtener en forma rápida la información de uno o varios pacientes.
✓ Obtener información médica o científica desde el internet.


¿Qué es una red inalámbrica?
Consejos de Seguridad
Riesgos de las Redes Inalámbricas
Tipos de Seguridad
MARCO REFERNCIAL
Mecanismos de Seguridad
Políticas de Seguridad
Métodos de Detección de Redes Inalámbricas
Diseño Recomendado

**MATRIZ DE CONSISTENCIA (ESTRUCTURA ANALITICA)**

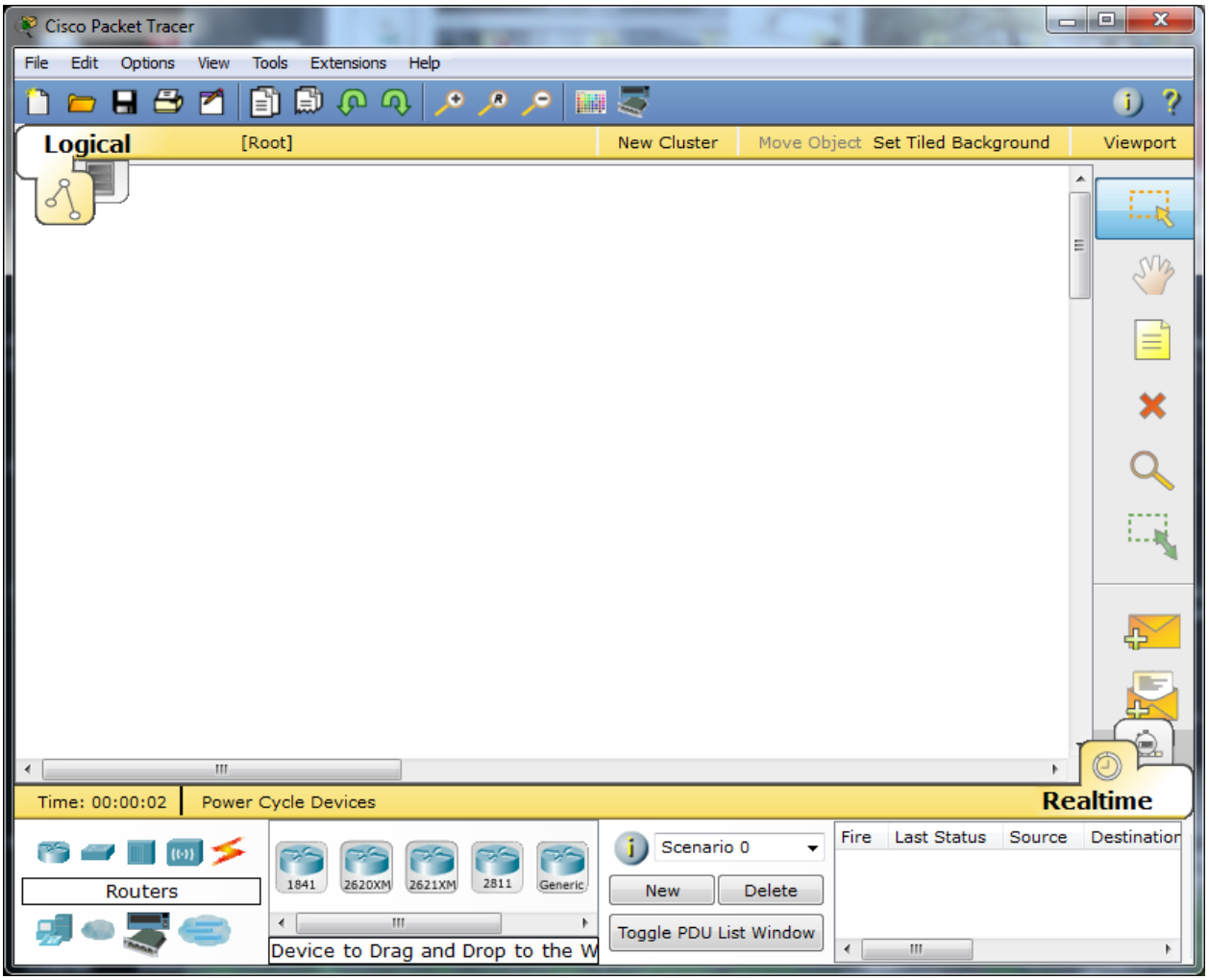
**TITULO DE LA INVESTIGACIÓN: “INSTALACIÓN Y SEGURIDAD DE LAS REDES INALAMBRICAS EN LA CLINICA “DR. RAFAEL HERNANDEZ TROYA”**

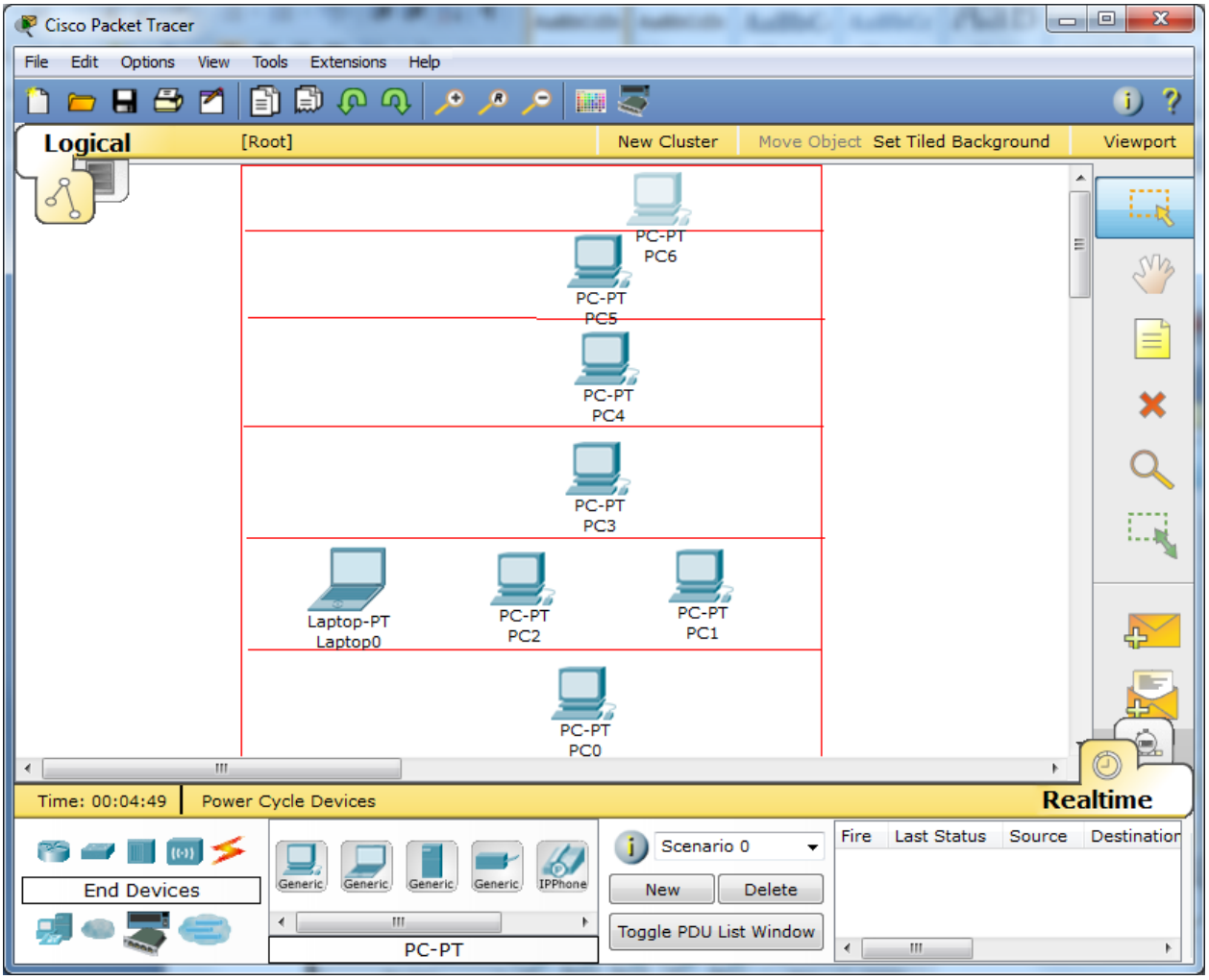
| PROBLEMAS | OBJETIVOS | HIPOTESIS | VARIABLES | INDICADORES | SUBINDICADORES |
|---|---|---|---|---|---|
| **“Como crear e instalar una red inalámbrica segura en la Clínica Dr. Rafael Hernández Troya”** | ✓ Crear e instalar una Red Inalámbrica Segura en la Clínica Dr. Rafael Hernández Troya, como | ¿Por qué crear e instalar una red inalámbrica en la Clínica “Dr. Rafael Hernández Troya”?, ubicada en las calles: García | **INDEPENDIENTE:** Para servir en la atención médica de los pacientes de escasos recursos económicos de la ciudad de Babahoyo.<br><br>**DEPENDIENTE:** Para ayudar en la | Apertura de historial clínico.<br>Recepción y emisión de la información.<br>Investigación científica por internet.<br>Interconsulta.<br><br>Consultas | ✓ Satisfacción en el paciente<br>✓ Rapidez<br>✓ Comprobación de la información |

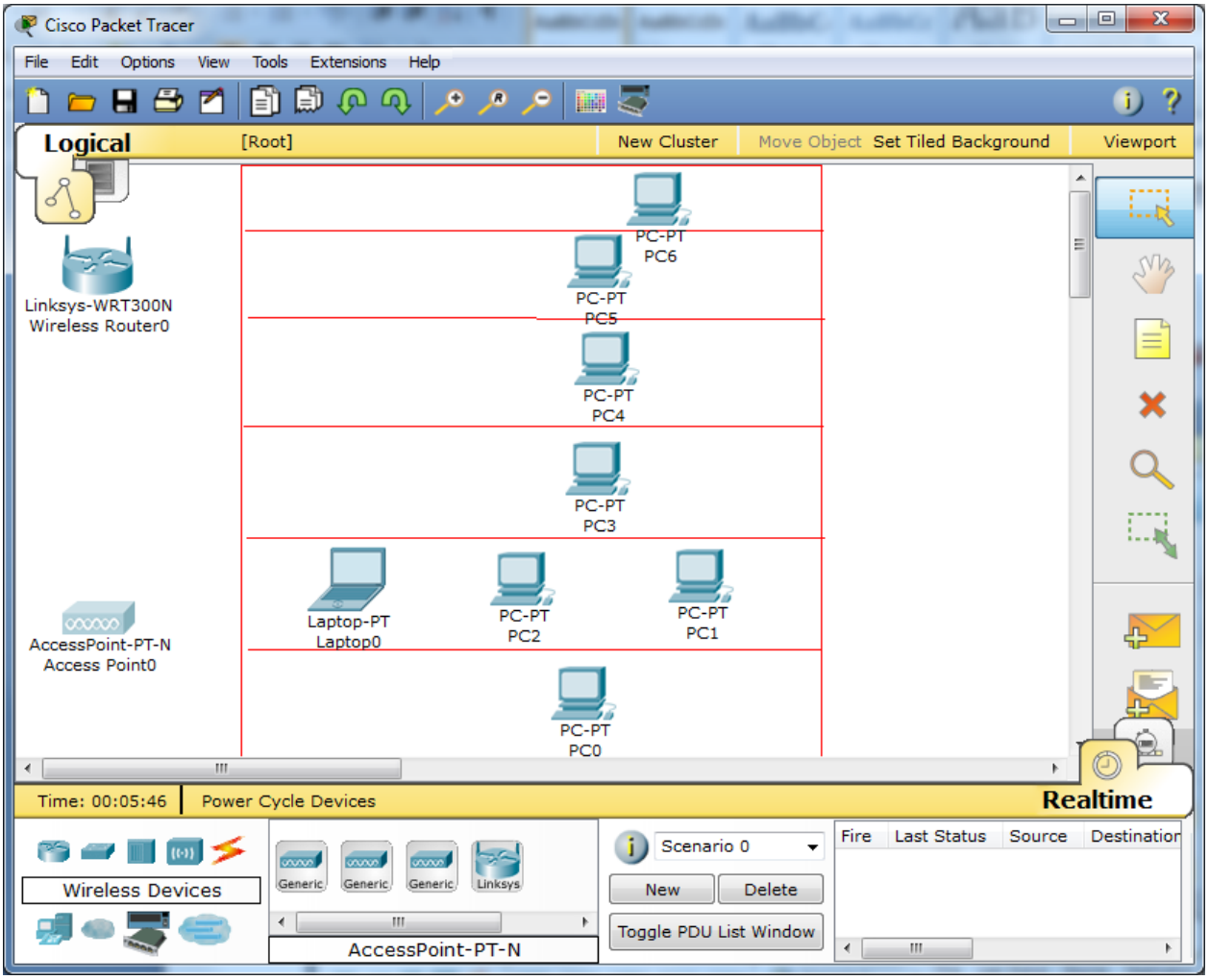
| | | | | | |
|---|---|---|---|---|---|
| | solución para recibir y enviar información de un terminal a los diferentes áreas de la clínica | Moreno 720 entre Eloy Alfaro y Sucre, de la ciudad de Babahoyo. | acción benéfica de la Fundación “Teolinda Troya Escobar” | gratuitas Cirugías gratuitas Interconsultas entre fundaciones | ✓ Ahorro en los pacientes<br>✓ Satisfacción en los miembros de la fundación |

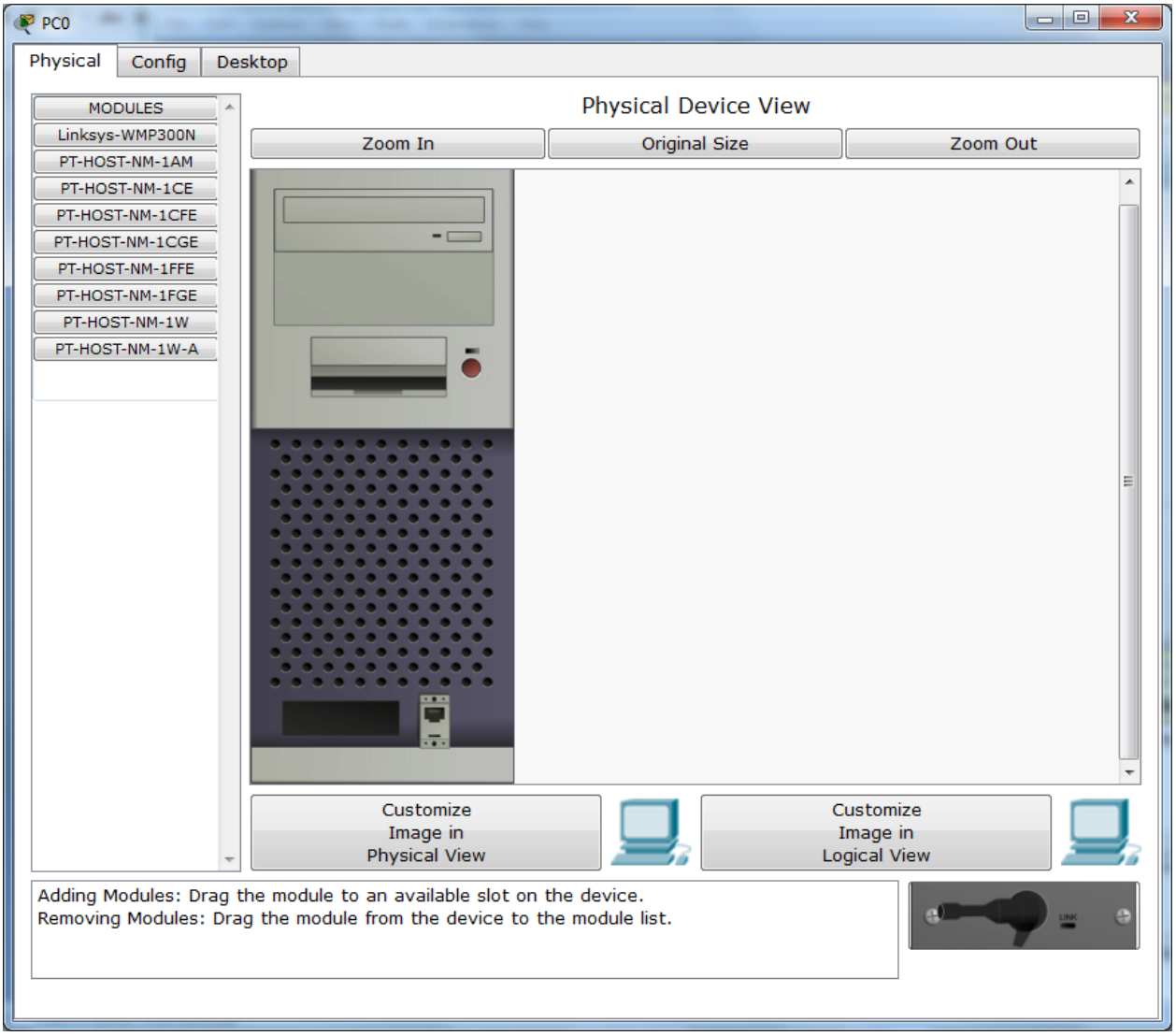
- ✓ **Edificio donde funciona la Clínica “Dr. Rafael Hernández Troya”**

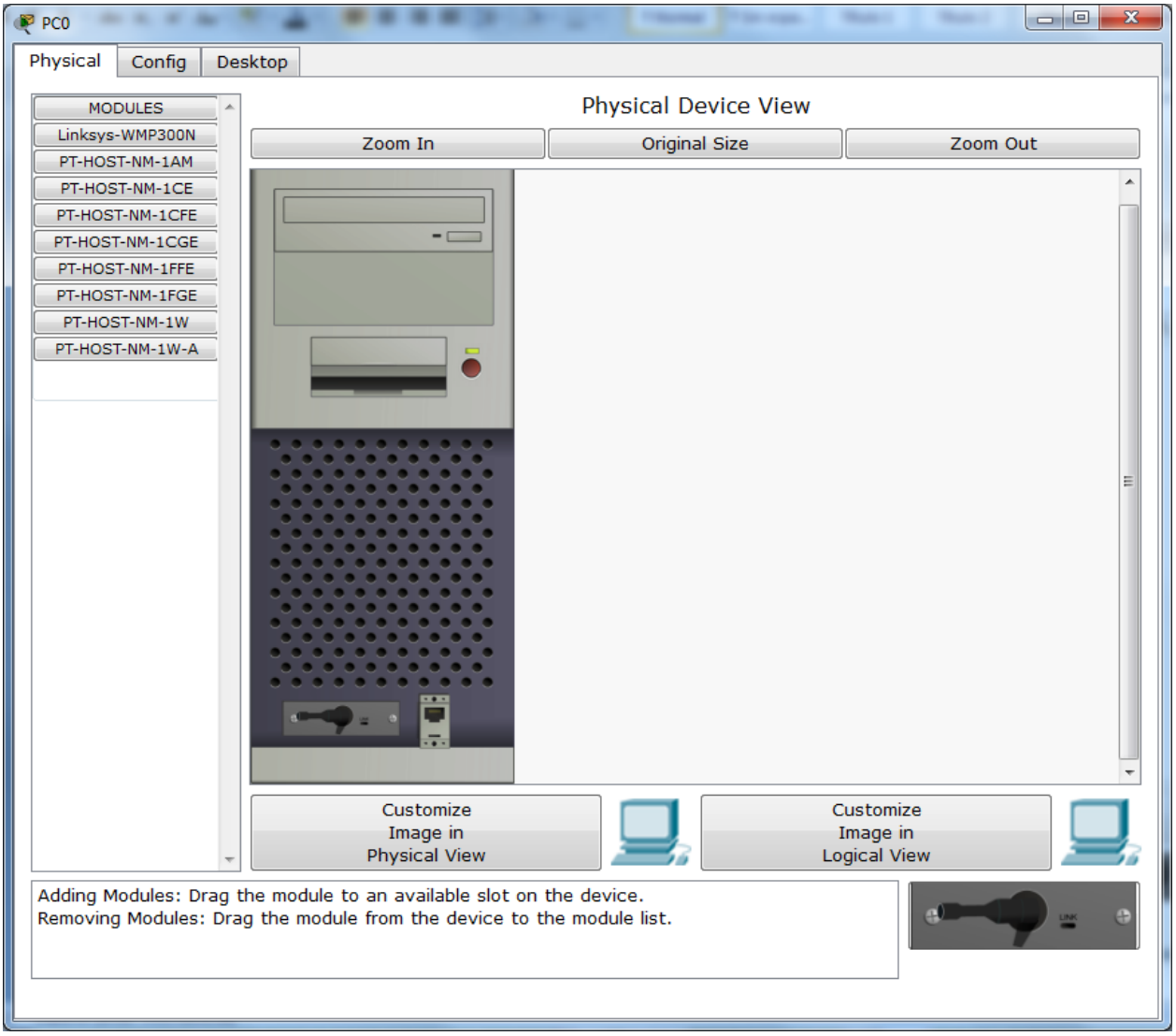
# SIMULACION DE LA RED

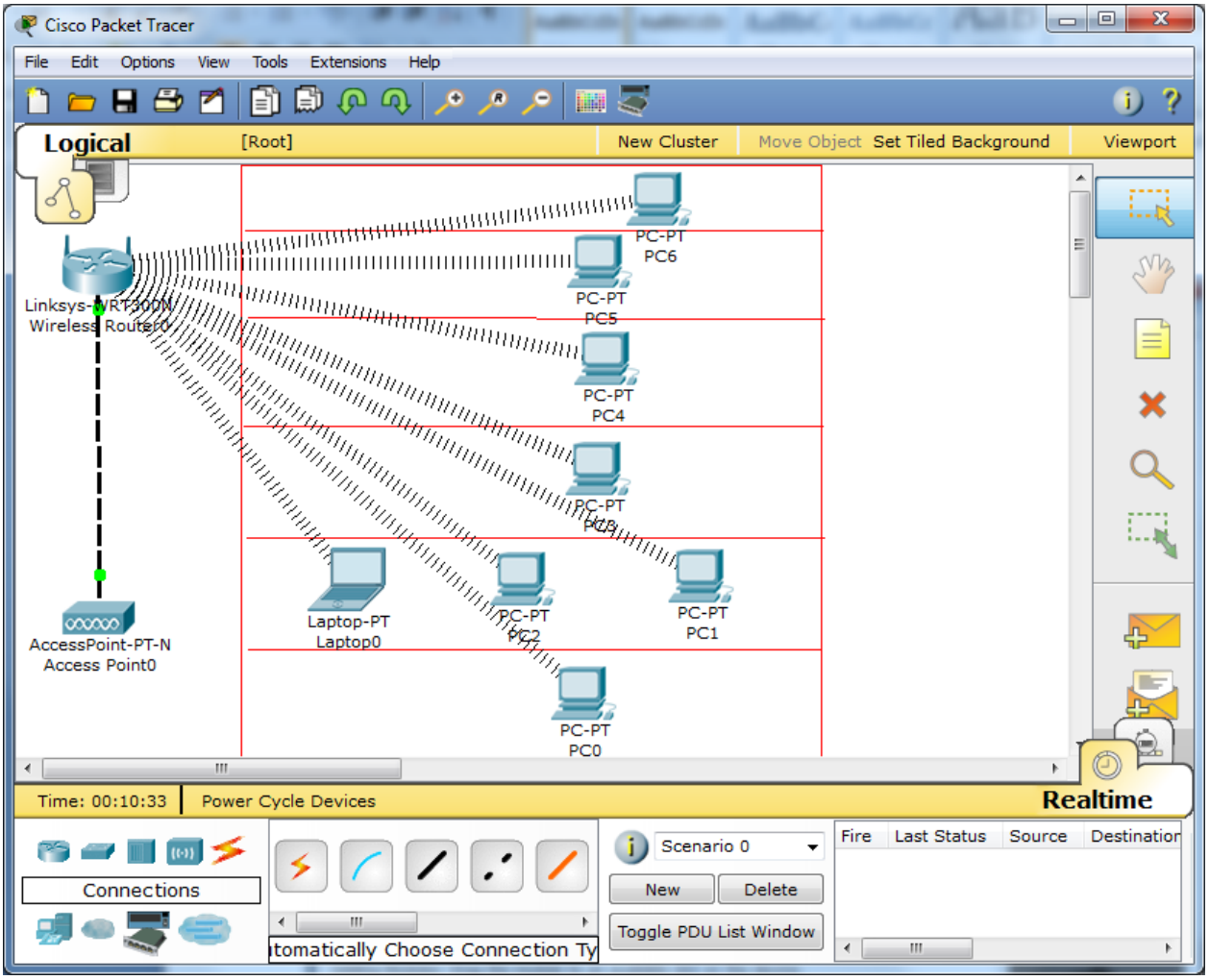



Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC-PT PC6
PC-PT PC5
PC-PT PC4
PC-PT PC3
Laptop-PT Laptop0
PC-PT PC2
PC-PT PC1
PC-PT PC0
Time: 00:04:49
Power Cycle Devices
Realtime
End Devices
Generic
Generic
Generic
Generic
IPPhone
PC-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Linksys-WRT300N
Wireless Router0
PC-PT
PC6
PC-PT
PC5
PC-PT
PC4
PC-PT
PC3
Laptop-PT
Laptop0
PC-PT
PC2
PC-PT
PC1
AccessPoint-PT-N
Access Point0
PC-PT
PC0
Time: 00:05:46
Power Cycle Devices
Realtime
Wireless Devices
Generic
Generic
Generic
Linksys
AccessPoint-PT-N
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination


PC0
Physical
Config
Desktop
MODULES
Linksys-WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Image in Physical View
Customize Image in Logical View
Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the device to the module list.


PC0
Physical
Config
Desktop
MODULES
Linksys-WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Image in Physical View
Customize Image in Logical View
Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the device to the module list.

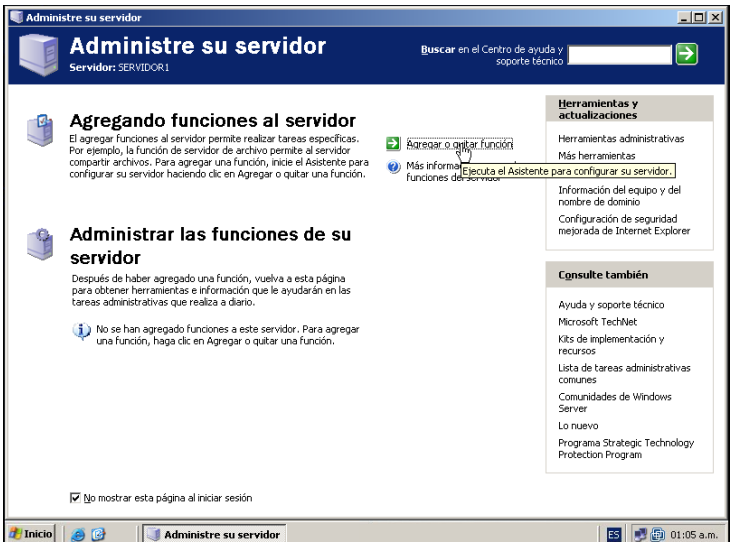

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Linksys-WRT300N
Wireless Router0
PC-PT
PC6
PC-PT
PC5
PC-PT
PC4
PC-PT
PC3
Laptop-PT
Laptop0
PC-PT
PC2
PC-PT
PC1
AccessPoint-PT-N
Access Point0
PC-PT
PC0
Time: 00:10:33
Power Cycle Devices
Realtime
Connections
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

# INSTALACIÓN Y CONFIGURACION DNS WINDOWS SERVER 2003

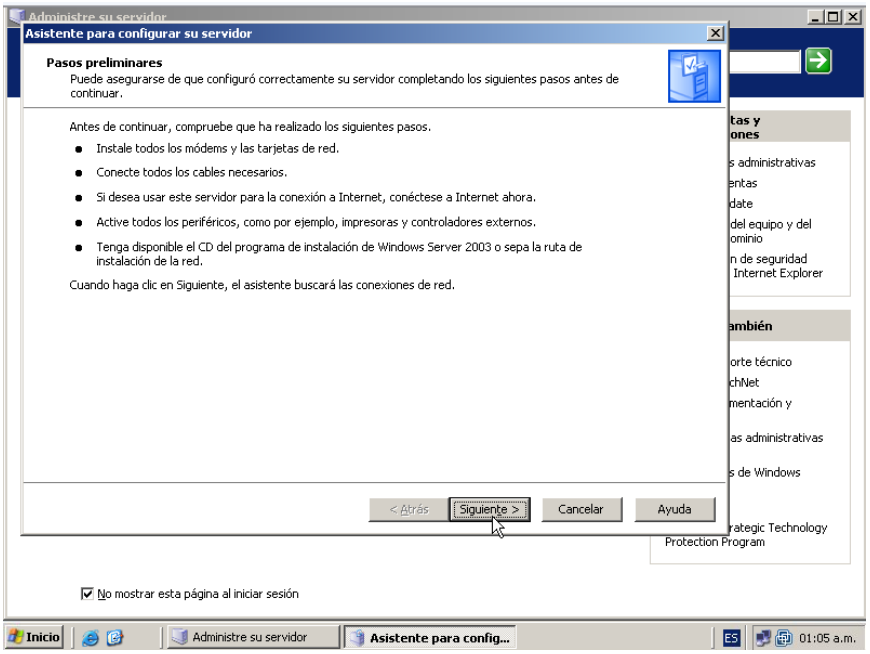
✓ <u>INSTALACION DNS</u>

Vamos a la opción administrar su servidor

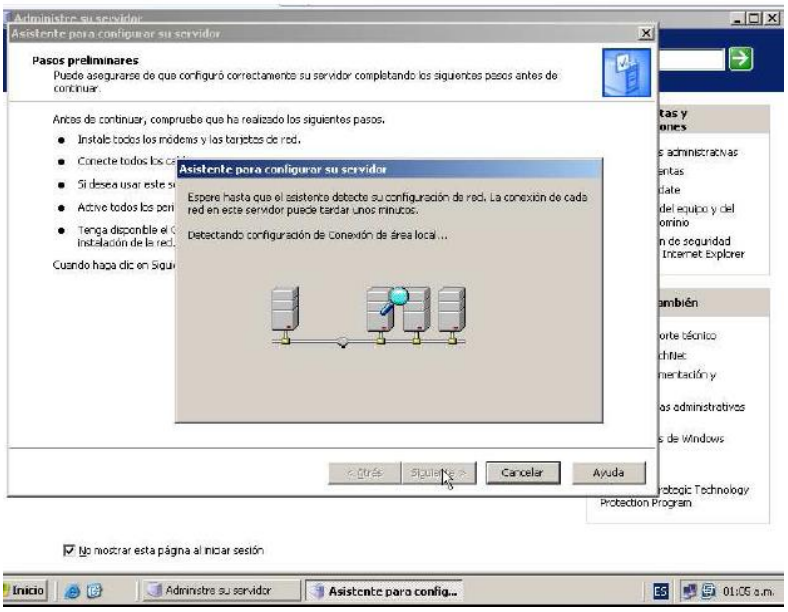

Hacemos click en la opción agregar o quitar función para agregar el servicio de resolución de nombres (dns).



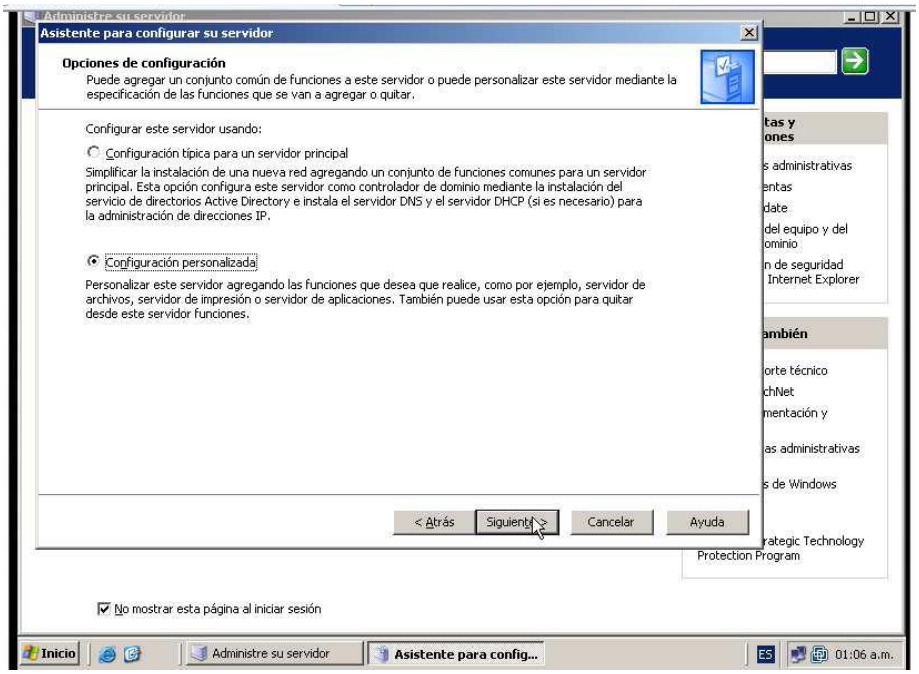

Esta opción ejecuta el asistente para la configuración del servidor. Hacemos click en siguiente



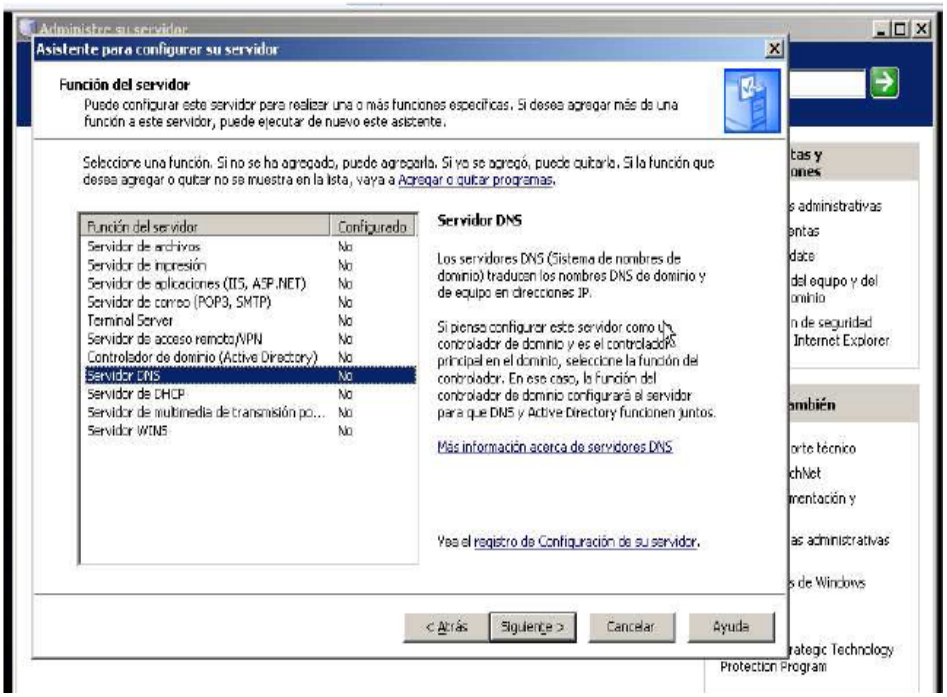

El asistente va a empezar a hacer una verificación de red y detectar como está la configuración de esta




Como este servidor esta recién creado vamos a opciones personalizadas para elegir los servicios que queremos agregar para realizar varias funciones específicas

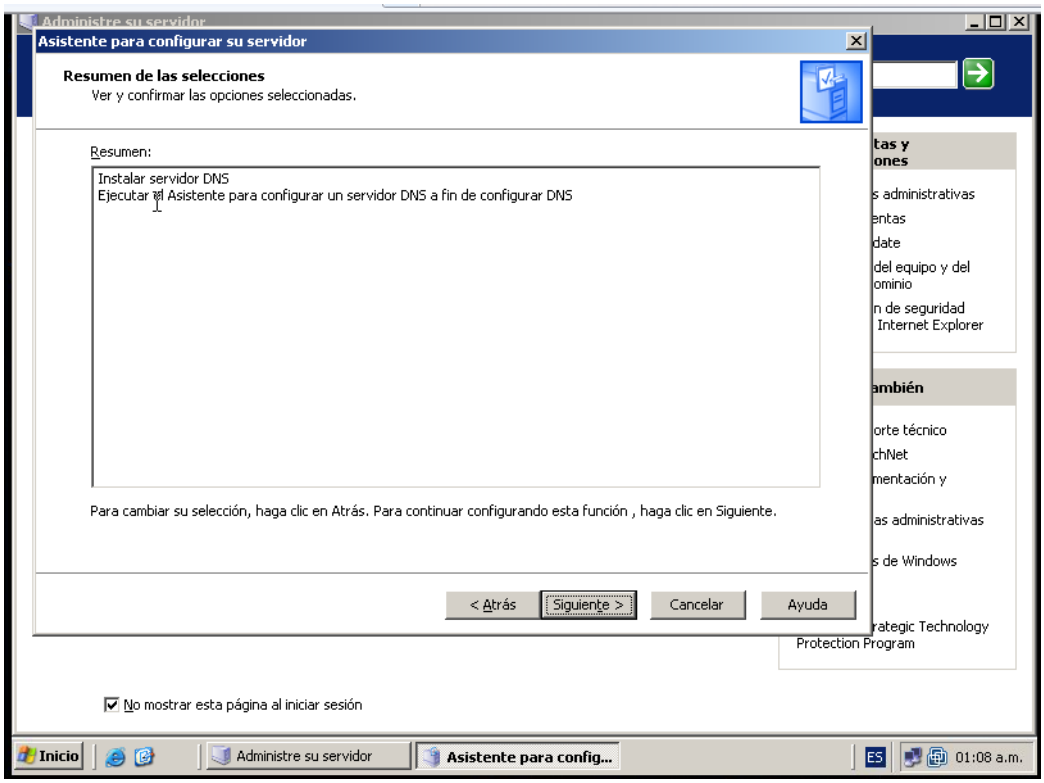



Aquí tenemos el listado de las funciones que queremos agregarle a nuestro servidor, en este caso el servicio que vamos a agregar va ser servicio dns, lo seleccionamos y le damos a siguiente. Este servicio nos traduce los nombres de dominios y de equipo en direcciones ip.

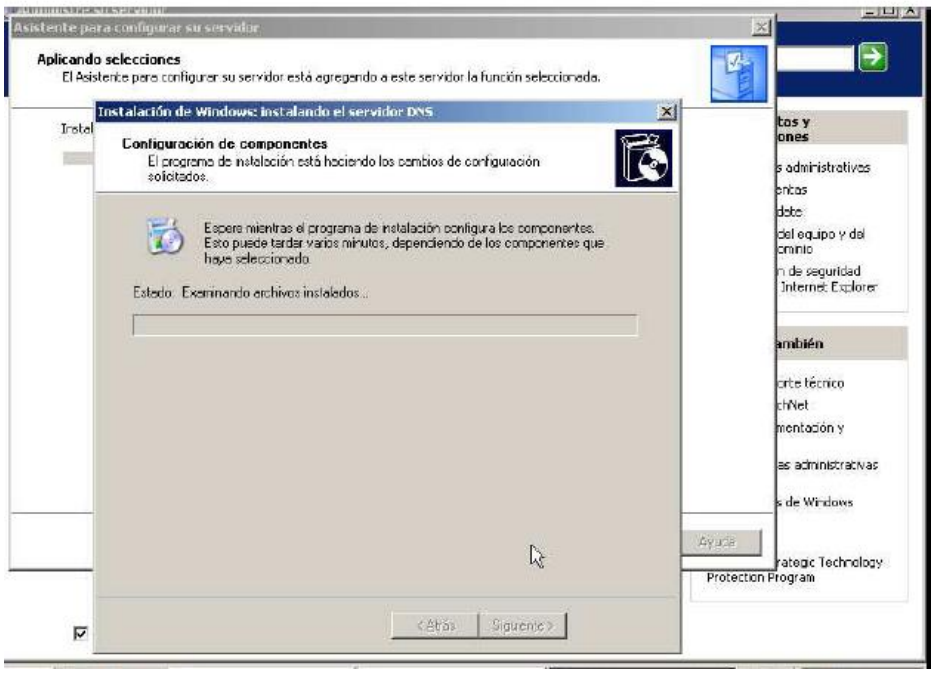



Aquí aparece un resumen de lo que se va a instalar

Hacemos click en siguiente para que comience la instalación del dns.

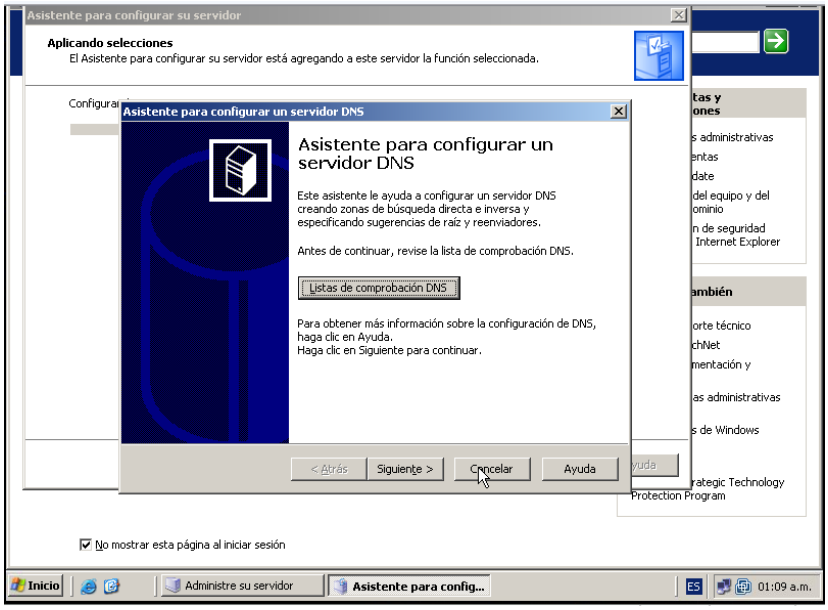



Ahora con el Cd de Windows server 2003 iniciamos la instalación de los servicios, se instalaran los archivos necesarios para la implementación de este servidor



Una vez finalizadas la instalación de las herramientas de administración

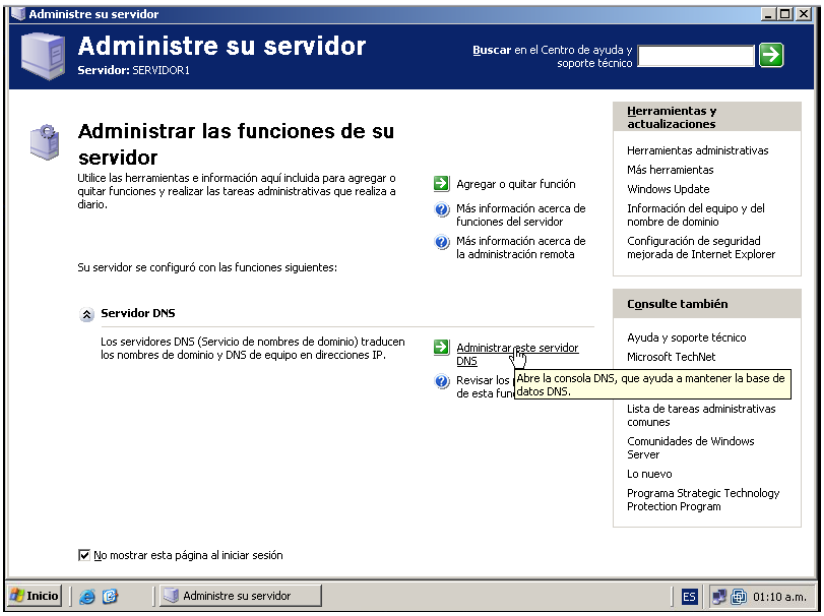
Tendremos el servidor de DNS instalado, lo que nos aparecerá ahora será un asistente para configurar el servidor DNS, hacemos click en cancelar para configurarlo manualmente



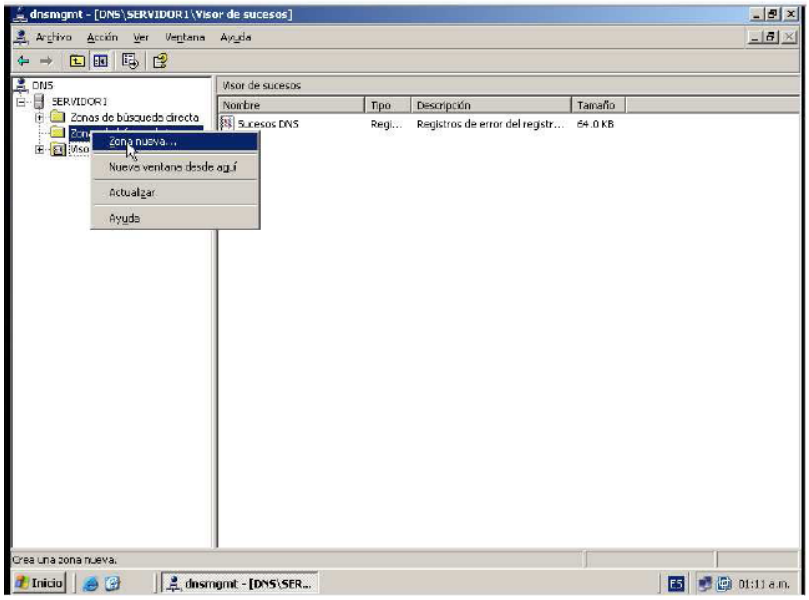

Aquí nos aparecerá una ventana indicando que la configuración del asistente no se pudo completar y le damos click en finalizar


Vamos a la opción administrar servidor y podremos ver que el servidor DNS está instalado.

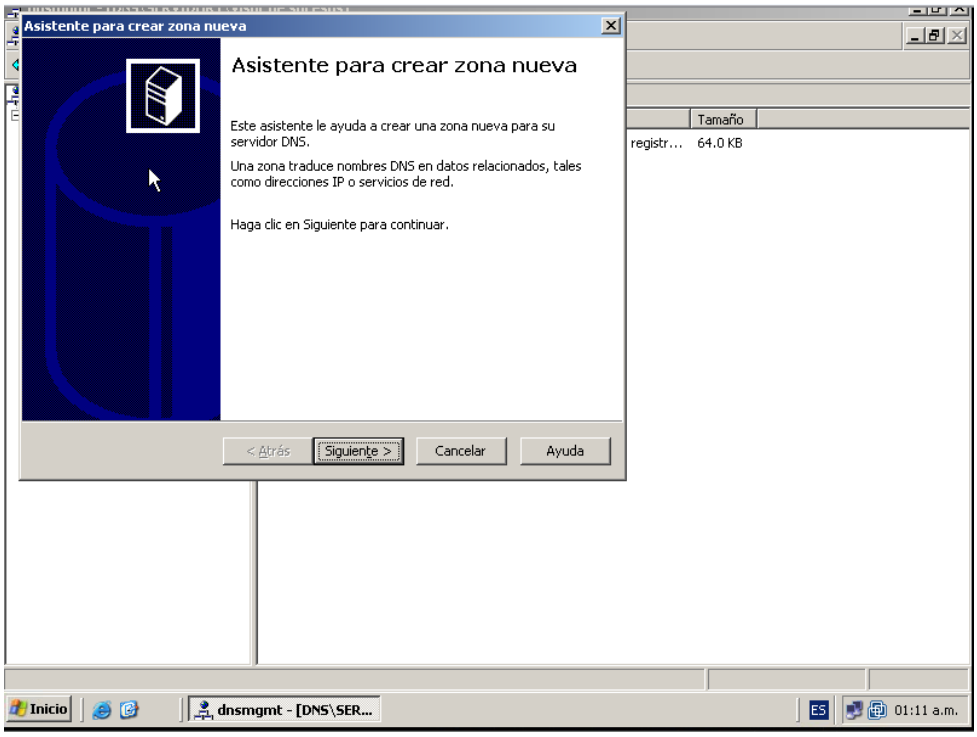
Hacemos click en administrar este servidor DNS




En nuestro servidor nos vamos a encontrar con dos tipos de zonas. Zonas de búsqueda directa y zona de búsqueda inversa. Lo primero que vamos a hacer va ser agregar la zona de búsqueda inversa, hacemos click con el botón secundario del mouse zona de búsqueda inversa y hacemos click en zona nueva.

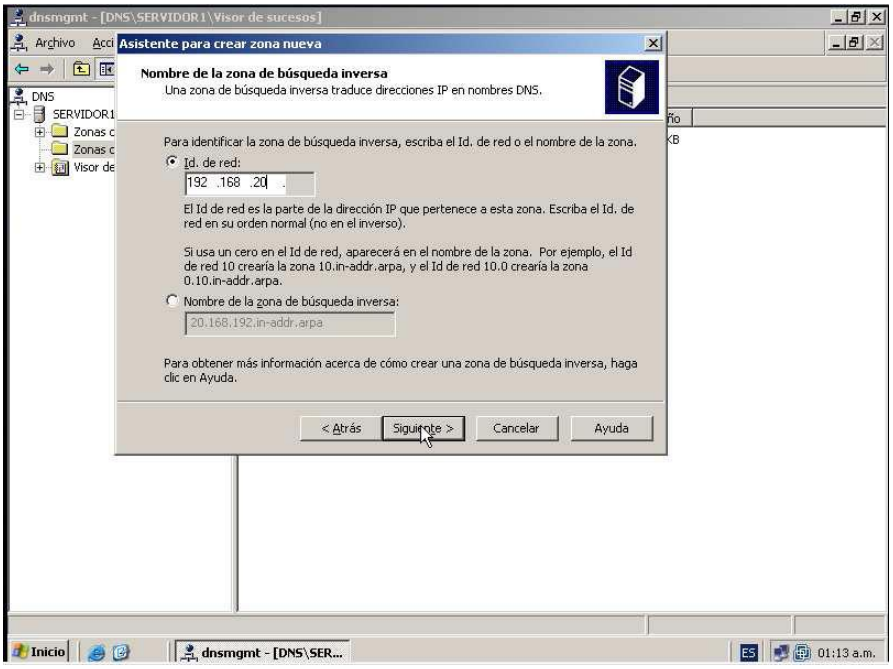



Nos aparecerá un asistente para crear una zona nueva, hacemos click en siguiente

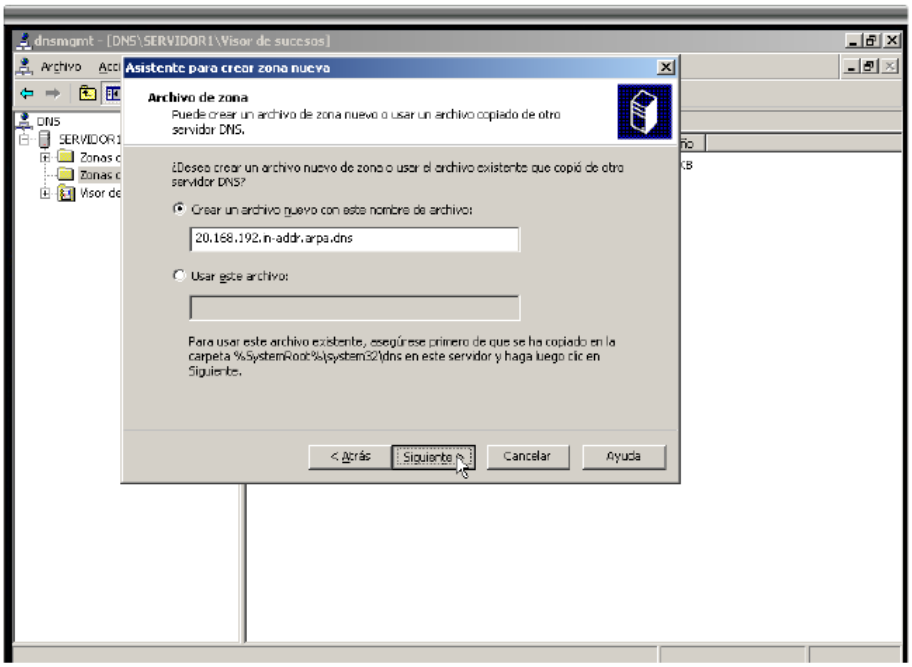



Aquí nos aparecerán tres tipos de zonas como es nuestro primer servidor seleccionamos zona principal y damos click a siguiente. Esta zona se actualiza directamente en este servidor

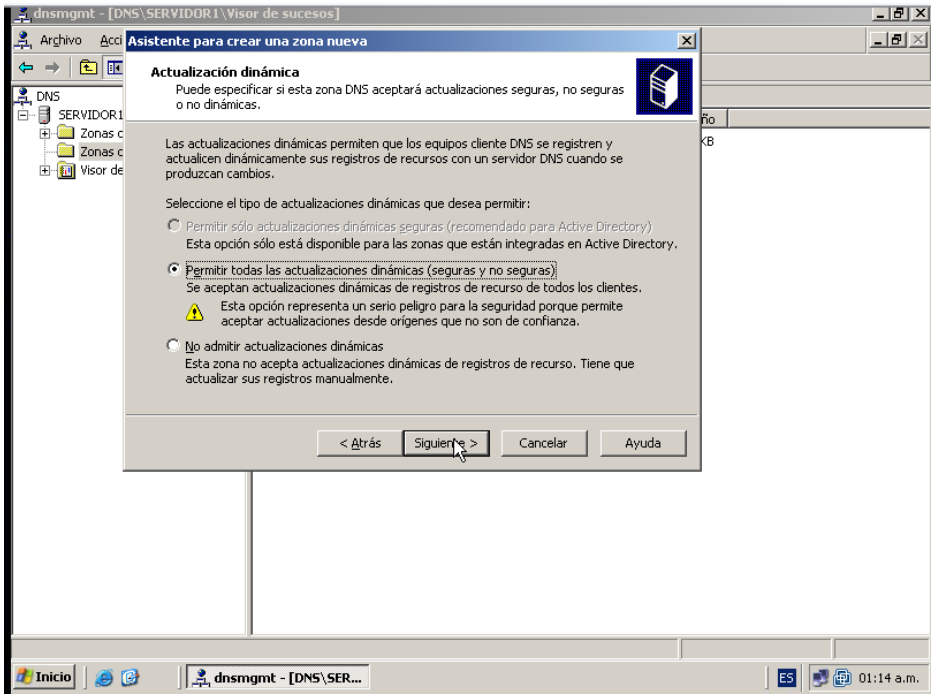

Aquí se nos va a preguntar cuál va a ser nuestra id de red o sea la ip a la que pertenece nuestra red, ingresamos la ip y seleccionamos siguiente



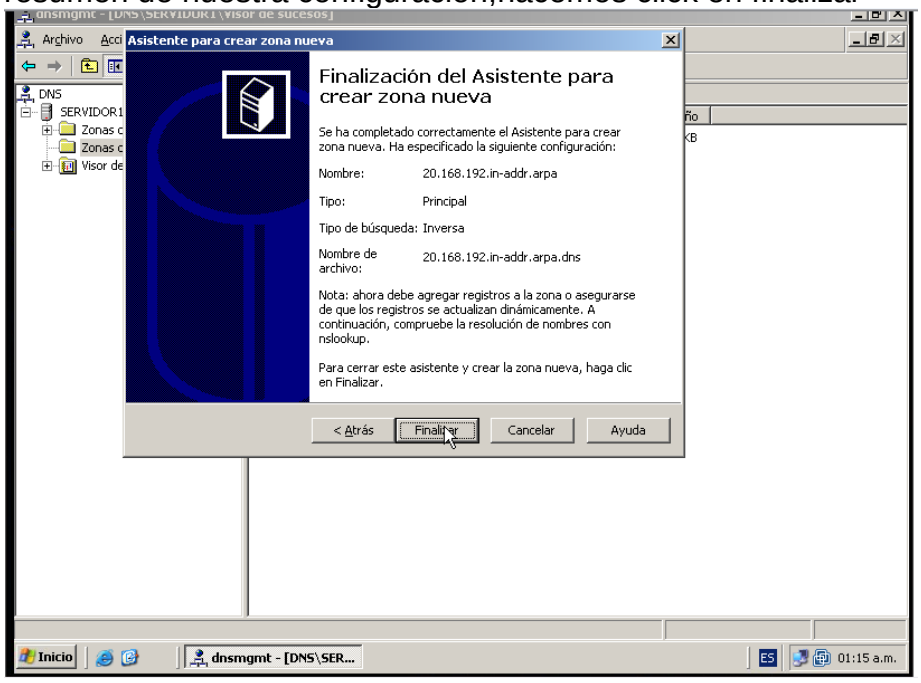

Esta información que ingresamos se va a guardar en un archivo de configuración de dns que tiene la dirección ip de forma invertida porque va a hacer la tarea de conversión a nombres,hacemos click en siguiente



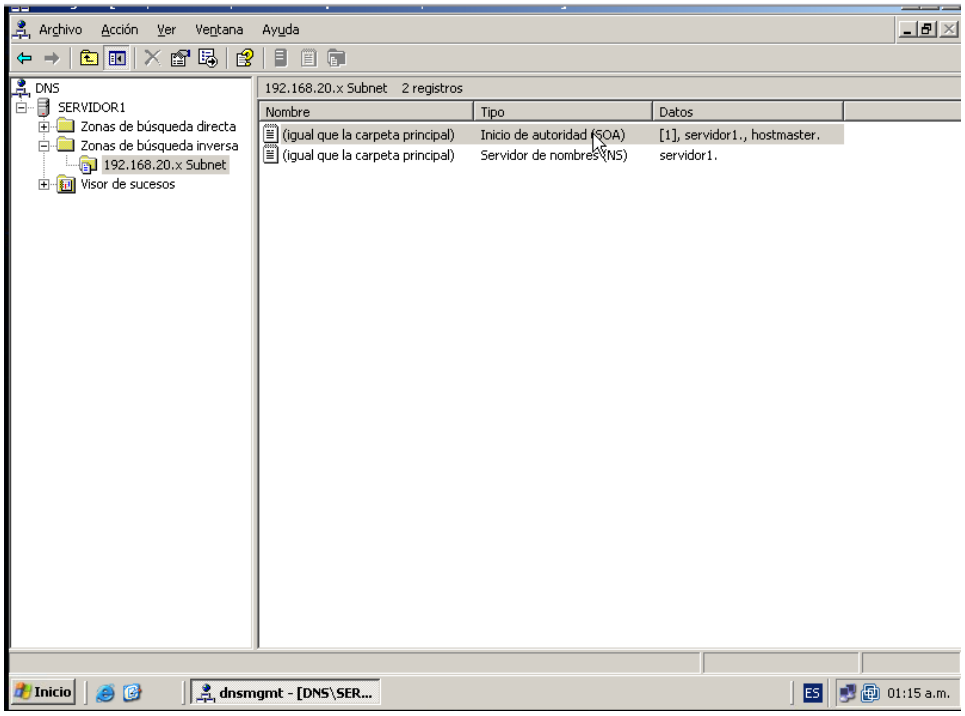

En las opciones de actualizaciones dinámicas hacemos click en permitir todas las actualizaciones dinámicas y hacemos click en siguiente. Esta opción nos permitirá aceptar actualizaciones dinámicas de registro de recursos de toda la red



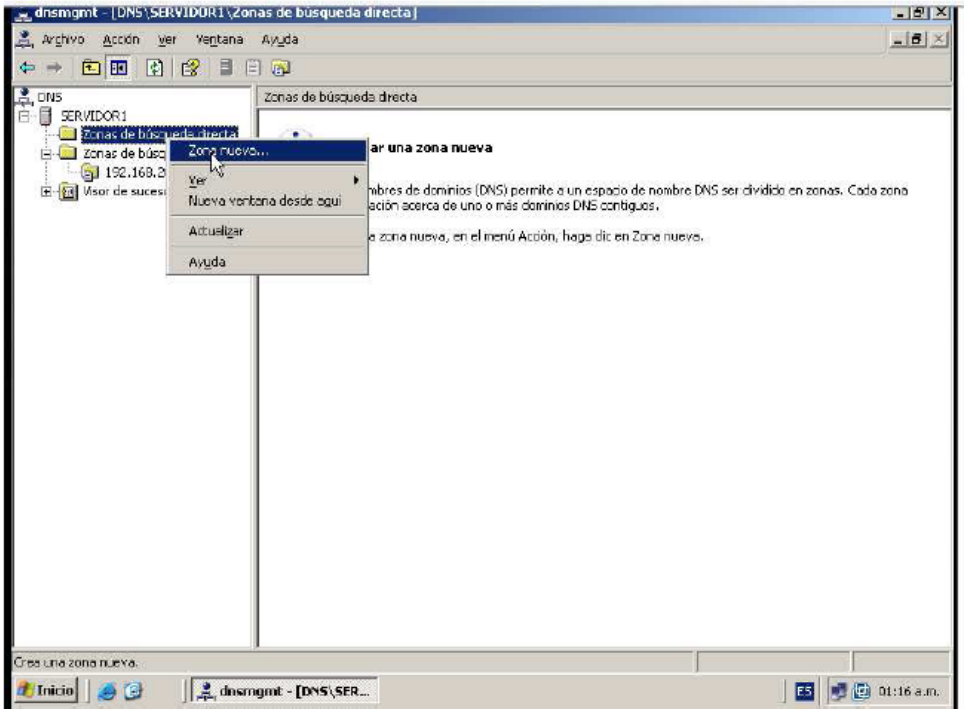

Finalización del asistente para crear nueva zona con un resumen de nuestra configuración,hacemos click en finalizar



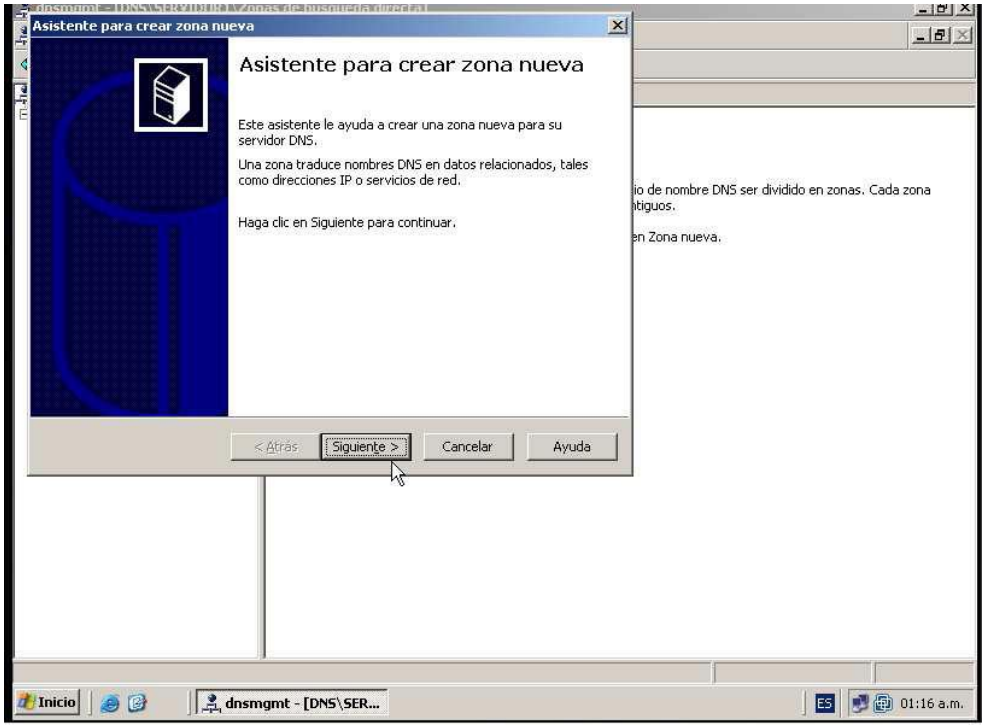

En la zona de búsqueda inversa ya tenemos la primera zona principal inversa que tiene los registros soa y el registro ns




Ahora vamos a crear la zona de búsqueda directa, hacemos click con el botón secundario del mouse en zona de búsqueda directa y seleccionamos la opción zona nueva



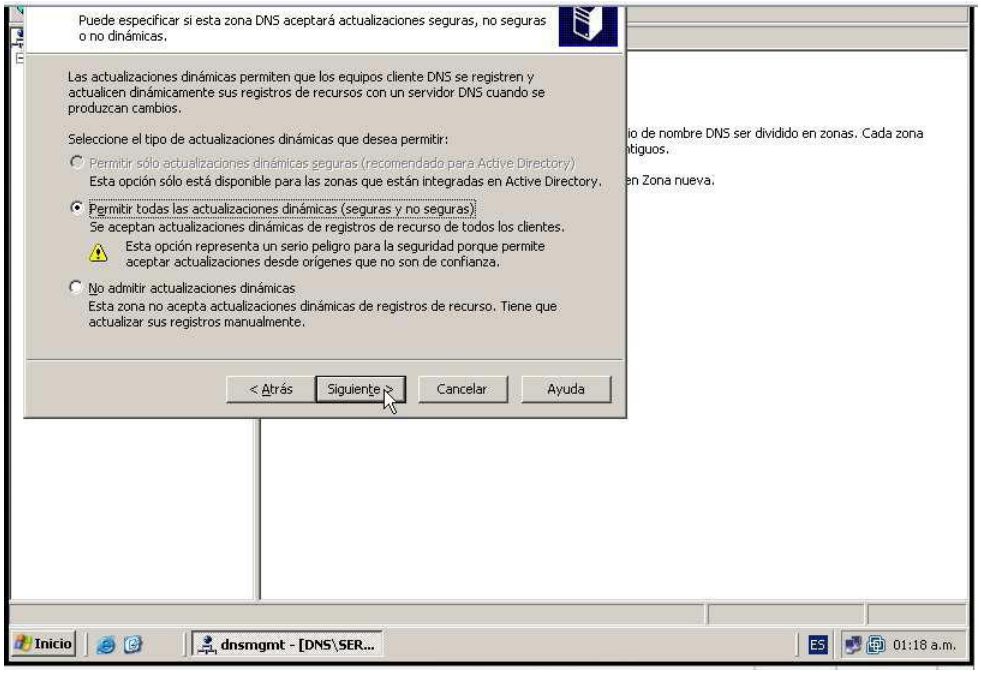
Nos aparece el asistente para crear la zona nueva, hacemos click en siguiente



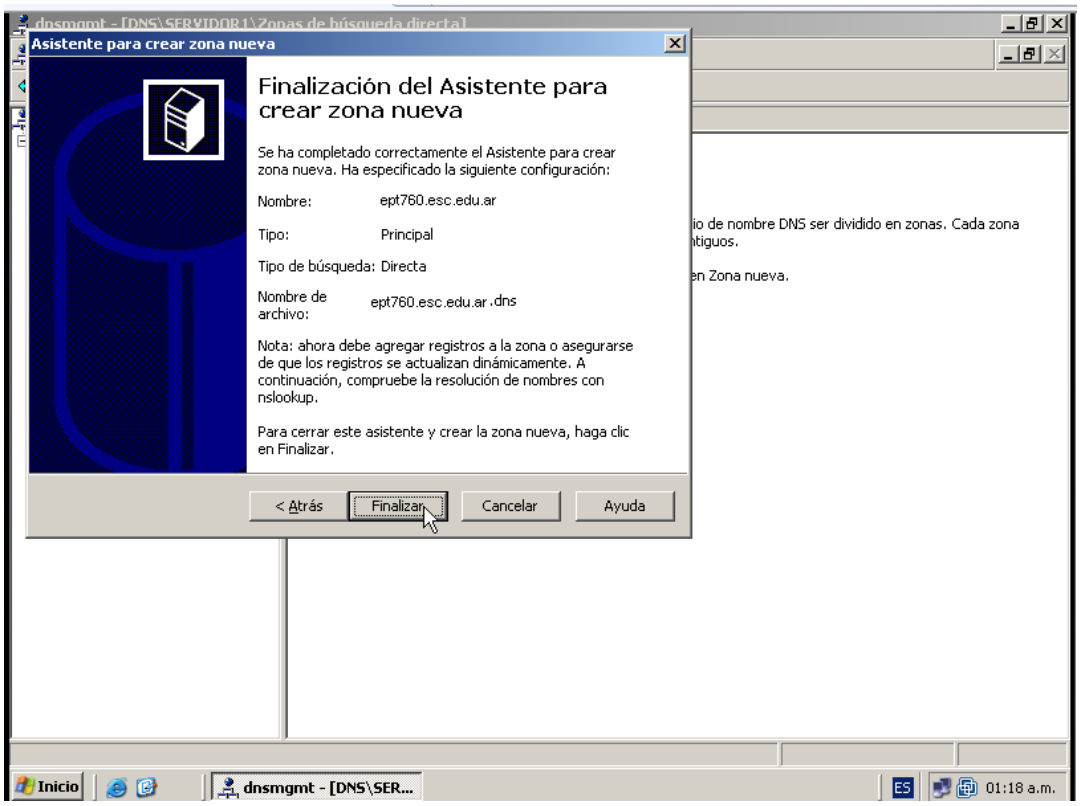

Nos aparecerán casi las mismas opciones anteriores, tenemos la tres zonas seleccionamos la zona principal y damos click a siguiente.

Aca es donde tenemos que definir el nombre del dominio que vamos a realizar, una vez escrito el nombre del dominio damos a siguiente

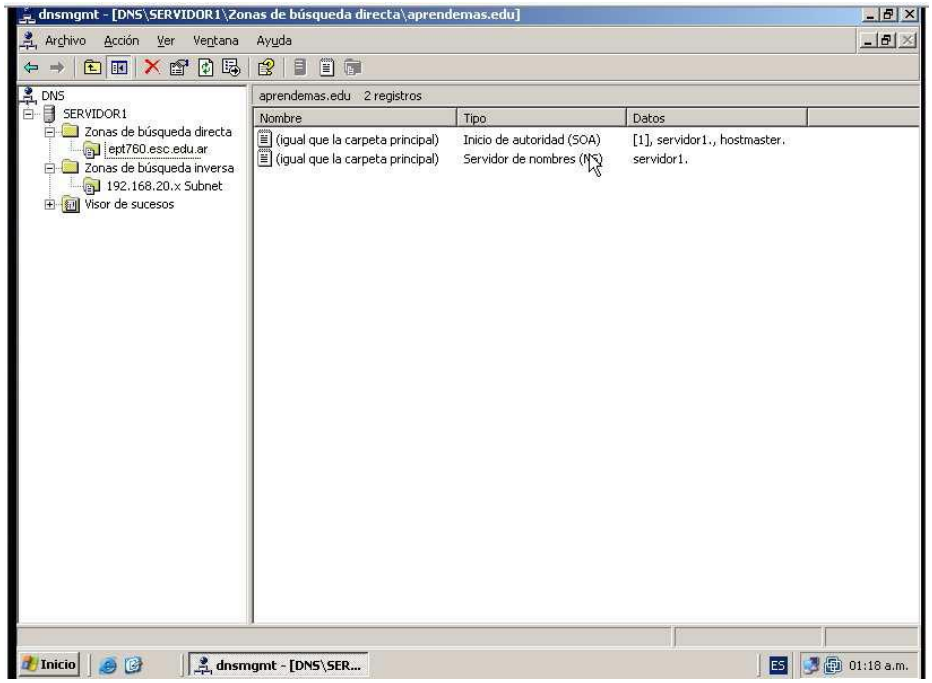

Ahora se creara un archivo que contendrá el nombre de dominio, hacemos click en siguiente sin modificar nada, y luego nos aparecerá la ventana de actualizaciones automáticas seleccionamos la opción permitir todas las actualizaciones automáticas y damos click a siguiente



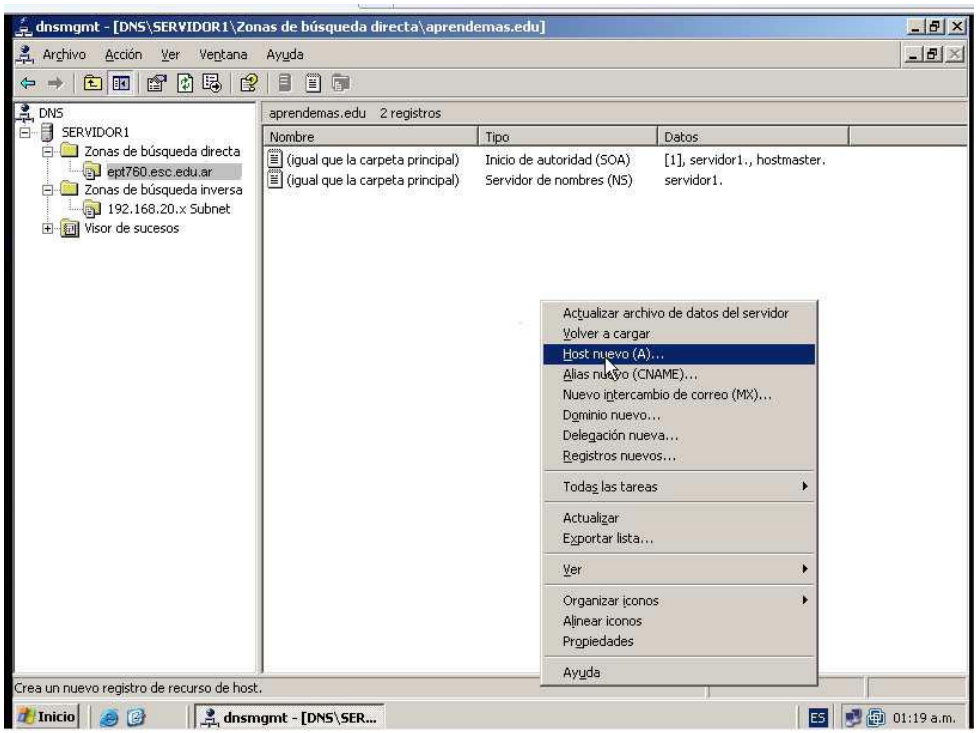
Finalizara el asistente para crear zona nueva con un resumen de nuestra configuración, damos click en finalizar.



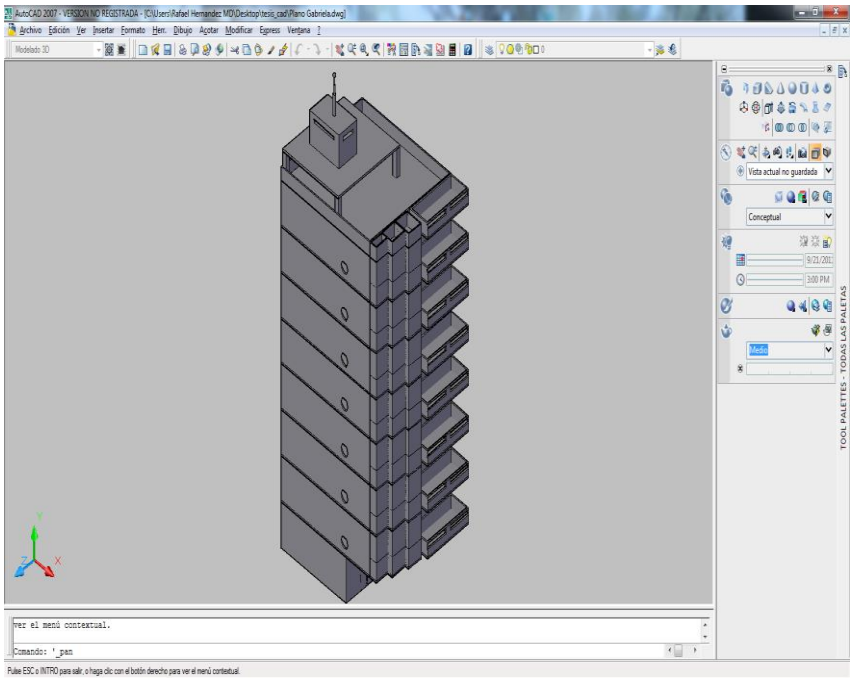

Aquí ya tenemos nuestra zona de búsqueda directa creada

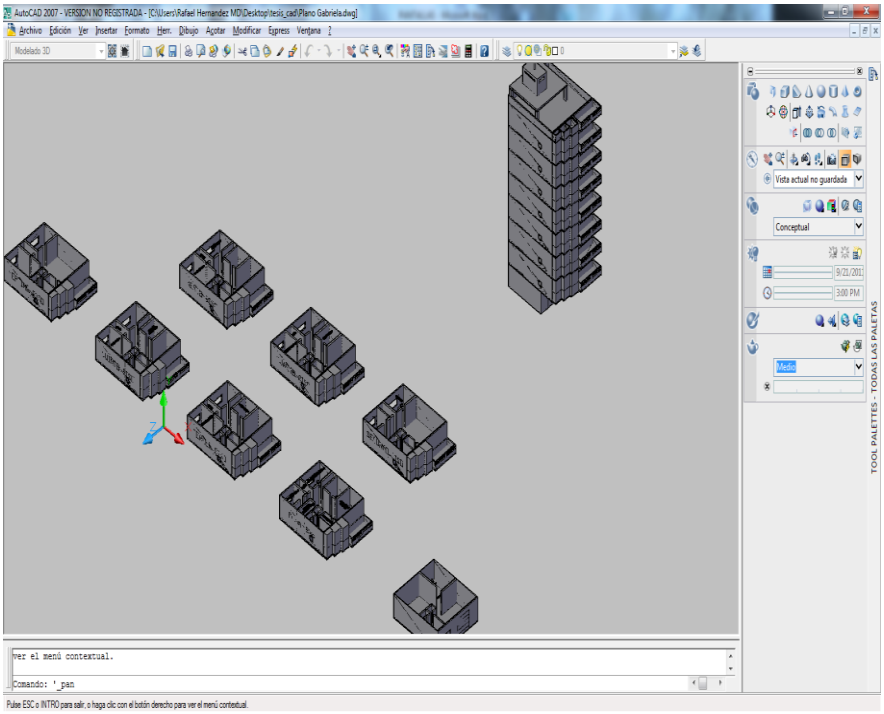


Para agregar un registro host en nuestra zona de búsqueda directa hacemos click con el botón secundario y seleccionamos la opción host nuevo




# ARQUITECTURA DEL EDIFICIO DONDE FUNCIONA LA CLINICA DR. RAFAEL HERNNADEZ TROYA




AutoCAD 2007 - VERSION NO REGISTRADA - [C:\Users\Rafael Hernandez MD\Desktop\tesis_cad\Plano Gabriela.dwg]
Archivo Edición Ver Insertar Formato Her. Dibujo Acotar Modificar Express Ventana ?
Modelado 3D
Vista actual no guardada
Conceptual
Medio
TOOL PALETTES - TODAS LAS PALETAS
ver el menú contextual.
Comando: '_pan
Pulse ESC o INTRO para salir, o haga clic con el botón derecho para ver el menú contextual.