# ESCUELA POLITÉCNICA NACIONAL

## ESCUELA DE INGENIERÍA

# IMPLEMENTACIÓN DE UN PROTOTIPO DE PRUEBA PARA LA AUTOMATIZACIÓN DEL MANEJO DE LA INFORMACIÓN DEL ESTADO CLÍNICO DE PACIENTES Y LA MEDICIÓN DE SIGNOS VITALES A TRAVÉS DE SENSORES, PARA LA CLÍNICA "DURÁN" DE LA CIUDAD DE AMBATO

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

KARINA ALEXANDRA GUERRÓN TACOAMÁN

JADIRA ALEXANDRA PROAÑO SALAZAR

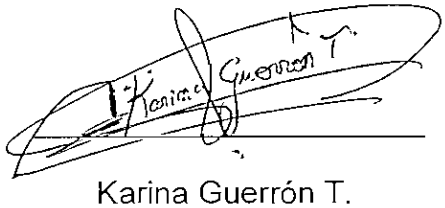
DIRECTOR: MSc. SORAYA SINCHE

Quito, Noviembre 2006

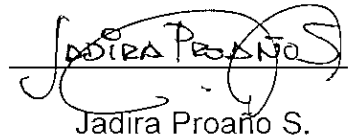
# DECLARACIÓN

Nosotras, Karina Alexandra Guerrón Tacoamán, y Jadira Alexandra Proaño Salazar, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Karina Guerrón T.



Jadira Proaño S.

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Karina Guerrón y Jadira Proaño, bajo mi supervisión.

Ing. Soraya Sinche' MSc.
DIRECTOR DEL PROYECTO

# AGRADECIMIENTOS

En primer lugar queremos dar gracias a Dios por la vida y a nuestros padres Franco y María Soledad e Isaac y Nancy, por ser un pilar fundamental para la realización de este trabajo.

Damos gracias a nuestra directora Ing Soraya Sinche MSC, por su constante apoyo y guía a lo largo del desarrollo de este proyecto, encaminando nuestra labor hacia una exitosa culminación.

Agradecemos a nuestros queridos profesores, que a lo largo de nuestra carrera nos compartieron sus conocimientos y valores, en especial a los ingenieros: Mayrita Valle, Xavier Armendáriz, Pablo Hidalgo, y Fernando Flores.

Brindamos un agradecimiento muy especial, a los profesionales en el campo médico, que nos orientaron adecuadamente en la selección y adquisición de los equipos clínicos utilizados en este trabajo, de manera particular a Maren Christenson de NONIN *Company*, Matt Welsh de *Harvard University*, al Dr. Carlos Almeida, a la Lcda. Elizabeth Guerrón, y al Dr. Franklin Salazar.

Queremos agradecer a nuestros amigos y compañeros, por habernos brindado toda su ayuda en la ejecución de este propósito, especialmente al Ing. Xavier Pazmiño, al Ing. Paúl Reyes, al Ing. Carlos Contreras, al Ing. Luis Garófalo, al Ing. Alvaro Cadena, al Ing. Jorge Insuasti, al Ing. William Albuja, al Ing. David Mejía, al Ing. Alexander Salazar, al Ing. Andrés Calle, a Iván, a Shirma Ortiz, a Jaime Ruales, a Alejandro Ayala, a Alexander Verdesoto, a Santiago Oñate, a Cristian Ulloa, y a Paúl Proaño.

Finalmente agradecemos a la Clínica Durán de la ciudad de Ambato, por darnos las facilidades necesarias para ejecutar este proyecto, de manera particular al Dr. Juan José Durán y esposa.

Kary y Jady

## DEDICATORIA

Dedico este trabajo a mi Divino Niño Jesús, por su presencia en mi corazón.

A mis padres por ser un ejemplo de vida, por guiar mi camino y por ser mis amigos. A mis hermanos, que son mis compañeros de vida y que son un apoyo constante.

A Ricardo, por llenar mi vida de alegría y enseñanzas. A Xavy por su cariño, comprensión, y ayuda constante.

A todos mis amigos, porque su sonrisa siempre me acompaña.

A Alejita, Fernando David, y Stefany Mishell, mis queridos sobrinos, y a mi abuelita Aura Elisa que me protege desde el cielo.

KaRy

## DEDICATORIA

A Dios, y a la Virgen Dolorosa por su protección y bendiciones a lo largo de mi vida y carrera universitaria.

A mis padres por darme todo su amor y compresión, y no permitir que decaiga ante las diversas dificultades que se me han presentado.

A mis hermanos Wellington y Paúl, y a mi tío Lenin por estar junto a mí siempre.

A mis verdaderos amigos por compartir conmigo todo este tiempo y enseñarme a ser mejor.

A Paúl por todo su amor, apoyo, y ayuda incondicional.

A mi papá Cesitar allá en el cielo.

Jady

# CONTENIDO

# RESUMEN

El presente proyecto busca mejorar el mecanismo de atención al paciente y la optimización de recursos y tiempo en lo que a personal se refiere, mediante la utilización de una red de datos y sensores, que permitan informar a tiempo, el estado clínico del paciente a los responsables de su cuidado, para la Clínica "Durán" de la ciudad de Ambato.

En el capítulo uno se realiza el estudio de los estándares IEEE 802.3 *Fast Ethernet*, *Gigabit Ethernet,* IEEE 802.11g, IEEE 802.15.4 ZigBee, e IEEE 802.15.1 *Bluetooth*.

En el capítulo dos, se determina el estado actual de funcionamiento de la red de la clínica, sus requerimientos y mecanismos de manejo de la información, para en base a ello realizar el diseño más adecuado.

Se realiza un análisis de equipos y elementos disponibles en el mercado, que satisfagan las exigencias de la clínica, y seleccionar los más adecuados.

Se diseña una red hibrida para toda la edificación de la clínica, describiendo mecanismos y políticas de seguridad a seguir.

En el capítulo tres se diseña e implanta una base de datos realizada en *MySQL* 5.0, que se interconecta con una aplicación de software elaborada en *Java Netbeans* 5.0, la cual permite administrar la información, tanto del personal médico como de pacientes. El software maneja los datos de medición de signos vitales obtenidos mediante los sensores.

En el capítulo 4 se implementa un prototipo de prueba, para el área de Consulta Externa, y se realizan las pruebas de campo pertinentes, con la finalidad de realizar los correctivos necesarios y garantizar un funcionamiento adecuado.

# PRESENTACIÓN

Los avances tecnológicos que se han venido dando en los últimos años, especialmente en el campo de las redes inalámbricas, han dado facilidad, flexibilidad y eficiencia en las operaciones cotidianas.

Con el pasar del tiempo se ha observado que las enfermedades que padece la población, han ido aumentando, llegando a necesitar de mayores cuidados y hasta de la presencia permanente de una enfermera por paciente. Las redes de sensores médicos inalámbricos, ayudarán al personal de cuidado médico a proporcionar servicios como: monitoreo constante, mejor manejo de los datos médicos, y atención efectiva en casos de emergencia.

Al mantener un monitoreo periódico del paciente, se evitarían complicaciones críticas, que podrían ser controladas a tiempo evitando problemas de mayor gravedad, ya que el personal médico estaría informado eficientemente del estado clínico del paciente. Este tipo de cuidado es esencial para bebés, ancianos y personas en estado crítico.

El manejo de la información a través del sistema, convierte a la clínica en una entidad cero papel, lo cual permite mantener un control adecuado y preciso del proceso de atención médica a los pacientes.

Es por este motivo que se presenta el siguiente proyecto, desarrollado con la finalidad de automatizar el manejo de la información del estado clínico de pacientes y la medición de signos vitales a través de sensores, para la Clínica "Durán" de la ciudad de Ambato, el cual servirá como referencia para mejorar el cuidado médico de un paciente en hospitales, clínicas y centros médicos.

# CAPÍTULO 1

# REDES LAN Y PAN

# 1. REDES LAN Y PAN

Para el campo de las telecomunicaciones, una red se define como un sistema en el que se conectan entre sí varios equipos independientes, para compartir datos y periféricos, como discos duros e impresoras. La capacidad de compartir información de forma eficiente es lo que le da a las redes de computadores su potencia y atractivo.

## 1.1 TIPOS DE REDES

El concepto de red incluye diferentes tipos y posibles configuraciones de las mismas, por lo que surge la necesidad de establecer clasificaciones que permitan identificar estructuras de red concretas, siendo las más comunes y aceptadas las que se describen a continuación.

### 1.1.1 CLASIFICACIÓN DE LAS REDES

#### 1.1.1.1 Desde el Punto de Vista de Cobertura[1]

##### *1.1.1.1.1 Redes PAN (Personal Area Network)*

Las redes de área personal son redes de ordenadores que ofrecen cobertura en el rango entre 1 y 10 metros, se utilizan en el hogar o en lugares separados entre si a cortas distancias.

##### *1.1.1.1.2 Redes LAN (Local Area Network)*

Las redes de área local son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología de transmisión de medio compartido.

Las velocidades de transmisión típicas de una LAN van de 10 a 100 Mbps. Dentro de este tipo de redes se han desarrollado un sinnúmero de estándares, entre los cuales se destacan IEEE 802 y *Ethernet*.

---

[1] TANENBAUM, Andrew; Redes de Computadoras; Tercera edición / HIDALDO, Pablo; Redes de Área Local; Octubre 2003.

*1.1.1.1.3 Redes MAN (Metropolitan Area Network)*

Las redes de área metropolitana son redes de ordenadores de tamaño superior a una LAN, abarcando el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en una misma área metropolitana, por lo que, en su tamaño máximo comprenden un área de 1 a 10 kilómetros.

*1.1.1.1.4 Redes WAN (Wide Area Network)*

Las redes de área extendida tienen un tamaño superior a una MAN, y consisten en una colección de computadores o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de enrutadores. Su tamaño puede oscilar entre 10 a 10.000 kilómetros.

*1.1.1.1.5 Redes Internet*

Una Internet es una red de redes, vinculadas mediante *gateways* o puentes. Un *gateway* es un equipo especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ir desde 10000 kilómetros en adelante, y su ejemplo más claro es el Internet, la red de redes mundial.

### 1.1.1.2 Redes Inalámbricas[2]

Las redes inalámbricas emplean como medio de transmisión al aire, están basadas en el intercambio de datos mediante ondas de radio, microondas, satélites e infrarrojos. Para el presente proyecto se considera únicamente el estudio de las redes WLAN (*Wireless* LAN), y WPAN (*Wireless* PAN), tal como se describe a continuación.

Los componentes básicos de una red inalámbrica son, la estación de trabajo equipada con tarjeta de red inalámbrica y el Punto de Acceso (AP *Access Point)* que actúa como dispositivo de interconectividad entre computadores. Además un *Bridge* o Puente que permite interconectar varios AP.

[2] SINCHE, Soraya; Redes de Área Local Inalámbricas

La creación de la tecnología inalámbrica permite introducir el concepto de portabilidad en las redes de datos, brindando gran flexibilidad además de garantizar cobertura en sitios inaccesibles, y acceder a la instalación de una red de manera rápida, lo cual justifica plenamente su gran aceptación.

A continuación se detallan los diversos estándares para las redes inalámbricas WLAN y WPAN más utilizados actualmente.

*1.1.1.2.1 IEEE 802.11*

IEEE[3] 802.11 en un inicio fue creado para trabajar en la banda de 2.4 GHz y con velocidades de transmisión de 1 y 2 Mbps. Especificando además tres tipos de capas físicas: Infrarrojo Difuso (DFIR *Diffuse Infrared*), Espectro Ensanchado con Salto de Frecuencia (FHSS *Frequency Hopping Spread Spectrum*) y Espectro Ensanchado con Secuencia Directa (DSSS *Direct Sequence Spread Spectrum*).

Actualmente, las bandas de frecuencia en las que opera IEEE 802.11 son: 900 MHz, 2.4 GHz y 5.8 GHz, conocidas como las bandas ISM (*Industry Scientific Medic*), en las que se permite la operación sin licencia para dispositivos que utilizan hasta 1 Watt de potencia.

En el avance del desarrollo del estándar, se presentaron problemas de interoperabilidad entre las tecnologías de modulación de espectro ensanchado FHSS y DSSS propuestas por los fabricantes, lo cual dio lugar a la creación de suplementos para el estándar inicialmente propuesto.

La IEEE 802.11b, define sistemas DSSS que operan a 1, 2, 5.5 y 11 Mbps en la banda de 2.4 GHz totalmente compatibles con IEEE 802.11.

El suplemento IEEE 802.11a, opera en la banda de 5.8 GHz, utiliza modulación OFDM, y es capaz de alcanzar velocidades de hasta 54 Mbps, pero incompatible con IEEE 802.11b.

---

[3] Instituto de Ingenieros Eléctricos y Electrónicos

La IEEE 802.11g, proporciona las mismas velocidades que 802.11a pero trabaja en la banda de 2.4 GHz, lo cual la hace compatible con IEEE 802.11b; el incremento de velocidad que ofrece este estándar se debe a que se emplea la técnica de Multiplexación por División de Frecuencia Ortogonal (OFDM *Orthogonal Frequency Division Multiplexing*).

#### *1.1.1.2.2 HIPERLAN*

*High Performance Radio LAN*, es un estándar europeo que plantea dos versiones:

- **HiperLAN/1**: define parámetros para compartir el acceso a WLANs entre dispositivos de usuario, mediante un protocolo no orientado a conexión. Opera en la banda de 5 GHz con velocidades de hasta 24 Mbps. Soporta calidad de servicio para datos, vídeo, voz e imágenes. Utiliza como esquema de modulación GMSK[4].
- **HiperLAN/2**: opera en la banda de 5 GHz, provee velocidades de hasta 54 Mbps, emplea un protocolo orientado a conexión y soporta calidad de servicio para transporte de tramas *Ethernet*, celdas ATM y paquetes IP. Emplea OFDM como técnica de modulación y es compatible con IEEE 802.11a.

#### *1.1.1.2.3 HOMERF SWAP*

Es una especificación industrial abierta que emplea el Protocolo de Acceso Inalámbrico Compartido (SWAP *Shared Wireless Access Protocol*).

Es ideal para comunicaciones inalámbricas digitales entre PCs y dispositivos electrónicos al interior del hogar. Opera en la banda de 2.4 GHz, con velocidades de 1 y 2 Mbps mediante FHSS. Soporta transporte de voz y datos.

#### *1.1.1.2.4 BLUETOOTH*

Es un estándar para redes PAN inalámbricas. Su estandarización corresponde a IEEE 802.15.1. Opera en la banda de 2.4 GHz, con velocidades menores a 1

[4] *Gaussian Modulation Shift Keying*

Mbps empleando FHSS. Éste es un estándar apropiado para trabajar con dispositivos de baja potencia y a cortas distancias.

*1.1.1.2.5 ZIG BEE*

Es un estándar, que ha permitido la creación de productos de monitorización y control inalámbricos, de bajo costo y consumo, que puedan conectarse en red, basados en un estándar abierto y global.

A este estándar se lo conoce como LR-WPAN (baja velocidad, *Low Rate Wireless Personal Area Network*), está representado mediante IEEE 802.15.4, con velocidades de hasta 250 Kbps y distancias de hasta 20 metros.

*1.1.1.2.6 WIMAX*

Este estándar se formó para facilitar el despliegue de redes inalámbricas de banda ancha basadas en el estándar IEEE 802.16, ayudando a asegurar la compatibilidad e interoperabilidad de equipos de acceso inalámbrico de banda ancha.

En un inicio fue definido para trabajar en la banda 10 a 66 GHz, pero en su suplemento IEEE 802.16a, se cambia por el rango de 2 a 11 GHz, a velocidades de hasta 75 Mbps, cubriendo áreas de hasta 48 Kilómetros.

*1.1.1.2.7 MBOA (ULTRAWIDE BAND)*

La alianza MBOA *(Multiband OFDM Forum)* permite definir una especificación de *Ultra WideBand* (UWB) basada en OFDM, que incorpora esta especificación al estándar emergente IEEE 802.15.3a.

Trabaja en la banda de frecuencias de 3.1 GHz hasta 10.6 GHz, con velocidades de 110 a 480 Mbps y alcances menores a 10 m.

La tecnología UWB se emplea para la conectividad inalámbrica de una gran variedad de dispositivos, incluyendo envío local de vídeo y sincronización rápida de dispositivos móviles y ordenadores personales.

### 1.1.2 CLASIFICACIÓN DE LAS REDES SEGÚN LA TECNOLOGÍA DE TRANSMISIÓN

#### 1.1.2.1 Redes de Difusión

Son redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red.

#### 1.1.2.2 Redes Punto a Punto

Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra, a veces es necesario que éstos pasen por máquinas intermedias, siendo obligatorio en tales casos, un trazado de rutas mediante dispositivos ruteadores.

## 1.2 FUNDAMENTOS BÁSICOS DE LAS REDES *FAST ETHERNET* Y *GIGABIT ETHERNET*

### 1.2.1 REDES *FAST ETHERNET*

*Fast Ethernet* o *Ethernet* a alta velocidad es un conjunto de especificaciones desarrolladas por el comité IEEE 802.3, para proporcionar una red a 100 Mbps compatible con *Ethernet* y a un bajo costo en el mercado, permitiendo así el trabajo de aplicaciones complejas, como bases de datos, o aplicaciones cliente-servidor que requieren un mayor ancho de banda.

#### 1.2.1.1 Características

*Fast Ethernet* tiene las siguientes características:

- Incrementa la velocidad de la señal en un factor de 10, respecto de Ethernet.
- El tamaño mínimo de trama se mantiene en 512 *bit-times* de *Ethernet*, el retardo en este caso es de 5.12 µseg. y el alcance (longitud total de la red) se divide para diez.

- Está definida por la especificación IEEE 802.3u que está basada enteramente en el estándar IEEE 802.3, utilizando CSMA/CD[5] como método de acceso al medio, tipo de trama, y detección de errores.

#### 1.2.1.2 Especificaciones de *Fast Ethernet*

La norma 100BASE-T[6] comprende: la subcapa de Control de Acceso al Medio (MAC *Medium Access Control*), la subcapa de Control de Enlace Lógico (LLC *Logical Link Control*), y las tres capas físicas 100BASE-TX, 100BASE-FX, y 100BASE-T4.

##### *1.2.1.2.1 La Subcapa MAC (Control de Acceso al Medio)*

La subcapa MAC está basada en el Protocolo CSMA/CD. Los datos entre *Ethernet* y *Fast Ethernet* pueden moverse sin necesidad de protocolos de traducción debido a que la subcapa MAC y el control de errores son idénticos entre 10BASE-T y 100BASE-T.

##### *1.2.1.2.2 Subcapa LLC (Control Lógico del Enlace)*

LLC define una interfaz estándar entre la subcapa MAC y cualquiera de las tres capas físicas 100BASE-TX, 100BASE-T4, y 100BASE-FX.

Además ayuda a la subcapa MAC a la transferencia de bits a través de los distintos tipos de medios cableados, haciéndolos transparentes a la subcapa MAC.

##### *1.2.1.2.3 La Capa Física*

La capa física se encarga del transporte de los datos de entrada y salida del dispositivo conectado, realizando la codificación y la decodificación de datos, escucha de portadora, detección de colisiones, la interfaz eléctrica y mecánica con el medio conectado. *Fast Ethernet* funciona con los mismos medios físicos que 10BASE-T tales como: par trenzado sin apantallar (UTP), par trenzado

---

[5] Acceso Múltiple con Detección de Portadora / Detección de Colisión
[6] HIDALGO Pablo, Redes de Área Local.

apantallado (STP) y fibra óptica. La especificación *de Fast Ethernet* define 3 tipos de capas físicas:

- **100BASE-TX**

  Hace uso de dos pares del cable UTP de Categoría 5 o superior, o dos pares del STP IBM tipo 1. Esta capa trabaja con señales *Full-Duplex* de FDDI (ANSI X3T9.5) y utiliza un esquema de señalización MLT-3.

- **100BASE-T4**

  Utiliza los cuatro pares del cable UTP categoría 3 o superior y opcionalmente se permite el uso de cable UTP categoría 5. El método de señalización utilizado por esta capa es 8B6T.

- **100BASE-FX**

  Trabaja con dos segmentos de fibra 62.5 µm, uno de ellos es utilizado para la transmisión y el otro para la detección de colisiones y para la recepción (basada en FDDI). Utiliza la técnica de codificación 4B/5B-NRZI.

| CARACTERÍSTICA | 100BASE-TX | 100BASE-T4 | 100BASE-FX |
|---|---|---|---|
| Cable | UTP Cat.5 | UTP Cat.3/5 | Fibra 62,5/125µ |
| Pares | 2 | 4 | 2 |
| Topología | Estrella | Estrella | Estrella |
| Distancia Segmento | 100, máx 200 m | 100, máx 200 m | 400 m |
| Codificación | MLT-3 | 8B6T | 4B5B-NRZI |
| Tipo Conector | RJ-45 | RJ-45 | SC |

**Tabla 1. 1 Estándares para capa física de *Fast Ethernet*** [7]

### 1.2.2 REDES *GIGABIT ETHERNET*

A finales del año 1995, el comité IEEE 802.3 formó el grupo de trabajo para desarrollar un estándar de alta velocidad con el fin de investigar las estrategias para transmitir paquetes con formato *Ethernet*, a velocidades en el orden de los

[7] HIDALGO Pablo, Redes de Área Local

*Gigabits* por segundo, así nace un conjunto de estándares a 1000 Mbps, definido en los estándares IEEE 802.3ab e IEEE 802.3z.

*Gigabit Ethernet* opera en modo *half-duplex* y *full-duplex*, permitiendo en esta segunda modalidad la implementación de un *backbone* conmutado operando a 2 Gbps. El modo *full-duplex*, es idéntico a *Fast Ethernet*, pero más rápido, para lo cual utiliza CSMA/CD con ciertas mejoras con respecto al funcionamiento de los concentradores, realizando: Extensión de Portadora y Ráfagas de tramas.

#### 1.2.2.1 Características

Entre las características de *Gigabit Ethernet*, se destacan:

- Velocidad de transmisión: 1000 Mbps.
- Debido a que la ventana de colisiones se mantiene en 4096 bit-times, que en este caso será 0.512 microsegundos, el alcance (longitud total de la red), se divide para mil.
- Utiliza modo de operación *Half-Duplex* y *Full-Duplex*.
- Las técnicas de codificación de la señal son 8B/10B y PAM5.
- Acepta 4 tipos de medios físicos, definidos en IEEE 802.3z (1000Base-X) e IEEE 802.3ab (1000Base-T)

#### 1.2.2.2 Capa de Acceso al Medio

La especificación a 1000 Mbps utiliza el mismo formato para las tramas y protocolo que el CSMA/CD usado en las versiones de IEEE 802.3 a 10 Mbps y 100 Mbps. Como se mencionó anteriormente, se han introducido dos mejoras respecto al esquema CSMA/CD básico en lo que se refiere al funcionamiento de los concentradores.

- **Extensión de Portadora**

  Esta mejora consiste en añadir una serie de símbolos al final de la trama MAC, de tal manera que el bloque resultante tenga una duración equivalente a 4.096 bits, mucho mayor que los 512 bits exigidos en el estándar a 10 y 100 Mbps.

- **Ráfaga de tramas**

  Cuando una estación tiene un número de paquetes cortos a trasmitir, se envía el primer paquete si es necesario usando extensión de portadora y los siguientes paquetes se trasmiten uno detrás de otro, con el mínimo intervalo inter trama (IFG, *Inter Frame Gap*) hasta que finalice el tiempo de ráfaga (8192 bytes), todo esto sin necesidad de dejar el control del CSMA/CD. Las ráfagas de tramas evitan la redundancia y gasto que conlleva la técnica de la extensión de la portadora, en el caso de que una estación tenga preparadas para transmitir varias tramas pequeñas.

La Figura 1.1 y la Figura 1.2 muestran las tramas tanto para la transmisión utilizando Extensión de Portadora o Ráfaga de Tramas.

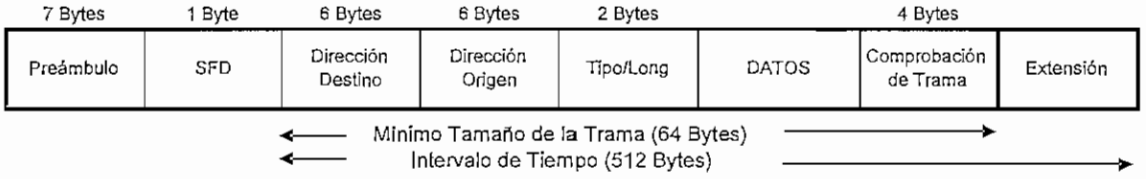



**Figura 1.1 Transmisión Utilizando Extensión de Portadora**

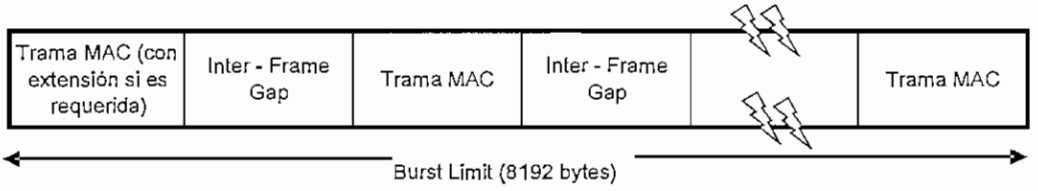



**Figura 1.2 Transmisión Utilizando Ráfaga de Tramas**[8]

### 1.2.2.3 Capa Física

La especificación actual del IEEE 802.3 a 1 Gbps define las siguientes alternativas:

- **1000BASE-SX (802.3z):** usa longitudes de onda pequeñas, proporciona enlaces dúplex de 275 m usando fibras multimodo de 62.5 µm o hasta 550

[8] http://www.monografias.com/trabajos12/giga/giga.shtml

m con fibras multimodo de 50 µm. Las longitudes de onda están en el intervalo comprendido entre 770 y 850 nm.

- **1000BASE-LX (802.3z):** utiliza longitudes de onda mayores, proporciona enlaces dúplex de 550 m usando fibras multimodo de 62.5 µm o 50 µm, o de 5 km con fibras monomodo de 10 µm. Las longitudes de onda están entre los 1.270 y los 1.355 nm.
- **1000BASE-CX (802.3z):** proporciona enlaces de 1 Gbps entre dispositivos localizados dentro de una habitación (o armario de conexiones) utilizando hilos de cobre (cables de pares trenzados de menos de 25 m con un apantallamiento especial). Cada enlace consiste en dos pares trenzados apantallados, cada uno de los cuales se usa en un sentido y operación en el *backbone*.
- **1000BASE-T (802.3ab):** esta opción utiliza cuatro pares no apantallados categoría 5 o superior, para conectar dispositivos separados hasta 100 m.

| CARACTERÍSTICA | 1000BASE-T | 1000BASE-CX | 1000BASE-SX | 1000BASE-LX |
|---|---|---|---|---|
| Cable | UTP Cat.5 | STP | Fibra Óptica | Fibra Óptica |
| Pares | 4 | 2 | 2 | 2 |
| Full Dúplex | Sí | Sí | Sí | Sí |
| Topología | Estrella | Estrella | Estrella | Estrella |
| Distancia Segmento | 100 m | 25 m | 275, máx 500 m | 550, máx 5000 m |
| Tipo Codificación | PAM 5 | 8B/10B | 8B/10B | 8B/10B |
| Tipo Conector | RJ-45 | DB-9 | SC | SC |

**Tabla 1.2 Estándares para capa física de *Gigabit Ethernet*** [9]

## 1.3 CARACTERÍSTICAS BÁSICAS DEL ESTÁNDAR IEEE 802.11g

### 1.3.1 DESCRIPCIÓN DEL ESTÁNDAR IEEE 802.11

IEEE 802.11 es un estándar definido para redes de área local inalámbricas (WLAN).

Al realizar el diseño de una WLAN se deben considerar ciertos problemas de implementación y conectividad como: propagación multi-trayectoria, pérdida por

[9] HIDALGO Pablo, Redes LAN.

trayectoria, interferencia de la señal de radio, tiempo de vida de las baterías, interoperabilidad de sistemas, seguridad de la red, problemas de conexión, consideraciones de la instalación y riesgos en la salud.

La arquitectura que define IEEE 802.11 incluye, la capa física (PHY *Physical Layer*) y la capa enlace; esta última a su vez se encuentra subdividida en las subcapas LLC y MAC. Para la subcapa LLC se emplean las especificaciones definidas en el estándar IEEE 802.2.

Al emplear medios de transmisión inalámbricos, se deben tomar en cuenta aspectos como: topología dinámica, estaciones ocultas, medios no protegidos, medios no guiados, y medios no confiables, ya que esto conlleva a formatos de tramas y especificaciones de nivel físico diferentes.

#### 1.3.1.1 Topología de IEEE 802.11

La arquitectura IEEE 802.11 define dos posibles topologías[10], *Ad Hoc* y de Infraestructura. Las topologías que se emplean en redes inalámbricas, son únicamente reglas básicas de comunicación, más no disposiciones estáticas de dispositivos.

El bloque constructivo fundamental de una WLAN, es el conjunto de servicios básicos (BSS *Basic Service Set*). Un BSS es un conjunto de estaciones que coordinan su acceso al medio a través de un procedimiento dado, en el cual se define un identificador del grupo de servicios (SSID *Service Set Identifier*), para determinar el nombre o dominio de la WLAN.

El área de cobertura geográfica de un BSS se denomina Área de Servicios Básicos (BSA *Basic Service Area*), sus límites se pueden ver afectados entre otros factores, por condiciones ambientales o elementos arquitectónicos del sitio.

Una topología *Ad Hoc* consiste en un grupo de estaciones donde cada una se encuentra dentro del límite de acción de las otras, y generalmente son de naturaleza temporal. Éstas son creadas y administradas sin la necesidad de un

[10] SINCHE Soraya, Redes de Área Local Inalámbricas.

control central o de un AP, por lo cual la señalización es controlada por las estaciones. La BSS utilizada para formar una topología de este tipo se la conoce como IBSS (BSS Independiente).

En el estándar se define que se puede interconectar un conjunto de BSSs mediante un Sistema de Distribución (DS *Distribution System*), dando lugar a un Conjunto de Servicios Ampliados (ESS *Extended Service Set*).

Cada BSS tiene un AP que presenta la funcionalidad de una estación y permite acceder al DS. Un ESS permite también el acceso a una red cableada, para lo cual utiliza dispositivos llamados Portales.

Una topología de infraestructura es la combinación de: uno o varios BSS, de un sistema de distribución y de uno o más portales.

#### 1.3.1.2 Servicios Soportados en IEEE 802.11

IEEE 802.11 no define en detalle el sistema de distribución, en su lugar se especifica servicios empleados por la subcapa MAC.

Se definen cinco servicios de distribución:

- **Asociación**: permite a la estación establecer una conexión con el AP.
- **Reasociación**: se produce cuando una estación se mueve de un AP a otro.
- **Desasociación**: se origina cuando una estación sale del área de cobertura del AP o se apaga.
- **Distribución**: permite al AP enrutar los datos hacia las estaciones.
- **Integración**: maneja el direccionamiento y formato de traducción al estándar requerido, cuando las tramas van a ser enviadas por una red no IEEE 802.11.

Define además cuatro servicios de estación:

- **Entrega de datos**: brinda el servicio mediante el cual la estación transmite y recibe datos.

- **Privacidad**: protege el acceso al contenido de los mensajes, a través de diversos tipos de encripción.
- **Autenticación**: una estación establece la identidad de otra estación, a través del protocolo WEP[11].
- **Desautenticación**: se produce cuando una estación deja la red.

### 1.3.2 IEEE 802.11 CAPA FÍSICA (PHY)

Esta capa se encarga de proveer una serie de servicios a la subcapa MAC. El estándar define diferentes tecnologías de capa física para transmitir por el medio inalámbrico. La capa física se divide en dos subcapas: subcapa de Procedimiento de Convergencia de Capa Física (PLCP *Physical Layer Convergence Procedure*) y subcapa Dependiente del Medio Físico (PMD *Physical Medium Depend*), como se muestra en la Figura 1.3.

| Estándar | Capas | Modelo OSI |
|---|---|---|
| IEEE 802.2 | Subcapa LLC ( IEEE 802.2) | Capa Enlace |
| IEEE 802.11 | Subcapa MAC | |
| | Procedimiento de Convergencia de Capa Física (PLCP) | Capa Física |
| | Capa Dependiente del medio físico (PMD). | |

**Figura 1.3 Capas Física y Enlace de IEEE 802.11 e IEEE 802.2**

#### 1.3.2.1 IEEE 802.11 Subcapa PMD

Define las características y métodos de transmisión y recepción de datos, a través de un medio inalámbrico entre dos o más estaciones, incluye además técnicas de codificación y modulación a emplear sobre el medio.

Esta capa provee también un conjunto de primitivas que describen el interfaz entre la PLCP y la PMD. Este interfaz se denomina punto del acceso al servicio (PMD-SAP PMD *Service Access Point*).

Dentro del estándar se definen mecanismos para conseguir el acceso al medio físico, estas técnicas de acceso pueden ser por medio de Infrarrojos DFIR, FHSS

[11] *Wired Equivalency Protocol*, mecanismo de seguridad.

y DSSS. Posteriormente se introducen OFDM para IEEE 802.11a y HRDSSS (*High Rate - Direct Sequence Spread Spectrum*) para IEEE 802.11b.

*1.3.2.1.1 Salto de Frecuencia FHSS*

La técnica de acceso al medio de Espectro Ensanchado por Salto de Frecuencia, es utilizada como mecanismo para combatir la interferencia. Asigna frecuencias que van cambiando de acuerdo a un patrón de salto pseudo-aleatorio, tal que, tanto el transmisor como el receptor al estar sincronizados, garantizan una transmisión exitosa.

Dispone de velocidades de 1 y 2 Mbps, mediante 2 y 4 estados de modulación GFSK (*Gaussian Frequency Shift Keying*) respectivamente.

Opera con 79 canales en la banda de 2.4 GHz con un ancho de banda de 1MHz cada uno. El tiempo de utilización de un canal de frecuencia es variable, pero no mayor a 400 ms.

*1.3.2.1.2 Secuencia Directa DSSS*

La técnica de acceso al medio de espectro ensanchado en secuencia directa, emplea dos técnicas de modulación para alcanzar velocidades de 1 y 2 Mbps, la modulación de intercambio de fase con dos estados (DBPSK *Differential Binary Phase Shift Keying*) y la modulación de intercambio de fase en cuadratura con 4 estados (DQPSK *Differential Quadrature Phase Shift Keying)* respectivamente.

Emplea una secuencia *Barker*[12] de 11 chips para representar el 0 y 1 lógicos; divide la banda de 2.4 GHZ en 11 canales sobrelapados y espaciados entre si a 5 MHz.

*1.3.2.1.3 Infrarrojos DFIR*

Este medio inalámbrico requiere que exista línea de vista entre el transmisor y receptor, siendo por ello usado en ambientes interiores. Trabaja en la banda de

[12] Secuencia producida por un generador de código que inserta a la señal original de datos los "*code bits* o chips" para ampliar el espectro de la señal. La secuencia es: +1-1+1+1-1+1+1+1-1-1-1.

850 – 900 nm, con velocidades de 1 y 2 Mbps llamadas *basic access rate* y *enhanced access rate* respectivamente, y con un alcance máximo de 20 metros.

Utiliza técnicas de modulación 16-PPM[13] para 1 Mbps y 4-PPM para lograr 2 Mbps. Para 1 Mbps se utilizan palabras de 4 a 16 bits que se codifican con el código de *Gray*[14], generando palabras de 16 bits con quince ceros y un uno; y para 2 Mbps se utilizan palabras de 2 a 4 bits que se codifican con el código de *Gray*, teniendo palabras de 4 bits con tres ceros y un 1.

*1.3.2.1.4 OFDM*

La técnica de Multiplexación por División de Frecuencia Ortogonal es empleada en la banda de 5 GHz por el estándar IEEE 802.11a/g para tener velocidades de hasta 54 Mbps; define 64 frecuencias, 12 como subportadoras cero, 4 para sincronización, y 48 para datos.

Es una técnica de comunicación, que trasmite un flujo de datos a alta velocidad, sobre múltiples flujos de datos paralelos a baja velocidad, en diferentes canales de frecuencia sobre un medio de transmisión; esto es, se transmiten múltiples portadoras para garantizar que sus componentes de frecuencia principales, no sean afectadas por problemas de interferencia o desvanecimiento por múltiple trayectoria. Con la frecuencia adecuada se recupera la señal, tomando en cuenta únicamente dichas principales armónicas, alcanzando mayores velocidades.

La ortogonalidad de esta técnica se consigue al alinear el pico de amplitud de una subportadora con el valor nulo de otra subportadora y así el receptor detecta la señal portadora a este pico de amplitud, sin que exista interferencia desde otras subportadoras.

*1.3.2.1.5 DSSS de Alta Velocidad (HR - DSSS)*

Permite velocidades de 5,5 y 11 Mbps adicionales a 1 y 2 Mbps en la banda de 2.4 GHz, mediante la técnica de modulación CCK (*Complementary Code Keying*).

---

[13] Modulación por Posición de Pulso.
[14] Codificación con el menor número de transiciones posibles.

CCK aplica una secuencia de 1.375 Mbaudios con 4 y 8 bits por baudio para conseguir 5,5 y 11 Mbps respectivamente. CCK emplea un conjunto de 64 palabras código, cada una de ellas de 8 bits, para codificar las velocidades mencionadas; su principal objetivo es distinguir correctamente la información enviada por el transmisor al receptor en ambientes de ruido e interferencia.

#### 1.3.2.2 IEEE 802.11 Subcapa PLCP

Proporciona la función de convergencia para transformar las unidades de datos (PDU *Packet Data Unit*), a un formato de trama adecuada para su transmisión y recepción a través de un medio físico. La estructura de cada PLCP depende de la definición de la capa física en particular. Cada PDU MAC se transforma en una trama PLCP. Los campos de la trama PLCP son:

- **Preámbulo PLCP**: formado por los campos Sincronización y Delimitador de Inicio de Trama.
- **Cabecera PLCP**: formado por Servicio, Longitud y CRC[15].
- **PLCP PDU (PPDU)**: corresponde a la MPDU (PDU MAC) encapsulada como datos.

El estándar define para cada tipo de capa física su correspondiente capa PLCP.

#### 1.3.2.3 IEEE 802.11 Subcapa MAC

Para establecer prioridades en el acceso al canal, se definen los espacios inter-trama (IFS *Inter Frame Space*). Estos espacios son intervalos de tiempo entre transmisión de tramas.

El estándar define también las Funciones de Coordinación, para determinar cuando una estación en un BSS puede transmitir y recibir información. Los tipos de funciones disponibles son, Función de Coordinación Distribuida (DCF *Distributed Coordination Function*) y Función de Coordinación Puntual (PCF *Point Coordination Function*).

[15] Código de Redundancia Cíclica

*1.3.2.3.1 Función de Coordinación Distribuida DCF*

Esta función permite la transmisión de datos asíncronos de unidades de datos MAC empleando el método del mejor esfuerzo. DCF opera en modo de contención mediante el protocolo CSMA/CA[16], y es empleado en redes *Ad Hoc* ya que no se cuenta con un control central.

*1.3.2.3.2 Función de Coordinación Puntual PCF*

En este tipo de coordinación se tiene un control centralizado desde una estación base sobre toda su área de cobertura (celda).

La estación base pregunta a las estaciones si tienen datos que transmitir mediante un sondeo, como la estación base asigna los permisos de transmisión se evitan las colisiones. La utilización del medio está controlada por el AP con lo cual no existe lucha por acceso al canal.

*1.3.2.3.3 Tipos de Tramas*

Existen tres tipos de tramas a nivel MAC:

- Control: ACKs (*Acknowledgments*) positivos y *handshake*[17] para acceso al canal.
- Datos: información a ser transmitida sobre el canal.
- Gestión: asociación y desasociación de estaciones con el AP, para tareas de autenticación.

Estas se especifican de acuerdo al campo de control de la trama, que consta en la cabecera MAC.

**1.3.2.4 Cabecera MAC**

La cabecera MAC proporciona información de: control, duración, direccionamiento y control de secuencia de trama.

[16] Acceso múltiple con detección de portadora con prevención de colisiones
[17] Señales de control para el establecimiento de la comunicación.

| Bytes 2 | 2 | 6 | 6 | 6 | 2 | 6 | 0 - 2312 | 4 |
|---|---|---|---|---|---|---|---|---|
| Control de Trama | Duración /ID | Dirección 1 | Dirección 2 | Dirección 3 | Control de Sec. | Dirección 4 | Cuerpo de Trama | FCS |

**Figura 1.4 Formato de trama MAC**[18]

*1.3.2.4.1 Campo Control de Trama (Frame Control)*

El campo de control de la trama transporta instrucciones correspondientes a la naturaleza del paquete. Especifica el tipo de señal de control o gestión que el paquete desea hacer. Consiste de los subcampos mostrados en la Figura 1.5.

| 2 bits | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Versión Protocolo | Tipo | Subtipo | Hacia el DS | Desde el DS | Más Frag. | Retry | Admin. Potencia | Más Datos | WEP | Orden |

**Figura 1.5 Campo de Control de trama**

La descripción de cada campo de la Figura 1.5, se resume en la siguiente tabla:

| Campos | Descripción |
|---|---|
| Versión del Protocolo | Versión del protocolo a emplear en la transmisión. |
| Tipo | Tipo de trama: administración, control o datos. |
| Subtipo | RTS, CTS, etc. |
| Hacia el DS | Trama dirigida al sistema de distribución. |
| Desde el DS | Trama desde el sistema de distribución. |
| Más Fragmentos | Indica que hay más fragmentos. |
| Retry | Marca que es una trama de retransmisión. |
| Administración de Potencia | Pone al receptor en estado de espera. |
| Más Datos | El emisor tiene más tramas que enviar. |
| WEP | El cuerpo de la trama ha utilizado WEP. |
| Orden | La secuencia de tramas debe procesarse en orden estricto. |

**Tabla 1.3 Descripción de los campos de control de trama**

*1.3.2.4.2 Campo Duración (Duration / ID)*

Este campo especifica cuanto tiempo ocupará el canal la trama y su confirmación de recepción. A través de este campo se maneja el mecanismo de Vector de Asignación a la Red (NAV *Network Assignation Vector*) con tramas de control.

[18] SINCHE Soraya, Redes de Área Local Inalámbricas

NAV es un indicador temporal de cada estación que se mantiene mientras la transmisión se inicia, cuando el medio inalámbrico está ocupado.

*1.3.2.4.3 Campos de Direcciones*

Los cuatro campos de dirección identifican origen, destino y APs a los que ellos se conectan.

*1.3.2.4.4 Campo Control de Secuencia*

El campo de control de secuencia consta de dos subcampos: Número de Secuencia y Número de Fragmento.

Permite agregar un número de secuencia único al MSDU[19] o MMPDU[20], mientras que el número de fragmento lo identifica cuando la trama ha sido fragmentada.

*1.3.2.4.5 Campo Cuerpo de Trama*

El cuerpo de trama contiene la información de la subcapa LLC de nivel superior, la cual se encapsula como datos para la trama MAC. Tiene un tamaño variable que oscila entre 0 y 2312 bytes.

*1.3.2.4.6 Trailer FCS*

La secuencia de chequeo de trama, emplea CRC de 4 bytes como mecanismo de protección de la información del cliente MAC.

### 1.3.3 ESTÁNDAR IEEE 802.11g

Este suplemento[21] del estándar IEEE 802.11, fue creado debido a la imperiosa necesidad de incrementar la velocidad de transmisión de los datos en una red. Oficialmente fue designado como *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

---

[19] MAC *Service Data Unit*
[20] MPDU *Management Data Units*
[21] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*, IEEE 802.11g, Junio del 2003.

IEEE 802.11g define un interfaz aire entre dos clientes inalámbricos o un cliente inalámbrico y un AP, alcanzando velocidades de hasta 54 Mbps en la banda de 2.4 GHz; garantiza compatibilidad con IEEE 802.11b. Incorpora una Capa Física de Velocidad Extendida (ERP *Extended Rate Physical*) con técnicas de modulación combinadas, como DSSS, HR-DSSS, CCK a velocidades de 1, 2, 5.5, y 11 Mbps; adicionalmente adopta la técnica OFDM de IEEE 802.11a para alcanzar velocidades de 54 Mbps.

La principal modificación de este estándar respecto de IEEE 802.11, inicia en el formato de la trama PLCP, por lo cual se lo describe en el Anexo A.

### 1.3.3.1 Capa Física de Velocidad Extendida (ERP) de 802.11g

El estándar define esta capa con las siguientes opciones de modulación: DSSS para velocidades de 1 y 2 Mbps, CCK y PBCC[22] (opcional) para velocidades de 5.5 y 11 Mbps; adicionalmente la capa ERP provee velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Se especifican dos tipos de modulación opcionales: ERP – PBCC para velocidades de 22 y 33 Mbps y DSSS – OFDM para velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

#### *1.3.3.1.1 Formato de la Trama PLCP de IEEE 802.11g*

En esta trama se considera obligatorio el preámbulo corto PLCP de IEEE 802.11b (Anexo 1A), para alcanzar las velocidades mencionadas anteriormente. Una estación que opere con capa física ERP, debe soportar tres combinaciones de preámbulo y cabecera.

El primer formato incluye el Preámbulo Grande y la Cabecera, es empleado para las velocidades de 1, 2, 5.5 y 11 Mbps.

Esta trama provee interoperabilidad con BSSs y estaciones que trabajen a las velocidades mencionadas. La modulación empleada es DSSS–OFDM y como modulación opcional ERP–PBCC.

---

[22] *Packet Binary Convolutional Coding*, esquema de codificación para obtener velocidades de 2, 5.5 y 11 Mbps

El segundo formato define Preámbulo Corto y Cabecera, soporta velocidades de 2, 5.5 y 11 Mbps y emplea tanto DSSS-OFDM y ERP-PBCC.

El tercer formato especifica Preámbulo ERP-OFDM y Cabecera de acuerdo al estándar IEEE 802.11a (Anexo 1A) con ciertas modificaciones.

#### *1.3.3.1.2 ERP-OFDM*

El formato de trama para ERP-OFDM, define el mismo Preámbulo, Señalización y Datos que para IEEE 802.11a (Anexo 1A), pero para utilizar al máximo todas las capacidades de la capa física OFDM, se incluyen las siguientes diferencias:

- La banda de frecuencias a utilizar es la de 2.4 GHz.
- Nivel máximo de potencia de la señal de entrada de -20 dBm, en lugar de los -30 dBm definido en IEEE 802.11a.
- El espacio corto entre tramas SIFS es de 10 µs en lugar de 16 µs de IEEE 802.11a.

#### *1.3.3.1.3 DSSS-OFDM*

Este esquema es la combinación de DSSS con OFDM y utiliza los preámbulos corto y grande de 802.11g.

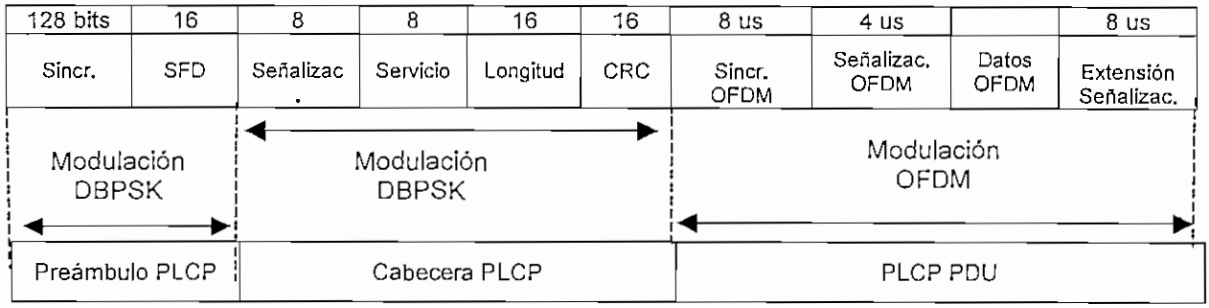



Figura 1.6 Formación de la Trama PLCP PDU para DSSS - OFDM[23]

Para todas las velocidades y preámbulos DSSS-OFDM, el campo Señalización definido en IEEE 802.11b se establece a 3 Mbps, con lo cual los 8 bits de este campo tienen el valor de $X1E_H$, lo cual indica que aquellas estaciones que no

[23] SINCHE Soraya, Redes de Área Local Inalámbricas

tengan la capacidad de trabajar con ERP, deben leer el campo longitud y no emplear el canal durante este tiempo.

En la Figura 1.6 se muestra la formación de la trama PLCP PDU para DSSS-OFDM.

*1.3.3.1.4 Campo PLCP PDU de DSSS-OFDM*

La trama PLCP PDU está compuesta por 4 secciones principales: Sincronización OFDM, Señalización OFDM, Datos OFDM y Extensión de Señalización como se puede observar en la figura anterior.

El campo de Sincronización OFDM consta de un intervalo de guarda (1.6 us) y dos símbolos de entrenamiento grandes (3.2 us); además contiene 52 subportadoras moduladas con DBPSK. Es empleado para la adquisición de parámetros de recepción para el demodulador.

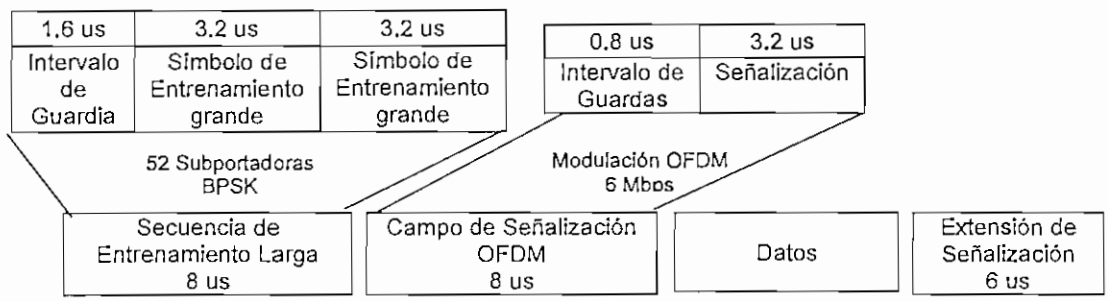



**Figura 1.7 Campo PLCP PDU de DSSS - OFDM[24]**

El campo Señalización OFDM provee información al receptor sobre la longitud y velocidad del campo de Datos OFDM. Este campo es idéntico al campo Señalización definido en IEEE 802.11a.

El campo Extensión de Señalización define un intervalo de tiempo prohibido para la transmisión, lo cual permite al demodulador haga la decodificación de los códigos convolucionales empleados en la modulación.

[24] SINCHE Soraya, Redes de Área Local Inalámbricas

## 1.4 CARACTERÍSTICAS PRINCIPALES DE LA TECNOLOGÍA *BLUETOOTH*[25]

*Bluetooth* es una tecnología desarrollada por la SIG[26] (Grupo de Interés Especial *Bluetooth*), constituido principalmente por: Nokia, Ericsson, IBM, Intel, y Toshiba. Las especificaciones *Bluetooth* fueron publicadas en el año 1999, para dar paso a la conectividad inalámbrica entre dispositivos a corta distancia; éstos pueden llegar a formar redes con diversos equipos de comunicación: computadoras móviles, radio-localizadores, teléfonos celulares, PDAs, e inclusive electrodomésticos.

La IEEE ha desarrollado un protocolo equivalente denominado *Wireless Personal Area Network* (WPAN) 802.15, con el objetivo de lograr la interoperabilidad con otros dispositivos inalámbricos. IEEE 802.15.1 cubre *Bluetooth* más otros estándares adicionales (IEEE 802.15.3 e IEEE 802.15.4).

### 1.4.1 ESPECIFICACIONES BÁSICAS

*Bluetooth* soporta comunicaciones de voz y datos, tanto punto a punto como punto a multipunto. Es una tecnología con bajo consumo de recursos, que optimiza el modelo de uso para todos los dispositivos móviles y proporciona:

- Posibilidades de utilización en todo el mundo.
- Gestión de datos y de voz.
- La habilidad de establecer conexiones y redes ad hoc.
- La habilidad de resistir a las interferencias procedentes de otras fuentes que operen en la banda abierta.
- Un consumo de potencia despreciable, en comparación con otros dispositivos de uso similar.
- Un estándar de interfaz abierta.
- Un bajo costo por unidad, comparado con los equivalentes no basados en *Bluetooth*.

---

[25] http://www.bluetooth.com
[26] SIG: *Bluetooth Special Interest Group*

### 1.4.2 CARACTERÍSTICAS

Entre las características principales de *Bluetooth* se pueden señalar las siguientes:

- **Ancho de Banda**: utiliza el ancho de banda ISM, que puede operar en todo el mundo, excepto países como en Francia, España y Japón que tiene ciertas restricciones. La banda ISM de 2.45 GHz, tiene el rango que va desde los 2,4 GHz a los 2,5 GHz.
- **Datos o voz**: utiliza un canal para la transferencia de datos, voz o ambos a la vez, integrando los servicios.
- **Búsqueda de dispositivos**: cuando dos o más dispositivos *Bluetooth* están dentro del alcance, se establece un proceso de localización de dispositivos para realizar un enlace, siempre y cuando operen en la misma banda de frecuencia y estén dentro del radio de cobertura.
- **Bajo consumo de potencia**: los dispositivos *Bluetooth* son pequeños y su portabilidad requiere de un uso adecuado de la energía.
- **Alcance**: basado en la transmisión por radio de corto alcance, con un alcance normal de 10 metros o bien de 100 metros.
- **Seguridad**: emplea FHSS, como técnica de multiplexaje, lo que disminuye el riesgo de que las comunicaciones sean interceptadas o se presente interferencia con otras aplicaciones. Provee también especificaciones para autenticar dispositivos que intenten conectarse a la red *Bluetooth*, así como cifrado en el manejo de llaves para proteger la información
- **Bajo costo**: los dispositivos *Bluetooth* pueden ser pequeños microchips, lo cual hace que su costo sea reducido. Además al operar en la banda de 2.45 GHz, que no requiere licencia, hace que esté disponible para cualquier sistema de radio en todo el mundo.
- **Transmisión omnidireccional**: debido a que basa su comunicación en radiofrecuencia, no requiere línea de vista y permite configuraciones punto-multipunto.
- **Establecimiento de redes**: permite formar redes en una topología donde, un dispositivo hace las veces de maestro y hasta siete trabajando como esclavos.

### 1.4.3 CONECTIVIDAD

*Bluetooth* es un sistema que utiliza la conectividad AD HOC a gran escala y su disposición es abierta a gran parte del público.

Un sistema AD HOC son sistemas descentralizados, donde no existe una estación base o terminales distinguibles, un ejemplo de éstos es el *walky-talky*, utilizado por militares, policías, etc.

### 1.4.4 LIMITACIONES DE LA BANDA DE OPERACIÓN

La banda de los 2.45 GHz tiene gran interferencia y limitaciones de potencia. Para la eliminación de la interferencia se utilizan esquemas tipificados o técnicas de ensanchamiento de espectro, siendo las últimas más utilizadas.

### 1.4.5 DEFINICIÓN DEL CANAL

*Bluetooth* utiliza un esquema FH/TDD[27], cuyo canal es dividido en *slots* de 625 (μs), cada *slot* utiliza un salto de frecuencia distinto transmitiendo un paquete. Los *slots* consecutivos son usados para transmitir y recibir (TDD).

Dos o más unidades que comparten un canal forman una Picored. El canal FH está determinado por la secuencia de saltos y la fase de esta secuencia.

En cada Picored una unidad actúa como maestro y el resto como esclavos. El tamaño máximo de unidades en una Picored es 8. La secuencia de saltos está determinada por la identidad del maestro y la fase por el reloj de éste.

Para recrear el reloj maestro en el esclavo, cada unidad debe agregar un *offset*[28] a su reloj nativo. De esta forma cada unidad a partir de la identidad del maestro y el *offset* respectivo podrá seleccionar adecuadamente la secuencia de salto y permanecerá sincronizada con el resto.

---

[27] División de Tiempo Dúplex
[28] Secuencia de sincronización

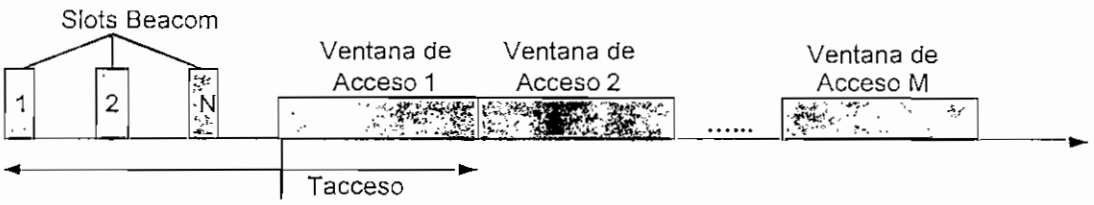



Figura 1.8 Definición del canal *beacom* y ventana de acceso

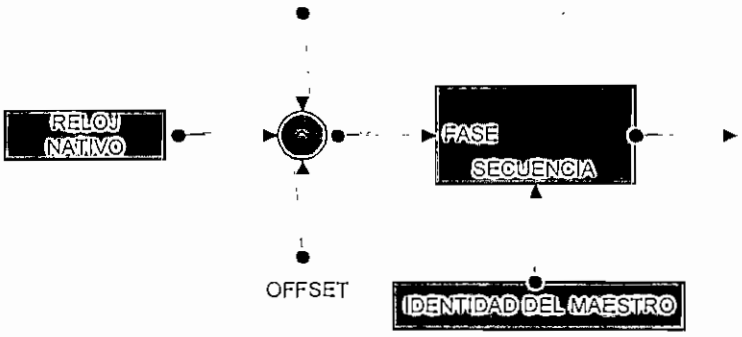



Figura 1.9 Selección de la secuencia de salto[29]

### 1.4.6 MODULACIÓN

En la banda ISM el ancho de banda para los sistemas FH está limitada en 1 MHz. El ancho de banda disponible es de 79 MHz, por lo que se dispone de 79 canales de salto.

*Bluetooth* utiliza FSK con pulsos *Gaussianos* y un índice de modulación nominal k=0.3. Con esto se logra una tasa de transmisión cercana a 1 Mbps. La elección de este esquema radica en su robustez y simplicidad de implementación (demodulación no coherente).

### 1.4.7 SCATTERNET

Dos o más picoredes que comparten una parte de su espacio físico de transmisión forman una *Scatternet*.

Las *Scatternet* permiten aprovechar mejor el ancho de banda, y el *throughput* individual de los usuarios es mucho mayor que si todos ellos estuviesen

[29] SINCHE Soraya, Comunicaciones Inalámbricas

conectados a una misma Picored. Puesto que las secuencias de salto no son ortogonales, a medida que aumenta el número de Picoredes el desempeño se degrada.

Una estimación bastante simplificada del *throughput* normalizado es:

$$TH = \left(1 - \frac{1}{79}\right)^{N-1}$$

**Ecuación 1.1 Estimación de *Throughput* en *Bluetooth*** [30]

Donde N es el número de picoredes.

La información intercambiada por una Picored solo es compartida por los miembros de esa Picored, no por toda la *Scatternet*. Una unidad puede participar en distintas Picoredes por medio de TDD (instantáneamente solo puede estar en un canal), pero solo en una Picored puede ser maestro.

### 1.4.8 CONTROL DE ACCESO AL MEDIO

En teoría[31], si las secuencias de salto fuesen ortogonales, se podría alcanzar un límite de 79 Mbps. Sin embargo, en *Bluetooth* las secuencias son deliberadamente no ortogonales. La razón principal es que es poco probable que todas las unidades en un cierto rango necesiten comunicarse entre ellas, o sea requerir una capacidad total cercana a 79 Mbps. Esto permite que su implementación sea más sencilla, comparado con una ortogonalidad total.

Aparte de definir la Picored, el maestro controla el tráfico y el acceso a la red. El maestro establece un control centralizado; y así solo es posible la comunicación entre maestro y esclavo. Para que no se produzcan colisiones el maestro utiliza sondeo. En cada *slot* el maestro decide quien transmite. Este esquema se realiza mediante una conexión de pares. El maestro transmite un paquete a un esclavo el cual debe responder en el *slot* siguiente y no en otro.

---

[30, 31] SINCHE Soraya, Redes de Área Local Inalámbricas

### 1.4.9 DEFINICIÓN DE CAPA ENLACE

Se definen dos tipos de enlace:

- Enlace sincrónico orientado a la conexión (SCO)
- Enlace asincrónico no orientado a la conexión (ACL)

El enlace SCO soporta conexiones simétricas punto a punto y con conmutación de circuitos. Típicamente usado para voz.

Para establecer este tipo de conexión se reservan dos *slots* consecutivos cada cierto período fijo. La reserva se realiza cuando se establece la conexión entre el maestro y el esclavo.

Los enlaces ACL soportan conexiones simétricas o asimétricas, punto a multipunto y con conmutación de paquetes. Por defecto, cuando se establece la Picored la unidad maestra establece una conexión ACL con las unidades esclavas. La conexión SCO debe establecerse explícitamente después de que se ha creado la Picored.

### 1.4.10 DEFINICIÓN DE PAQUETES

#### 1.4.10.1 Direccionamiento *Bluetooth*

Es posible establecer cuatro tipos de direccionamiento:

a) Direccionamiento de Dispositivo *Bluetooth*. (BD_ADDR *Bluetooth device address):* éste define a cada *transceiver Bluetooth* con una única dirección de 48-bit, los cuales son derivados del estándar IEEE 802.
b) Direccionamiento de Miembros Activos. (*AM_ADDR Active member address):* éste identifica a cada esclavo activo (no al master) en la Picored con 3 bits de direccionamiento. La dirección de todos ceros es reservada para mensajes de *broadcast*. Cuando un esclavo está desconectado o en estado de parqueo, se pierde el AM_ADDR.
c) Direccionamiento de Paquetes Miembros *(PM_ADDR):* éste identifica a un esclavo en el modo parqueo y emplea 3 bits.

d) Direccionamiento de Acceso Requerido. *(AR_ADDR Access request address):* éste es empleado por un esclavo para identificar el esclavo-maestro en la ventana de acceso para enviar un mensaje de requerimiento de acceso. Esto es asignado por el maestro cuando un esclavo entra en el modo de parqueo.

En cada *slot* se intercambia un paquete entre el maestro y algunas de las unidades esclavo.

Los paquetes tienen formato fijo. Cada paquete comienza con un código de acceso de 72 bits que se deriva de la identidad del maestro y es único para ese canal.

| 72 bits | 54 bits | 0 – 2745 bits |
|---|---|---|
| Código de Acceso | Cabecera | Payload |

**Figura 1.10 Campos de la Trama de Direccionamiento *Bluetooth*[32]**

Los receptores en la Picored comparan el paquete entrante con el código de acceso. Si éstos no calzan, descartan el paquete. Además el código de acceso se usa también para sincronización.

El código de acceso es seguido de un encabezado. Éste contiene importante información de control tal como la dirección del esclavo, tipo de paquete, control de flujo y bits para el ARQ (*Automatic Retransmission Query*).

| 3 | 4 | 1 | 1 | 1 | 8 |
|---|---|---|---|---|---|
| M_Adress | Tipo | Control de Flujo | ARQ | Numero de Secuencia SEQN | HEC |

**Figura 1.11 Campos de la cabecera de la Trama de Direccionamiento**

El ARQ se basa en un sistema de Parada y Espera (*Stop-and-Wait*) con un período de espera de un *slot*.

Es decir el éxito o fracaso de la transmisión se indica en el campo ARQN del paquete de vuelta.

[32] SINCHE Soraya, Comunicaciones Inalámbricas

Basados en la información del bit ARQN, el transmisor decide si envía un nuevo paquete o retransmite el anterior.

El receptor tiene 220 µs entre la transmisión del último bit y el envío de la respuesta. En ese tiempo debe verificar la validez del paquete.

El campo SEQN (*Sequence Number*) permite distinguir si el paquete es nuevo o es una retransmisión.

El *header* está protegido con un FEC 1/3, el cual se basa en repetir 3 veces cada bit. Los paquetes pueden o no contener *payload*. El tamaño de éste puede variar entre 0 y 2745 bits.

Para alcanzar *payloads* mayores a 280 bits, se utiliza formato *multislot*. Un paquete puede ocupar 1, 3 o 5 *slots*, dependiendo del tamaño del *payload*. Durante la transmisión de un paquete se mantiene la misma frecuencia.

Los tipos de paquetes se dividen entre paquetes de control y paquetes de información.

Los paquetes de control son de 4 tipos:

- **ID:** Paquete de identificación. Consiste solo en el código de acceso.
- **NULL:** Consisten solo en el código de acceso y la cabecera. Sirve para enviar información de control.
- **POLL:** Similar al anterior; usado por el maestro para forzar al esclavo a responder.
- **FHS:** Paquete de sincronización. Sirve para intercambiar información de identidad e información de reloj.

Además se definen 12 códigos de paquete (Tabla 1.4), que sirven para definir el tipo de servicio que se entrega (sincrónico o asincrónico) y el tamaño en *slots* del paquete. El *payload* puede o no ser protegido con FEC (1/3 o 2/3).

Considerando una transmisión sin FEC se puede lograr una máxima tasa asimétrica de 723.2 Kbps con un enlace de retorno de 57.6 Kbps.

| Tipo | Simétrico (kbps) | Asimétrico (kbps) |
|---|---|---|
| DM1 | 108.8 | 108.8 108.8 |
| DH1 | 172.8 | 172.8 172.8 |
| DM3 | 256.0 | 384.0 54.4 |
| DH3 | 384.0 | 576.0 86.4 |
| DM5 | 286.7 | 477.8 36.3 |
| DH5 | 432.8 | 723.2 57.6 |

**Tabla 1.4 Tasas de Transmisión en *Bluetooth*[33]**

Los paquetes DH1[34] (*Data High Rate*) son similares a los paquetes DM1 (*Data Medium Rate*), se diferencian únicamente en que los primeros no poseen codificación FEC en los datos. Esto significa que los paquetes DH1 pueden llevar más de 28 bytes de información en un *time slot.*

El DH3 es similar excepto que puede cubrir en 3 *time slots* y llevar más de 185 bytes. Finalmente, el paquete DH5 cubre en 5 *time* slots y lleva más de 341 bytes. Los paquetes DM1 llevan datos de información únicamente, conteniendo un código CRC de 16 bits y 18 bytes de información. Éstos se codifican usando 2/3 FEC y los paquetes pueden cubrir un solo *time slot.*

El paquete DM3 es similar al anterior, pero cubre 3 *time slots* llevando más de 123 bytes. Finalmente los paquetes DM5 pueden cubrir 5 *time slots* y llevar 226 bytes de información.

### 1.4.11 ENLACE CONFIABLE DE DATOS

La tasa de saltos en FH es bastante alta (1600 saltos/seg.). Si se pierde un paquete, se pierde solo una pequeña fracción de la información. Los paquetes pueden ser protegidos con FEC. El esquema ARQ permite retransmitir la información perdida con un mínimo retardo.

La voz transmitida en enlace SCO nunca se retransmite. En cambio se utiliza un esquema de codificación robusto basado en la Modulación Continua Variable Delta CVSD (*Continuos Variable Slot Delta Modulation*).

---

[33, 33] www.palowireless.com/infotooth/glossary.asp

### 1.4.12 ESTABLECIMIENTO DE CONEXIONES

Se definen 3 estados que permiten el establecimiento de conexiones

- Modo SCAN
- Modo PAGE
- Modo INQUIRY

#### 1.4.12.1 Modo SCAN

Cuando la unidad está en modo STANDBY (dormida), periódicamente escucha el canal tratando de captar el código de acceso asociado a su identidad.

Al despertar para escuchar abre una ventana de transmisión, la cual está adaptada a este código durante 10 (ms), en intervalos máximos de 3.84 (s).

Cada vez que la unidad se despierta para escuchar, lo hace en una frecuencia de salto distinta. Se define entonces una secuencia de "despertar" propia del receptor, la cual consta de 32 saltos que cubren al menos 64 MHz.

#### 1.4.12.2 Modo PAGE

Cuando hay una unidad que desea realizar una conexión (*paging unit*) con una unidad que está "dormida", ésta debe conocer primero la identidad del receptor.

La *paging unit* conoce entonces la "secuencia de despertar" del receptor, y comienza un proceso en donde por cada período de 3,84 (s) envía el código de acceso del receptor en la mitad de la "secuencia de despertar" (16 saltos) por cada 10 (ms), como se muestra en la Figura 1.12.

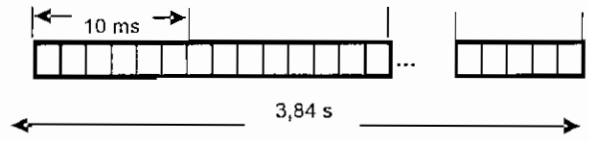



Figura 1.12 Establecimiento de Conexiones en Modo PAGE[35]

[35] SINCHE Soraya, Comunicaciones Inalámbricas

Si en algún instante la frecuencia de SCAN de la unidad dormida coincide con la frecuencia de PAGE la unidad dormida reconoce su código de acceso y envía en respuesta su mismo código de acceso. A esto la unidad de *paging* responde con un paquete FHS (secuencia de reloj y sincronización de fase)

Si en algún instante la frecuencia de SCAN de la unidad dormida coincide con la frecuencia de PAGE la unidad dormida reconoce su código de acceso y envía en respuesta su mismo código de acceso. A esto la unidad de *paging* responde con un paquete FHS (secuencia de reloj y sincronización de fase)

Con este procedimiento (PAGE-SCAN) se establece una Picored en donde la unidad de *paging* es la unidad maestra y la otra es la unidad esclava. Si en este intervalo la unidad no se conecta, quiere decir, que la unidad receptora se encontraba en la otra mitad de la secuencia de salto, por lo que la unidad de *paging* cambia su transmisión a esa mitad.

#### 1.4.12.3 Modo INQUIRY

Como se ha mencionado, para establecer la conexión, la unidad de *paging* debe conocer la identidad del receptor. Cuando ésta no es conocida de antemano la unidad de *paging* pasa al modo INQUIRY.

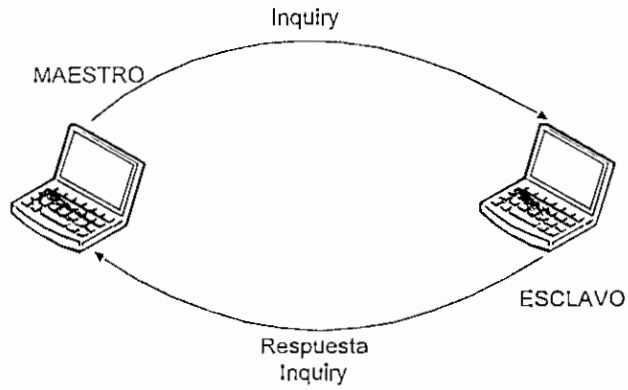



**Figura 1.13 Establecimiento de Conexiones en Modo INQUIRY**

En este modo la unidad que desea conocer las identidades de sus vecinos (unidad de *inquiry*) envía un código de acceso reservado en el estándar para el *Inquiry*, en una secuencia de 32 saltos también reservada en el estándar. Este

proceso se efectúa de la misma manera que la combinación SCAN-PAGE, pero de período 2,56 (s).

Cuando una unidad recibe un mensaje INQUIRY contesta mediante un paquete FHS. Para el retorno del paquete FHS se sigue un mecanismo de tiempo aleatorio de respuesta para prevenir que se produzcan colisiones. Luego de la respuesta la unidad entra al modo SCAN.

### 1.4.13 ARQUITECTURA GENERAL DE *BLUETOOTH*

El sistema *Bluetooth* emplea el método de acceso *time-slotted.* Un paquete puede usar hasta cinco *slots* pero debe tener un *slot* menos. En *Bluetooth* se puede transportar un canal de datos asincrónico, hasta tres canales simultáneos de voz, o un canal que simultáneamente soporte datos asincrónicos y voz sincrónica.

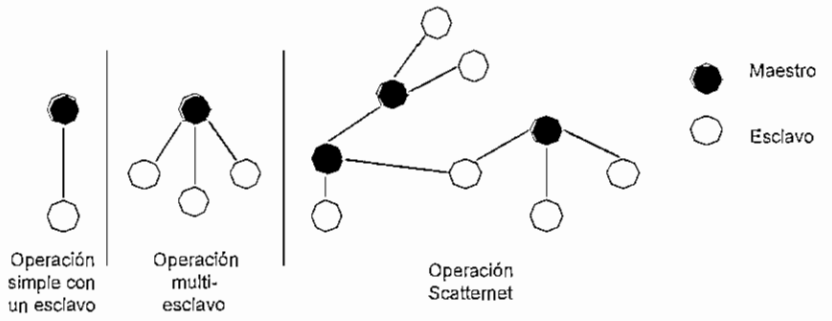



**Figura 1.14 Conexiones entre estaciones *Bluetooth*[36]**

Los diferentes tipos de enlaces soportados por *Bluetooth* son:

- Un enlace de 64-Kbps en cada dirección para un canal de voz,
- Un máximo de 723.2 Kbps asimétricos en una dirección (hasta 57.6 Kbps en dirección de retorno) o 433.9 Kbps simétricos para enlaces asimétricos.

La originalidad de *Bluetooth* procede de su arquitectura. Aunque *Bluetooth* no corresponda exactamente con el modelo de interconexión de sistemas abiertos

[36] MAYNÉ, Jordy, Estado Actual de las Comunicaciones Inalámbricas; año 2005.

OSI, una comparación entre los dos permite comprender mejor la división de responsabilidades dentro de la pila de protocolos *Bluetooth*. (Figura 1.18)

**Nivel Físico.** Responsable de la interfaz eléctrica con el medio de comunicación, incluyendo la modulación y la codificación de canal. *Bluetooth* lleva a cabo esta función a través de sus protocolos de banda base y de radio.

**Nivel de Enlace de Datos.** Proporciona los mecanismos de transmisión, *framing* y control de errores a través de un enlace determinado. En *Bluetooth*, esta función es gestionada por el protocolo de control de enlace, que lleva a cabo esta tarea, incluyendo la comprobación y corrección de errores.

**Nivel de Red.** Controla la transferencia de datos a través de la red, independientemente del medio físico y de la topología de red. Con el protocolo *Bluetooth*, la parte superior del controlador de enlace y una parte del gestor de enlace (LM, *Link Manager*) se encargan de estas responsabilidades de establecer y mantener múltiples enlaces.

**Nivel de Transporte.** Controla la multiplexación de los datos transferidos a través de la red y, por tanto, se solapa con la parte superior del LM y de la interfaz controladora de *host* (HCI, *Host Controler Interface*), que proporciona los mecanismos prácticos de transporte.

**Nivel de Sesión.** Proporciona los servicios de control de flujo de datos y de gestión que están cubiertos por el protocolo de adaptación y control del enlace lógico (L2CAP, *Logical Link Control and Adaptation Protocol*) y la parte inferior de RFCOMM/SDP[37].

**Nivel de Aplicación.** Responsable de gestionar las comunicaciones entre aplicaciones de las máquinas *host*.

La Figura 1.15 muestra la correspondencia entre la pila de Protocolo *Bluetooth* y el Modelo OSI.

[37] Protocolo de Reemplazo de Cable / SDP

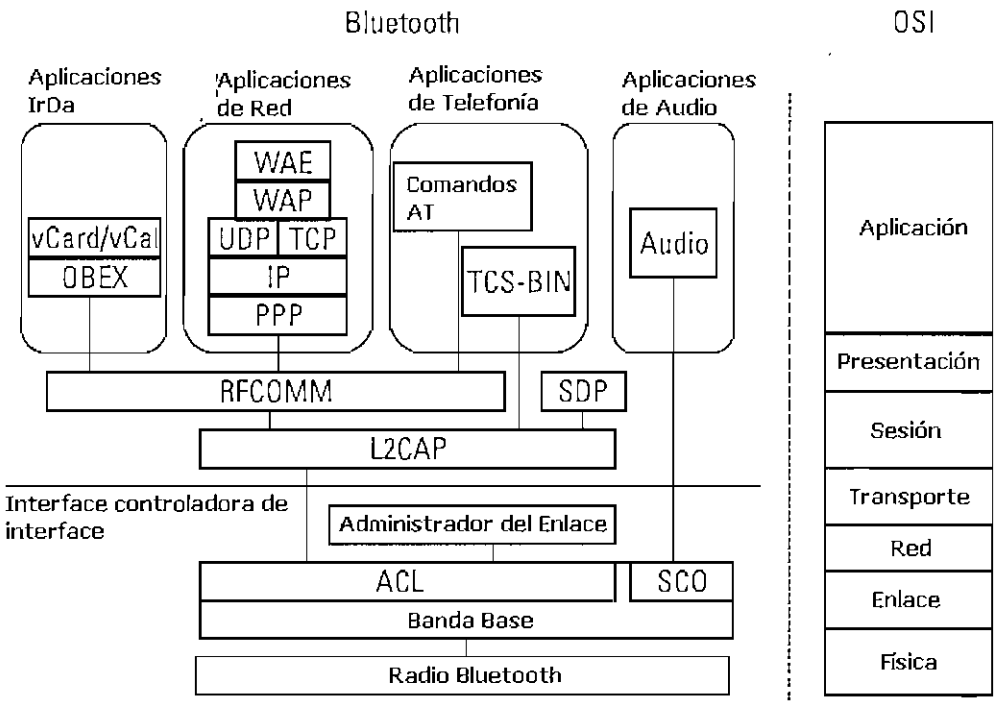



**Figura 1.15 Correspondencia entre *Bluetooth* y OSI**[38]

### 1.4.13.1 Paquetes

La composición general de un paquete para un canal de Picored se muestra en la Figura 1.16. Los paquetes son constituidos únicamente por código de acceso, o encabezado-código de acceso o datos-encabezado-código de acceso.

El código de acceso es usado para sincronización, compensación *dc offset*, identificación, *paging*, y procedimientos de *inquiry*. Éste siempre usa un preámbulo y a veces un trailer para propósitos de sincronización.

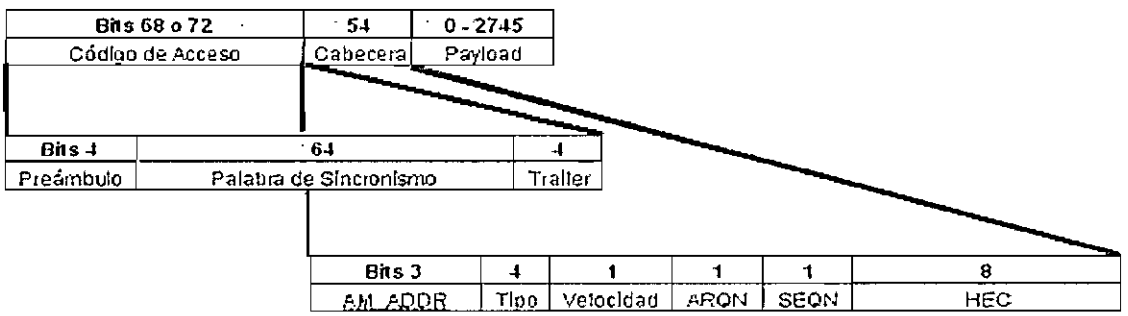



**Figura 1.16 Formato general de un paquete *Bluetooth***[39]

[38] ILYAS Mohammad, *Ad Hoc Wireless Networks*, 2004

El encabezado contiene información de control del enlace e incluye la dirección de destino, la indicación de uno de los 16 tipos de paquetes, información de control de flujo, indicación de ACK, y el HEC (*Header Error Check).*

Muchos formatos de datos son definidos, pero se identifican dos principalmente:

1. El campo de voz (sincrónico) con la fijación de longitud donde no hay encabezado.
2. El campo de datos (asincrónico), el cual consiste de tres subcampos: un encabezado de datos, un campo de datos, y posiblemente un código CRC.

Los paquetes ACL tienen únicamente el campo de datos, mientras que los paquetes SCO pueden contener únicamente el campo de voz o tener ambos.

Finalmente, es posible distinguir un grupo común de paquetes para ambos enlaces ACL y SCO y definir los paquetes para cada uno de ellos.

Los procesos de *bitstream*[40], contienen el encabezado de paquete y los datos ambos para transmisión y recepción, y son descritos en la Figura 1.16, donde algunos bloques son opcionales, dependiendo del tipo de paquete.

### 1.4.13.2 Sincronización Maestro/Esclavo

El reloj del maestro sincroniza la correspondiente picored, siguiendo una indicación desde el maestro, todos los esclavos deberán ajustar su sistema de reloj, esta información es contenida en los paquetes transmitidos. El mecanismo hace que un esclavo siempre siga al maestro. Se utiliza 28 bits contadores donde el LSB está en unidades de 312.5 µs.

En particular, una unidad de *Bluetooth* puede usar tres relojes:

- Reloj Nativo (CLKN *Native clock*).
- Reloj Estimado (CLKE *Estimated clock*).
- Reloj Maestro (*CLK Master clock*).

---

[39] IEEE 802.15.1, Agosto 2002.
[40] Flujo de bits

### 1.4.14 CANALES LÓGICOS

Las especificaciones *Bluetooth* definen dos canales lógicos:

1. **Canal de control de Enlace**. *(LC Link Control channel)*: lleva bajo nivel de información de control como ARQ, control de flujo, y la caracterización de los datos.

   Éste es el único canal lógico mapeado sobre el encabezado de paquete.

2. **Canal de Control de Administración de Enlace**. *(LM Link Manager Control channel:* lleva la información de intercambio de control entre los enlaces administradores del maestro y el esclavo(s) y es mapeado sobre los datos.

El sistema *Bluetooth* define además tres canales de usuario para el envío y recepción de datos, los cuales son:

1. **Canal de usuario UA** *(User Asynchronous):* tiene los datos de usuario L2CAP, los cuales pueden ser segmentados en uno o más paquetes en banda base y son mapeados en los datos.
2. **Canal de Usuario UI** *(User Isochronous):* tiene los datos que son soportados por los paquetes propietarios de inicio de *timing* en alto nivel y son mapeados sobre los datos.
3. **Canal de Usuario US** *(User Synchronous):* es únicamente llevado sobre el enlace SCO y mapeado sobre los datos.

## 1.5 ESTUDIO DEL PROTOCOLO IEEE 802.15.4 "*ZIGBEE*" Y SU APLICACIÓN A REDES DE SENSORES INALÁMBRICOS[41]

### 1.5.1 INTRODUCCIÓN A 802.15.4 *ZIGBEE*

Las características que hacen importante a este estándar son, su flexibilidad de red, bajos costos, y bajo consumo de energía; es ideal para aplicaciones en el

[41] http://www.zigbee.org; NAEVE Marco, IEEE 802.15.4 *MAC Overview*, Eaton Corporation, 2004.

hogar o en lugares que requieran una tasa de transmisión de datos relativamente baja.

Se considera un tensiómetro pequeño en una clínica. Este sensor no necesita reportar sus datos más que unas pocas veces por hora, es discreto y tiene un precio razonable.

Este tipo de aplicaciones se manejarían adecuadamente con un link de comunicación inalámbrica de baja potencia. El uso de cables de comunicaciones o de energía, es impráctico, ya que implicaría serias molestias tanto al paciente como al personal médico.

En el año 2000 dos grupos especialistas en estándares (*ZigBee* y el grupo 15 de trabajo IEEE 802) se unieron para dar a conocer la necesidad de un nuevo estándar para redes inalámbricas de baja potencia y por lo tanto bajos costos en ambientes industriales y caseros.

El resultado de estos estudios, dio sus primeros frutos para diciembre de ese año, formándose un comité para nuevos estándares IEEE (*NesCom*), él cual escogiera oficialmente un grupo de trabajo para el desarrollo de un nuevo estándar de baja transmisión en redes inalámbricas para áreas personales (LR-WPAN), lo que originó el estándar que ahora se conoce como el IEEE 802.15.4, llamado *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).*

Las características de mayor relevancia del estándar se resumen en la Tabla 1.5.

| Propiedad | Rango |
|---|---|
| Rango de transmisión de datos | 868 MHz: 20 kbps; 915 MHz: 40 kbps; 2.4 GHz: 250 kbps |
| Alcance | 10 – 20 m |
| Latencia | Bajo de 15 ms |
| Canales | 869/915 MHz: 11 canales.<br>2.4 Ghz: 16 canales. |
| Bandas de frecuencia | PHY: 869/915 MHz y 2.4 GHz. |
| Direccionamiento | Cortos de 8 bits o 64 bits IEEE |
| Método de acceso al Canal | CSMA - CA |

**Tabla 1.5 Características de IEEE 802.15.4**

Su arquitectura se presenta en la siguiente figura.

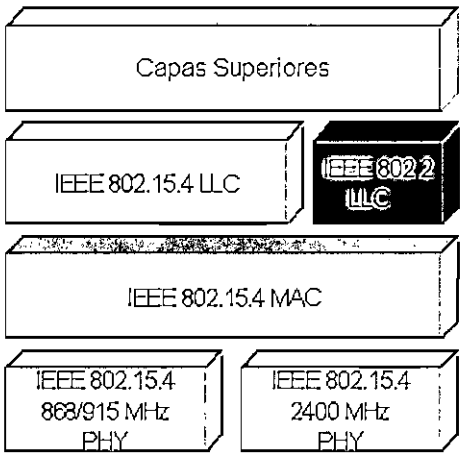



**Figura 1.17 Arquitectura de IEEE 802.15.4**

### 1.5.2 CAPA FÍSICA

Se encarga de las siguientes funciones:

- Activación y desactivación del transmisor RF.
- Detección de la energía dentro del canal presente.
- Indicar la calidad de los enlaces de los paquetes recibidos.
- Evaluación de la calidad de canal para CSMA-CA.
- Selección de canal libre.
- Transmisión y recepción de datos.

Este estándar se encuentra definido en 3 bandas de frecuencias, y cada una de ellas tiene distintas características, tanto de modulación como de canales de transmisión. Las Bandas de frecuencias en las cuales está definido este estándar se muestran en la Tabla 1.6.

| Banda | Velocidad por bit | Velocidad por símbolo | Canales disponibles | DSSS | |
|---|---|---|---|---|---|
| | | | | Modulación | Velocidad por Chip |
| 816 MHz | 20 kbps | 20 ksymbol/s | 1 | BPSK | 300 kchip/s |
| 915 MHz | 40 kbps | 40 ksymbol/s | 10 | BPSK | 600 kchip/s |
| 2,4 GHz | 250 kbps | 62,5 ksymbol/s | 16 | O-QPSK | 2 Mchip/s |

**Tabla 1.6 Bandas de Frecuencia para IEEE 802.15.4**

### 1.5.2.1 Especificaciones de Servicio de Capa Física

La capa física provee un interfaz entre la subcapa MAC y el medio de transmisión físico. Incluye una entidad de administración llamada PLME[42], la cual provee el interfaz a través del cual pueden invocarse las funciones de administración de capa.

La PLME también es responsable de mantener una base de datos de los objetos manejados pertenecientes a la capa física. Esta base de datos es llamada Base de Información PHY PAN (PIB *PHY PAN Information Base*).

La PHY proporciona dos servicios, accedidos a través de dos puntos de acceso al servicio (SAP *Service Access Point*): los servicios de datos de capa física (PD-SAP *PHY Data SAP*) y los servicios de administración de capa física (PLMESAP).

La descripción del modelo de referencia de la capa física se resume en la Fig. 1.18.

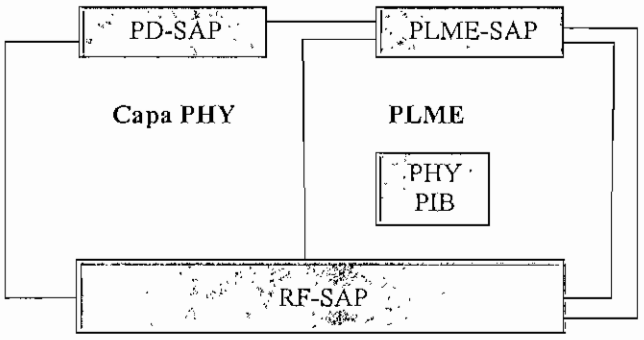



**Figura 1.18 Modelo de Referencia de Capa Física**

El PD-SAP soporta el transporte de MPDUs entre entidades correspondientes de la subcapa MAC.

La Tabla 1.7 lista las primitivas soportadas por el PD-SAP.

| Primitivas PD-SAP | *Request* | *Confirm* | *Indication* |
|---|---|---|---|

**Tabla 1.7 Primitivas de PD - SAP**

[42] *Physical Layer Management Entity*

### 1.5.2.2 Formato de la Trama PPDU

Por conveniencia, la estructura de la trama PPDU[43] se presenta para que los bits más significativos se transmitan o reciban primero. El mismo orden de transmisión debe aplicarse a los campos de datos transferidos entre la PHY y la subcapa MAC.

Cada paquete PPDU consta de los siguientes campos:

- Una cabecera de sincronización (SHR *Sync Header*), que permite a un dispositivo receptor volver a sincronizar la transmisión.
- Una cabecera de preámbulo (PHR *Preamble Header*), que contiene la información de longitud de trama.
- Datos de longitud variable, que llevan la trama de la subcapa MAC.

El formato general de la trama o paquete PPDU se detalla a continuación.

| Preámbulo | SFD | Longitud | Reservado | PSDU |
|---|---|---|---|---|
| 32 bits | 8 bits | 7 bits | 1 bit | Variable |
| SHR | | PHR | | Datos |

**Figura 1.19 Formato de PPDU**

- Preámbulo: este campo es usado por el transmisor para obtener un chip y un símbolo de sincronización con un mensaje de llegada. Está compuesto por 32 bits.
- SFD (*Start Frame Delimited*): el campo de delimitación de inicio de trama está compuesto por 8 bits, los cuales indican la terminación del campo de sincronismo y el inicio del paquete de datos.

  El formato de este campo se ilustra en la Figura 1.20.

| Bits: 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |

**Figura 1.20 Formato del campo SFD**

[43] *PHY Protocol Data Unit*

- Longitud: está compuesto por 7 bits, especifica el número de octetos contenidos en el *payload*. Tiene un valor entre 0 y 127 octetos.

  La Tabla 1.8 resume los tipos *de payload* versus la longitud de trama.

| Valores de Longitud de trama | Payload |
|---|---|
| 0 - 4 | Reservado |
| 5 | MPDU (ACK) |
| 6 -7 | Reservado |
| 8 a MPPS (*MaxPHYPacketSize*) | MPDU |

**Tabla 1.8 Valores de Longitud de Trama**

- PSDU: es de longitud variable y lleva los datos de la capa física. Para los tipos de longitud de trama 5 y el mayor tamaño permitido, la trama PSDU contiene la trama de la subcapa MAC.

### 1.5.2.3 Atributos PHY PIB (PAN *Information Base*)

La PHY PIB comprende los atributos necesarios para la administración de la capa física de un dispositivo. Cada uno de estos atributos pueden ser leídos o escritos empleando las primitivas *PLME–GET.request* y *PLME–SET.request*, respectivamente. Los atributos contenidos en la PHY PIB se presentan en la Tabla 1.9.

| Atributo | Identificador | Tipo | Rango | Descripción |
|---|---|---|---|---|
| phyCurrentChannel | 0 x 00 | Entero | 0 - 26 | Designa el canal RF a usar para todas las Tx y Rx. |
| phyChannelsSupported | 0 x 01 | Bitmap | | Los 5 bits mas significados se setean a cero y los 27 bits menos significativos indican el estado de los 27 canales válidos (1=disponible). |
| phyTransmitPower | 0 x 02 | Bitmap | 0 x 00 – 0xbf | Los 2 bits más significativos representan la tolerancia de la potencia del transmisor:<br>00 = ± 1 dB<br>01 = ± 3 dB<br>10 = ± 6 dB |
| phyCCAMode | 0 x 03 | Entero | 1 - 3 | Modo CCA |

**Tabla 1.9 Atributos de la PHY - PIB**[44]

[44] Estándar IEEE 802.15.4

### 1.5.3 BANDA DE 2.4 GHZ

Para esta banda de frecuencia la velocidad de transferencia de datos máxima es de 250 Kbps; para esto se modula la portadora con la técnica O-QPSK, en conjunto con DSSS.

El esquema de bloques de cómo se envían los datos que vienen en formato PPDU se muestra en la Figura 1.21.

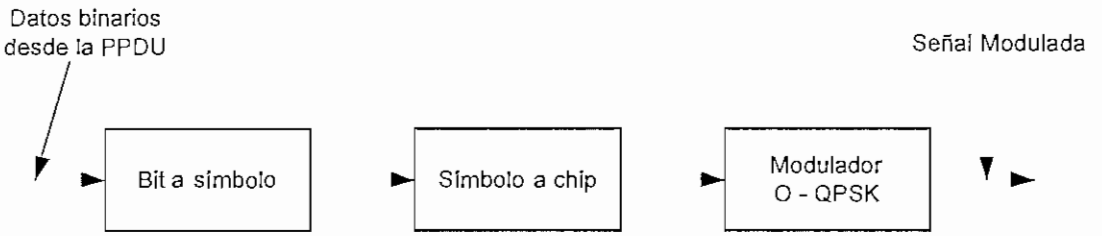



**Figura 1.21 Funciones de modulación y propagación**

Aquí se usa una secuencia pseudo-aleatoria de 32 chips para representar símbolos de 4 bits, la misma que está dividida en dos partes, la primera desde el 0-7 representan cambios cíclicos en múltiplos de 4 chips, mientras que del 8 al 15 son iguales pero usando una secuencia que es la combinación de los chips.

En el Anexo 1B se incluye la tabla de mapeo de símbolos a chips y la descripción de la modulación O-QPSK.

### 1.5.4 BANDA DE 816/915 MHz

Estas dos bandas utilizan el mismo sistema de modulación, la única diferencia es el número de canales que cada banda soporta.

Como se observó en la Tabla 1.6 de la banda de 816 MHz posee un canal y la banda de 915 MHz posee 10 canales. En estas bandas la capa física especifica el DSSS empleando modulación BPSK y los datos se codificarán en forma diferencial.

El diagrama de bloques de este proceso se muestra en la Figura 1.22.

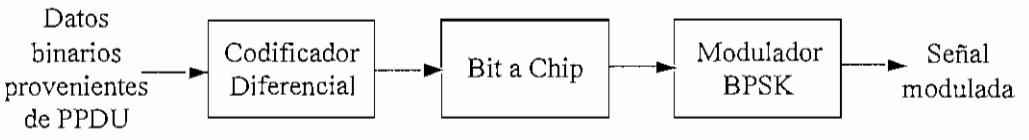



**Figura 1.22 Funciones de modulación y propagación.**

### 1.5.5 CAPA DE ENLACE DE DATOS

Esta capa se compone de dos subcapas, la subcapa MAC y la subcapa LLC.

La función de la capa MAC es proveer control de acceso al medio compartido y cumplir con las siguientes tareas:

- Generar el *beacon* de red si el dispositivo es un coordinador.
- Sincronizar a los *beacons*.
- Soporte de asociación y desasociación PAN.
- Soporta dispositivos de seguridad.
- Ocupa CSMA-CA para el acceso a los canales.
- Maneja y mantiene el mecanismo GTS (*Guaranteed Time Slot*).
- Provee una comunicación confiable entre dos pares de entidades MAC.

Este modelo difiere del modelo ISO/OSI en la capa física y MAC pero la sub-capa LLC puede ser la misma que se define en el estándar IEEE 802.2, como también se define una interfaz para poder introducir otra capa LLC que sea mas apropiado para medios inalámbricos.

### 1.5.6 TOPOLOGÍAS DE RED

La capa MAC provee aplicaciones de soporte para la creación de dos topologías de red. Estas topologías son estrella y punto a punto.

#### 1.5.6.1 Topología Estrella

Esta topología está enfocada en cubrir el segmento de aplicaciones hogareñas. Está conformada por un único coordinador PAN, el cual opera como maestro de red y se encarga de enviar los *beacon* para la sincronización de dispositivos

(Incluyendo el control de la supertrama) y para la guarda de la administración de asociación.

La forma de comunicación entre los distintos dispositivos se ilustra en la Figura 1.23, en la cual se ve la existencia de los dispositivos FFD (*Full Function Device*) y RFD (*Reduce Function Device*).

Los FFD son dispositivos que poseen toda la implementación del protocolo 802.15.4 los cuales, entre otras cualidades, pueden transformarse en los coordinadores de una PAN.

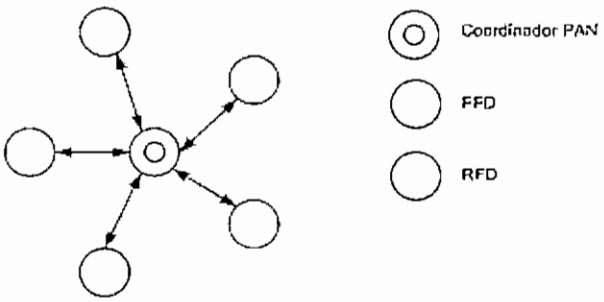



**Figura 1.23 Topología estrella**

Los RFD son dispositivos los cuales no poseen la implementación completa del protocolo, solo las partes importante, estos dispositivos son generalmente puntos finales de red y no pueden convertirse en coordinadores de una PAN.

Después de que un FFD es activado por primera vez, éste debe establecer su propia red y convertirse en el coordinador de la PAN. Debido a que cada red de estrella funciona en forma independiente de las otras redes estrella vecinas, se debe escoger un identificador de PAN, el cual no deberá ser usado por ninguna otra red dentro del área de cobertura.

Luego de que el identificador de red este determinado, el coordinador PAN debe permitir la incorporación de más dispositivos a la red indistintamente de si son FFD o RFD, este procedimiento lo hace enviando *beacons* y asociando a los dispositivos que respondan.

### 1.5.6.2 Topología Punto a Punto

Esta topología está enfocada al campo industrial y su principal característica es que los dispositivos FFD pueden comunicarse entre ellos sin pasar por un nodo central, además se pueden comunicar nodos que estén fuera del rango de cobertura física a través de cualquier otro dispositivo que se encuentre en medio de ellos por medio de un mensaje multi-salto.

La implementación de esta topología permite la formación de redes más complejas que permitan *ad hoc*, auto-organización y sean a prueba de fallas; el protocolo IEEE 802.15.4 no especifica los detalles de ninguna de estas redes, pero si se definen las funciones que tiene la capa MAC para poder permitir que éstas se formen. Un ejemplo de esta red se ve en la Figura 1.24.

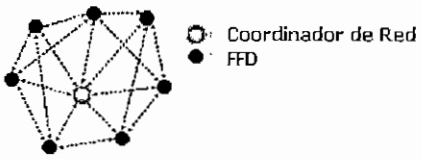



**Figura 1.24 Topología peer to peer**

Si bien en esta topología pueden existir dispositivos RDF, éstos son solo periféricos, ya que carecen de la capacidad para poder repetir paquetes.

Para poder mejorar el área de cobertura se puede implementar un tipo especial de red punto a punto, una red de grupo de árboles (*cluster-tree*); en esta red existen varios coordinadores de red, uno por cada grupo, los cuales son llamados cabeza de grupo (*cluster heads*) y un coordinador central llamado coordinador PAN (Figura 1.25).

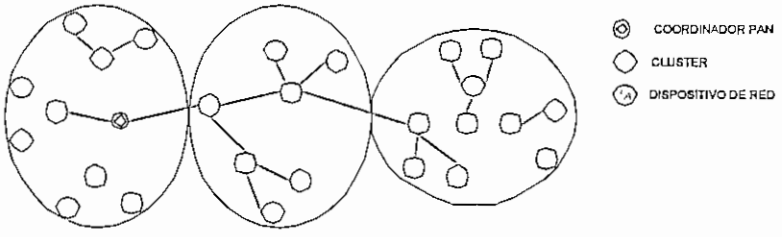



**Figura 1.25 Árbol de Cluster**

### 1.5.7 ESTRUCTURA DE LA SUPERTRAMA

La implementación de esta trama es opcional, la cual es manejada por el coordinador PAN y está definida por los mensajes *beacon* los cuales se programan para que sean enviados en intervalos regulares.

Cada *beacon* contiene la información necesaria para poder ayudar a los dispositivos de red a sincronizarse. Ésta contiene información como identificador de red, periodo de *beacon* y la estructura de la supertrama.

Cada supertrama está constituida por 16 *slots,* el primer *slot* de tiempo empieza y termina con una trama de *beacon* (Figura 1.26).

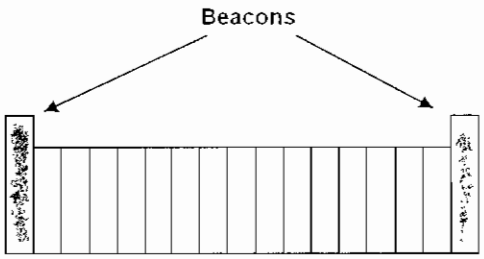



**Figura 1.26 Estructura genérica de supertrama**

Para que la comunicación entre un dispositivo y el coordinador PAN tenga éxito el dispositivo deberá intentar comunicarse entre dos tramas de *beacon* sucesivas. A este periodo de tiempo se le denomina Período de Acceso por Contención (CAP *Contention Access Period*). Para poder acceder al canal se debe utilizar CSMA-CA.

Además, el coordinador PAN puede asignar espacios de la supertrama dedicados a un dispositivo de red específico. A este segmento se le llama Periodos de Guarda (GTSs *Guaranteed Time Slots* Figura 1.27). Esto es útil para aplicaciones que requieran determinados anchos de banda y de latencia.

Dentro de la trama ahora se define un nuevo periodo de tiempo, llamado Período libre de Contención (CFP *Contention Free Period*), que son los *slots* de tiempo reservados para cada dispositivo.

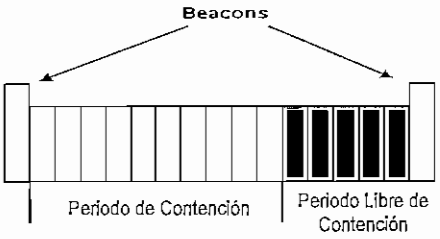



**Figura 1.27 Estructura de supertrama con GTSs**

Debido a que el medio de transmisión de los datos es inalámbrico, se debe implementar medidas para minimizar la pérdida de datos, por ello el protocolo define que para enviar información se debe usar CSMA-CA, como comprobador de integridad de trama en caso de que la información sea alterada.

### 1.5.8 ESTRUCTURA DE LA TRAMA MAC

Esta estructura se diseñó pensando en la simplicidad y flexibilidad que le debía proveer al protocolo. Ésta está constituida por 3 elementos (Figura 1.28):

- **Cabecera**: este elemento contienen el campo de control y el campo de direccionamiento. El campo de control indica el tipo de trama, seguridad empleada, y el formato y contenido del campo de direccionamiento. Éste también indica si es requerido un *Acknowledgment* por un receptor. El campo de direccionamiento contiene la fuente y el destino del paquete indicado en el campo de control.

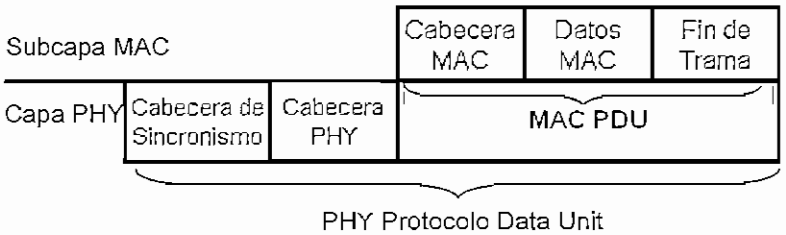



**Figura 1.28 Estructura básica de la trama MAC**

- **Carga de longitud variable**: este campo contienen la información especificada por el tipo de transacción y por la MAC; puede ser dividido en forma lógica para su uso por las capas superiores.

- **Trailer o Cola**: esta trama contiene 16 bits de verificación (FCS) basado en el estándar ITU-T 16 bits CRC.[45]

Cuando la trama MAC es ensamblada dentro de un paquete de la capa física este es llamado *MAC Protocol Data Unit* (MPDU).

Dentro del protocolo 802.15.4 se definen cuatro tipos de tramas MAC: *Beacon*, Datos, *Acknowledgment*, MAC control.

### 1.5.8.1 Trama de *Beacon*

Solo está disponible en redes que lo tengan habilitado. Aquí el campo de direcciones contiene la identificación de la PAN fuente y la dirección del dispositivo fuente.

El campo de *Payload* se divide en 4 secciones, las cuales se describen a continuación (Figura 1.29):

- **Campo de Especificación de Supertrama (*Superframe Specification*)**: contiene los datos que especifica a la supertrama.
- **Campo de Especificación de Direcciones en Trámite (*Pending Address Specification*)**: contienen el número y tipo de direcciones especificadas en *Address List*.
- **Campo de Lista de Direcciones (*Address List*)**: contiene la lista de las direcciones de los dispositivos disponibles en el coordinador PAN.
- **Campo *Beacon Payload***: es opcional y contiene datos de *broadcast*, de los dispositivos pertenecientes a la red en el radio de cobertura.

| Cabecera MAC | | | Datos MAC | | | | Fin Trama |
|---|---|---|---|---|---|---|---|
| Bits 16 | 8 | 40 | 16 | Variable | Variable | Variable | 16 |
| Control de Trama | # Secuencia | Campo Direccionamiento | Especificación Supertrama | Campo GTS | Direcciones Pendientes | Datos *Beacon* | FCS |

**Figura 1.29 Trama de *Beacon*[46]**

[45] Código de Redundancia Cíclica

### 1.5.8.2 Trama de Datos

Se utiliza para enviar datos, y el campo de direcciones contendrá la identificación de la PAN y del dispositivo, que sea fuente y/o destino (Figura 1.30).

| Cabecera MAC | | | Datos MAC | Fin Trama |
|---|---|---|---|---|
| Bits 16 | 8 | 32 a 160 | Variable | 16 |
| Control de Trama | # Secuencia | Campo Direccionamiento | Datos | FCS |

Figura 1.30 Trama de Datos

### 1.5.8.3 Trama *Acknowledgment*

Se envía como confirmación de los datos recibidos y se evalúa su FCS. Los campos de *Addressing Field* del MAC *Headers* no contienen datos, de igual forma que MAC *Payload*. Cuando se recibe un paquete *acknowledgment* se verifica si se esperaba alguno, y si corresponde a alguno de ellos. De lo contrario esta trama se descarta.

| Cabecera MAC | | Datos MAC | Fin Trama |
|---|---|---|---|
| Bits 16 | 8 | | 16 |
| Control de Trama | # Secuencia | | FCS |

Figura 1.31 Trama *Acknowledgment*

## 1.6 TIPOS DE SENSORES[47]

Un sensor es un dispositivo sensible que utiliza un fenómeno físico o químico dependiente de la naturaleza y el valor de la magnitud físico química a medir, lo cual permite la transducción del estímulo a una señal utilizada directa o indirectamente como medida. Previo a definir la clasificación de los sensores, se debe tener un panorama claro de los parámetros de selección de ellos, en base a los requerimientos del proyecto a desarrollar y su funcionalidad.

[46] IEEE 802.15.4, Octubre del 2003.
[47] CALLAWAY Edgar, *Wireless Sensor Networks: Architectures and Protocols*, 2004.

## 1.6.1 CRITERIOS GENERALES DE UNA RED DE SENSORES[48]

### 1.6.1.1 Elementos

Una red de sensores incluye los siguientes elementos:

- **SENSORES**: de distinta naturaleza y tecnología, toman del medio la información y la convierten en señales eléctricas.
- **NODOS SENSOR**: o procesadores de radio, toman los datos del sensor a través de sus puertas de datos, y envían dicha información a la estación base.
- **ESTACIÓN BASE**: recolector de datos basado en un ordenador común o sistema embebido.
- **GATEWAY**: elementos para la interconexión entre la red de sensores y una red TCP/IP.

### 1.6.1.2 Ambientes de Funcionamiento

Las principales aplicaciones para una WSN[49] son las siguientes:

- **Monitorización del Entorno:** aplicación donde se desea recoger lecturas de un entorno inaccesible y hostil en un período de tiempo para detectar cambios, tendencias, etc.
  Se tiene gran número de nodos sincronizados midiendo y transmitiendo periódicamente. Requiere sincronización precisa, y define topología física relativamente estable; además no necesita reconfiguración de la red frecuente. Ej.: control de agricultura, microclimas, monitoreo habitual de pacientes, etc.

- **Monitorización de Seguridad:** aplicación para detección de anomalías o ataques en entornos monitorizados continuamente por sensores. Los nodos no están continuamente enviando datos (*REPORT BY EXCEPTION*), por lo cual tienen menor consumo de energía.

---

[48] ESCOLAR, Ma. Soledad; *Wireless Sensor Networks*, Estado del Arte e Investigación.
[49] *Wireless Sensor Network*

Es de vital importancia el estado del nodo, y mantener una baja latencia en las comunicaciones. Ej.: control de edificios inteligentes, detección de incendios, aplicaciones militares, monitoreo de pacientes en estado crítico, etc.

- ***Tracking***: aplicación para controlar objetos que están *etiquetados* con nodos sensores en una región determinada.
  A diferencia del resto, la topología de la red es muy dinámica, debido al continuo movimiento de los nodos sensores, por lo que la WSN debe ser capaz de descubrir nuevos nodos y formar nuevas topologías.

- **Redes Híbridas**: en general, los escenarios de aplicación contienen aspectos de las tres categorías anteriores.

### 1.6.1.3 Estados en una Red de Sensores

Es de vital importancia conocer los estados por los que atraviesa un sensor, para en base a ello, determinar su ambiente de trabajo. Dichos estados son:

- *Sleep*: la mayor parte del tiempo.
- *Wakeup*: proceso de adquisición y transmisión de datos.
- *Active*: mínimo período de tiempo de trabajo y retorno inmediato al estado *sleep*.

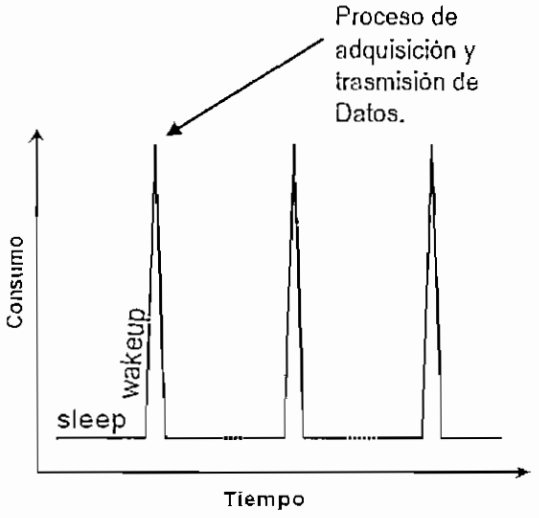



Figura 1.32 Estados de un nodo sensor.

#### 1.6.1.4 Parámetros de Diseño

Los principales problemas que implica la utilización de este tipo de redes, son:

- Optimización del consumo de energía en los nodos para lograr el máximo tiempo de vida de la red. El CPU debe ser capaz de quedar en estado "*sleep*" mientras "no tenga nada que hacer".
- Ancho de banda y cobertura de la red limitados.
- Recursos de computación limitados: memoria y CPU.
- Soluciones *ad-hoc* para redes *ad-hoc*.
- Topología muy dinámica de la red: elementos móviles, nodos con alta probabilidad de fallo y nodos que entran en el sistema.

La clasificación de los sensores es variada, dependiendo del punto de vista en que se los estudie. Para este proyecto se profundiza en la clasificación en base a los sensores inalámbricos, sin embargo la clasificación general de los sensores es la siguiente.

### 1.6.2 SENSORES DE CONTROL INDUSTRIAL Y MONITOREO

Los sensores inalámbricos para la industria tienen su aplicación en seguridad, estos sensores se pueden emplear para identificar la presencia de materiales peligrosos, permitiendo una rápida detección e identificación de agentes químicos o biológicos antes de que puedan realizar daños serios.

Las redes inalámbricas de sensores pueden emplear rutinas con algoritmos distribuidos, tener múltiples direcciones para poder realizar el monitoreo en varios sitios. En muchas aplicaciones los sensores inalámbricos son frecuentemente imprácticos, no obstante, pueden ser muy importantes para el monitoreo de la temperatura, vibración, lubricación, etc.

Otra aplicación en esta área de sensores inalámbricos son los sistemas HVAC (*Heating, Ventilating, and Air Conditioning*), que son controlados por un pequeño número de sensores de temperatura y humedad localizados estratégicamente. Los sistemas HVAC tienen otras ventajas, sirven también para el *monitoreo* de

áreas de vivienda, monitoreo de ductos para el cambio de dispositivos que pueden estar en mal estado. Por lo tanto, este tipo de sensores pueden dar un beneficio tanto a corto como a largo plazo y evitando catástrofes y pérdidas económicas.

### 1.6.3 SENSORES DE AUTOMATIZACIÓN EN EL HOGAR Y EQUIPOS ELECTRÓNICOS

Los sensores inalámbricos tienen una gran aplicación en el hogar. Muchas de las aplicaciones de la industria son descritas paralelamente a las aplicaciones en el hogar.

Una de estas aplicaciones es el control remoto "universal", que es un asistente digital personal tipo dispositivo PDA que puede controlar no únicamente la televisión, DVD *player*, estéreo, y otro tipo de equipos electrónicos. También las luces y cortinas pueden ser controladas con una red de sensores inalámbricos. Con el control remoto universal, uno puede controlar la casa con el confort y la tranquilidad que da este tipo de solución.

Otra mejora es la extensión a la aplicación en el hogar que es dada por *Remote Keyless Entry* (RKE) que funciona en los automóviles. Con la red de sensores, puertas y ventanas, luces, etc.; pueden ser controlados desde el automóvil y se puede tener notificaciones al usuario de cualquier tipo de cambio o problema que exista en cualquiera de estos ambientes.

### 1.6.4 SENSORES DE SEGURIDAD Y MILITAR

Los sistemas inalámbricos de seguridad son basados en los sistemas del hogar y pueden ser usados en aplicaciones de seguridad industrial. Estos sistemas, emplean protocolos de comunicación propietarios que han existido por muchos años. Como en muchas tecnologías, muchos de los propósitos del uso de los sensores inalámbricos fueron para aplicaciones militares.

Uno de los grandes beneficios de usar estos sensores es que se los puede usar para remplazar a guardias y controlar los perímetros de defensa. Estos sensores

pueden también ser utilizados para monitorear las minas, sin tener presente al personal en el sitio de la batalla o conflicto. Otro uso es para identificar localizaciones de potencial ataque, pueden ser equipados en micrófonos acústicos, sensores sísmicos de vibración, sensores magnéticos, radares, etc.

Estos sensores pueden ser pequeños, y pueden camuflarse fácilmente en rocas, árboles, etc. Tienen control distribuido y algoritmos de encaminamiento (sin puntos de falla), que los hace resistentes y difíciles de destruir en batalla. El uso de técnicas de espectro expandido combinado con la transmisión de ráfagas optimizan la vida de la batería.

### 1.6.5 SENSORES PARA LA AGRICULTURA Y EL MEDIO AMBIENTE

Estos sensores tienen la capacidad de medir la humedad de la tierra, temperatura, la necesidad de los pesticidas, y fertilizantes, y muchas otras cualidades. Este tipo de sensores son especialmente importantes para viñeros, donde el medio ambiente es susceptible a cambios y se necesita tener un control exhaustivo del proceso.

Los sensores para la agricultura son también utilizados en sistemas de control avanzados para automatizar los equipos de agricultura.

Muchos de estos sensores son ya utilizados en los ranchos para el control de cada animal, para prevenir su pérdida y realizar un seguimiento en los tratamientos para prevenir parásitos y tenerlos en caso de las gallinas en lugares donde la temperatura es adecuada para su vida. Así, se puede controlar y monitorear tanto a los animales y plantas para prevenir pérdidas económicas.

### 1.6.6 MONITOREO DE LA SALUD

Un grupo de redes de sensores que tiene un gran potencial de crecimiento, son los sensores de cuidado médico. La salud monitoreada es generalmente definida como el monitoreo de la información de salud no crítica, para diferenciarla de la telemetría médica, aunque muchas de las definiciones son muy abiertas y no

específicas, y algunas aplicaciones de telemetría médica pueden ser consideradas para redes de sensores inalámbricos.

Existen disponibles dos clases de aplicaciones para monitoreo de estado de salud, que utilizan redes de sensores inalámbricos.

Una es para el monitoreo de rendimiento atlético que toma información de pulso y respiración de personas entrenando, para tener un control y cuidado.

La otra clase se utiliza para el monitoreo del estado de salud desde el hogar, donde pacientes pueden ser controlados, por ejemplo: el control del azúcar en la sangre de pacientes diabéticos o con desórdenes crónicos.

## 1.7 SENSORES INALÁMBRICOS PARA CUIDADO MÉDICO Y SU DISPONIBILIDAD EN EL MERCADO

Con el pasar del tiempo se ha observado que las enfermedades que padece la población, han ido aumentando, llegando a necesitar de mayores cuidados y hasta de la presencia permanente de una enfermera para cada paciente.

Las redes de sensores inalámbricos, ayudarán al personal de cuidado médico a proporcionar servicios como: monitoreo constante, mejor manejo de los datos médicos, y atención efectiva en casos de emergencia.

El uso de redes de sensores inalámbricos para monitoreo médico, espera acelerar el desarrollo de sensores biológicos, los cuales pueden descubrir enzimas, ácidos nucleicos, y otros materiales biológicamente importantes.

Es deseable que los sensores sean muy pequeños y baratos, capaces de permitir desarrollar muchas aplicaciones en el campo farmacéutico y el cuidado médico.

Los sensores inalámbricos de cuidado médico deben permitir monitorear al paciente, brindando resultados confiables, tal que se eviten complicaciones por descuidos del personal médico.

Los sistemas inalámbricos de socorro a desastres, ya están en el mercado. Las señales de respuesta en caso de avalanchas, son enviadas continuamente al equipo de rescate, de tal modo que permitan brindar ayuda a tiempo y evitar pérdidas humanas.

Los sistemas existentes aún tienen sus limitaciones, sin embargo, lo importante es que éstos proporcionan información sobre los signos vitales de la víctima.

### 1.7.1 SENSORES *ZIGBEE*

Los sensores basados en el estándar IEEE 802.15.4, son totalmente programables, autoconfigurables, e incorporan el sistema operativo *TinyOS*, sin embargo, aún están limitados energéticamente. El punto más interesante con estos sensores, quizá sea cómo conseguir programar, de forma eficiente y fiable, cientos de pequeños nodos que puedan coexistir para formar una red.

Actualmente en el mercado se cuenta con una familia de dispositivos de redes de sensores inalámbricos de bajo consumo, de los cuales una parte se encuentran en investigación y desarrollo, mientras que otra ya está disponible a la venta.

Sin embargo en el campo médico, únicamente existen prototipos demostrativos (Ej.: Proyecto *CODEBLUE*[50]), razón por la cual únicamente se mencionan las principales plataformas de desarrollo de sensores *ZigBee*.

Los sensores de mayor acogida en el mercado, son los de la plataforma denominada "Mote IV", los cuales se han utilizado tanto para evaluar algoritmos, como para monitorización y desarrollo de rastreo de objetos. El fabricante de éstos, es CHIPCOM de TEXAS INSTRUMENTS.

Otros de los fabricantes que están entrando fuertemente en el mercado, son: PANASONIC e INTEL, este último dispone actualmente de un módulo prueba de telemedicina para pacientes con *Alzheimer*.

---

[50] SHNAYDER Victor, CHEN Borrong, LORINCZ Konrad, WELSH Matt; *Sensors Networks for Medical Care*; 2005.

### 1.7.2 SENSORES *BLUETOOTH*

Debido a lo costoso que resulta emplear tecnologías inalámbricas en sensores médicos, las compañías que los elaboran, han diseñado prototipos prueba y los han puesto a la venta, siendo una de las empresas pioneras NONIN.

NONIN ha desarrollado un módulo médico, llamado AVANT 4100, el cual, permite obtener inalámbricamente los valores de medición de Pulso y Ritmo Cardíaco, a través del puerto serial.

Para realizar la transmisión de los datos obtenidos, se emplea un receptor *Bluetooth* cualquiera, y una aplicación que abra el puerto serial, obtenga los datos, y se mantenga en espera por nuevas mediciones.

A la fecha de redacción de este documento, en el mercado únicamente se ha encontrado el modulo médico tipo *Bluetooth* mencionado, sin embargo, cabe señalar que se han encontrando un sinnúmero de proyectos tipo propietario, para hospitales y centros de atención médica, que incluyen el desarrollo de sensores de medición de signos vitales, tanto en un solo equipo, como individuales.

Adicionalmente cabe notar, que en el Hospital Boston de EEUU, se ha implementado una red de prueba de sensores inalámbricos, que incluye un electrocardiógrafo tipo *Bluetooth*, y sensores de signos vitales, para llevar a cabo un proyecto piloto de telemedicina con pacientes de avanzada edad y con problemas críticos por accidentes de tránsito o de trabajo.

## 1.8 SEGURIDAD DE UNA RED[51]

La interconexión de equipos en una red, hace que la información almacenada y que se transmite esté sujeta a ataques dentro y fuera de una organización.

Cuanto más grande es una empresa[52], más importante es la necesidad del establecimiento de la seguridad en la red y en los datos, por tanto se deben

[51] http://fmc.axarnet.es/redes/tema_10_m.htm
[52] http://www.zonagratuita.com/servicios/seguridad/wireles.html

establecer políticas de seguridad que abarquen desde el mantenimiento del entorno físico apropiado hasta la seguridad de la información enviada en la red.

### 1.8.1 IMPLANTACIÓN DE LA SEGURIDAD EN REDES

La planificación de la seguridad es un elemento importante en el diseño de una red. Es mucho más sencillo implementar una red segura a partir de un plan, que recuperar los datos perdidos.

Para la implantación de los mecanismos de seguridad, se debe considerar principalmente, el grado de importancia de la información circulando por la red y los recursos disponibles para protegerla.

### 1.8.2 PLANIFICACIÓN DE LA SEGURIDAD DE LA RED

En una red no solo debe asegurarse la privacidad de los datos más importantes para la organización, sino también se debe proteger las operaciones no intencionadas o deliberadas que pueden causar daño en la misma.

El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear este equilibrio.

Las cuatro amenazas principales que afectan a la seguridad de los datos en una red son: acceso no autorizado, soborno electrónico, robo y daño intencionado o no intencionado.

La tarea del administrador es asegurar que la red se mantenga fiable y segura. En definitiva, proteger y dar soluciones de seguridad a estas posibles amenazas.

### 1.8.3 NIVEL DE SEGURIDAD

La magnitud y nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red.

Una red que almacena datos para un banco importante, requiere una mayor seguridad que una LAN que enlaza equipos en una pequeña organización de voluntarios.

### 1.8.4 SEGURIDAD EN REDES CABLEADAS E INALÁMBRICAS

La seguridad en redes viene dada por mecanismos como: Filtrado MAC, WEP[53], WPA[54], IEEE 802.1x, e IEEE 802.11i.

Los servicios que proporciona un ambiente seguro de operación durante la transmisión de información son:

- **Autenticación**: comprueba que un usuario es quien dice ser, y a la vez, establecer si está o no autorizado para acceder a la red.
- **Confidencialidad**: garantiza a los usuarios de la red, es decir que sólo personal autorizado puede ver sus datos, así se previene que la información sea comprometida por ataques, manteniendo su privacidad.
- **Integridad**: mantiene intacta la información enviada o recibida en la red, tanto durante la transmisión entre clientes, como entre dispositivos de interconectividad de la misma.

### 1.8.5 PROBLEMAS DE SEGURIDAD

El acceso sin necesidad de cables, es la razón que hace tan populares a las redes inalámbricas, y es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre dentro del área de cobertura del AP, podría introducirse a la red inalámbrica y además debido a que las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.

En el caso de las redes cableadas, la seguridad de la red se ve afectada por otros factores como: software de análisis de paquetes, clonación de direcciones

---

[53] *Wireless Encryption Protocol*
[54] *Wi-Fi Protected Access*

MAC, entre otros, es por ello que se deben implementar mecanismos de seguridad apropiados, para garantizar un ambiente seguro de trabajo.

En el caso de las redes de área personal inalámbricas, como es el caso de *Bluetooth*, sus desarrolladores se encargaron de cuidar al máximo la robustez del mismo, tal que hasta ahora, no se han encontrado fallas de seguridad inherentes al protocolo.

Sin embargo, las vulnerabilidades se presentan en los dispositivos *Bluetooth*, ya que los fabricantes implantan esta tecnología en sus dispositivos sin ajustarse estrictamente a las recomendaciones del *Bluetooth* SIG, despreocupándose por implantar elementos de seguridad y dejando agujeros al descubierto que pueden ser aprovechados por un atacante malicioso, para comprometer el dispositivo y por ende la información que dependa del mismo.

### 1.8.6 TIPOS DE ATAQUES Y VULNERABILIDADES

Los tipos de ataques se dividen en dos grandes grupos, ataques pasivos y ataques activos.

#### 1.8.6.1 Ataques Pasivos

Este tipo de ataque permite que se gane parte de acceso a la red pero no se modifica el contenido de la información, son ataques pasivos: *Eavesdropping*[55] y Análisis de Paquetes.

##### *1.8.6.1.1 Escuchas Ilegales*

Este tipo de amenaza consiste en que un tercero no autorizado escuche ilegalmente las señales de radio intercambiadas entre una estación inalámbrica y un punto de acceso, comprometiendo la confidencialidad de la información propietaria o sensible.

Un operador de radio que envíe un mensaje está en riesgo de ser escuchado por todos los usuarios que tengan un equipo receptor y que estén dentro del rango de

[55] Escucha Ilegal

transmisión. Además, dado que la escucha ilegal no altera dados, el emisor y el receptor pueden ni siquiera darse cuenta de la intrusión.

#### *1.8.6.1.2 Análisis de Paquetes*

Son amenazas mediante programas que capturan un paquete, lo desencapsulan y obtienen la información que llevan dentro. Generalmente cuando los paquetes viajan encriptados, los atacantes, capturan cierto número de paquetes, para mediante técnicas computacionales, descubrir el mecanismo de encripción y sus claves.

### 1.8.6.2 Ataques Activos

En este caso existe la modificación de la información y sus consecuencias generalmente son: pérdidas de la información, costos legales, y pérdida del servicio en la red; este tipo de ataques son difíciles de prevenir aunque su detección sea más sencilla.

Se identifican como ataques activos a: acceso no autorizado o enmascaramiento, interferencias aleatorias e intencionadas, y amenazas físicas, los cuales se describen a continuación.

#### *1.8.6.2.1 Acceso No Autorizado*

Es una amenaza donde un intruso ingresa en el sistema de una red, disfrazado como un usuario autorizado, una vez adentro puede violar la confidencialidad e integridad de la información y causar daños irreparables.

#### *1.8.6.2.2 Interferencias Aleatorias e Intencionadas*

Las interferencias de radio, son una amenaza para la seguridad de una red inalámbrica, aquí se puede degradar seriamente el ancho de banda. En muchos casos estas interferencias son accidentales, ya que otros tipos de dispositivos electromagnéticos que operen en el espectro de infrarrojo o la banda de radio-frecuencia podrían solaparse con el tráfico de la red.

*1.8.6.2.3 Amenazas Físicas*

Una red puede venirse abajo cuando la infraestructura está dañada o destruida. Todos los componentes físicos como: equipos de interconectividad, cables, antenas, adaptadores de red, etc., pueden sufrir daños limitando la intensidad de las señales, y reduciendo el área de cobertura o ancho de banda, dificultando a los usuarios la capacidad para acceder a la información.

Estos componentes físicos también son vulnerables a sabotajes y robos, por ello deben estar bajo seguridad, para que no se tenga acceso no autorizado a la red.

### 1.8.6.3 Vulnerabilidades

El principal inconveniente de la seguridad de una red, viene dado por problemas detectados tanto en protocolos, como en la desacertada configuración de los equipos de interconectividad, introduciendo vulnerabilidades que a corto o largo plazo son descubiertas por los atacantes.

Debido a lo expuesto, es necesario implementar no solo un mecanismo de seguridad, sino varios y de diversos grados de protección.

## 1.8.7 MECANISMOS DE SEGURIDAD

Para ayudar a proteger una red, se deberían considerar al menos los mecanismos de seguridad básica. Entre los mecanismos de seguridad más conocidos se tienen:

### 1.8.7.1 Filtrado de Direcciones MAC

Este método consiste en la creación de una tabla de direcciones *MAC* en cada uno de los equipos de interconectividad de la red, en las cuales se incluyen las direcciones de los equipos que pueden conectarse y acceder a la red.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas, pero esta simplicidad, ayuda a que se introduzcan las

siguientes desventajas: clonación de direcciones MAC y transmisión de información sin encripción.

### 1.8.7.2 WEP (*Wired Equivalent Privacy*)

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado.

Opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

RC4 es un algoritmo de cifrado de flujo, funciona expandiendo una semilla para generar una secuencia de números pseudo aleatorios de mayor tamaño. Esta secuencia de números pseudo aleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de inicialización (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña que genera la semilla de entrada al algoritmo RC4 y así evita secuencias iguales; de esta manera se crean semillas nuevas cada vez que varía.

El principal problema con este algoritmo, es el tamaño de los vectores de inicialización. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de inicialización, y por lo tanto sea fácil descubrir la clave. Adicionalmente se debe mencionar que, incrementar los tamaños de las claves de cifrado sólo extiende el tiempo necesario para descubrirlas.

CRC no es lo suficientemente apropiado para mantener la integridad de la información, ya que fácilmente puede generarse un mensaje distinto que produzca la misma secuencia, lo ideal es un *hash* como MD5.

### 1.8.7.3 IEEE 802.1x

IEEE 802.1x 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 fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas.

El protocolo 802.1x involucra tres participantes:

- El suplicante, o equipo cliente, que desea conectarse a 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. IEEE 802.1x fue diseñado para emplear servidores *RADIUS* (*Remote Authentication Dial-In User Service*).
- El autenticador, que es el equipo de interconectividad que recibe la conexión del suplicante.

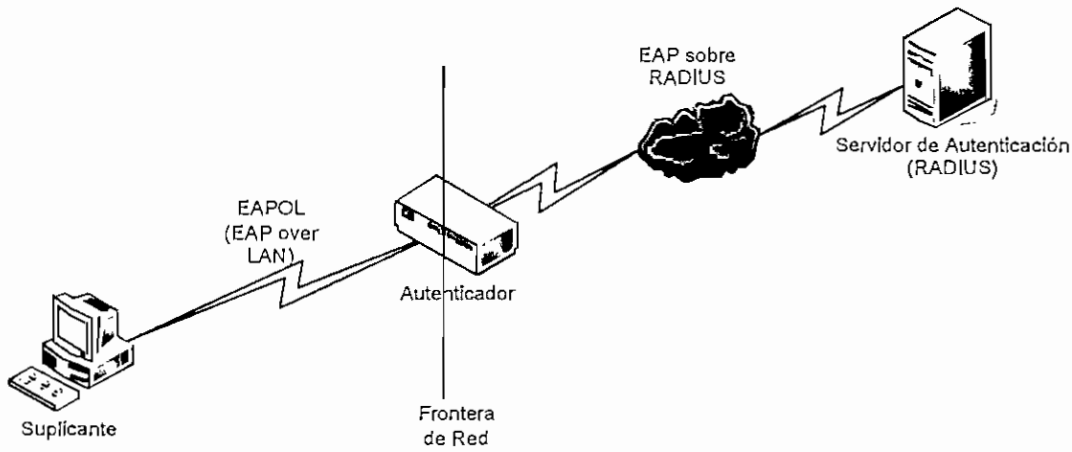



**Figura 1.33 Arquitectura de un sistema de autenticación IEEE 802.1x**

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.

- La autenticación del cliente se lleva a cabo mediante el protocolo EAP (*Extensible Authentication Protocol*) y el servicio *RADIUS.*

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje *RADIUS-Access-Accept* un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el AP.

El servidor *RADIUS* se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave.

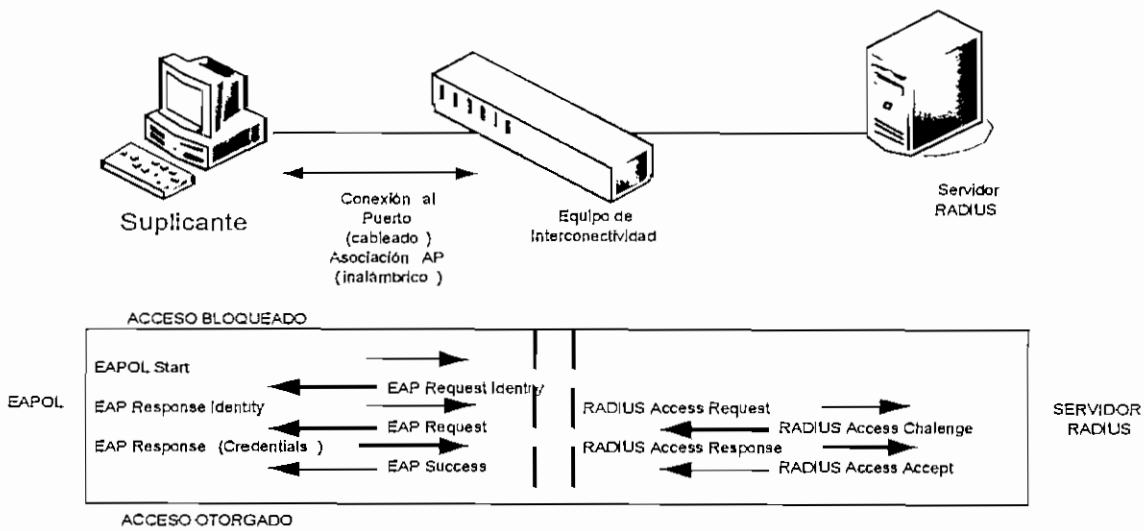



Figura 1.34[55] Diálogo EAPOL - RADIUS

### 1.8.7.4 WPA (WI-FI Protected Access)

WPA es un estándar propuesto por los miembros de la alianza Wi-Fi en colaboración con la IEEE. Las principales características de WPA son la distribución dinámica de claves, utilización robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA propone un nuevo protocolo conocido como TKIP (*Temporary Key Integrity Protocol*). Este protocolo se encarga de cambiar la clave compartida entre un AP y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

[56] Redes de Área Local Inalámbricas, Sinche Soraya MSc.

Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs[57], con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea IEEE 802.1x y EAP. Para verificar la integridad de los datos de las tramas se emplea el Código de Integridad de Mensaje MIC (*Message Integrity Code*) o código Michael.

Según la complejidad de la red, un AP compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: opera mediante un servidor RADIUS en la red. El AP emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
- Modalidad de red casera, o PSK (*Pre-Shared Key*): no se dispone de un servidor RADIUS. Se requiere introducir una contraseña (20 o mas caracteres) compartida en el AP y en los dispositivos móviles. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso.

#### 1.8.7.5 IEEE 802.11i

Es un protocolo de la serie 802.11 del IEEE que fue adoptado en junio del 2004, y recibió el nombre comercial de WPA2[58] por parte de la alianza Wi-Fi.

Las caracteristicas principales del 802.11i son:

- **Cifrado**: *Advanced Encryption Standard* (AES), es un algoritmo de cifrado de bloque con clave simétrica. Soporta claves de: 128, 192 y 256 bits.
- **Integridad de datos**: *Counter-Mode/CBC-MAC Protocol* (CCMP), es un modo de operación especial del AES para el chequeo de la integridad. Opcionalmente se dispone de *Wireless Robusted Authentication Protocol* (WRAP).

[57] Vectores de Inicialización
[58] WPA versión 2.

- **Autenticación**: provee el esquema de autenticación mutua IEEE 802.1x / *Extensible Authentication Protocol* (EAP) o clave pre-compartida (PSK *Pre Shared Key*).

El estándar IEEE 802.11i introduce varios factores fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas, como para los grandes entornos de red corporativos.

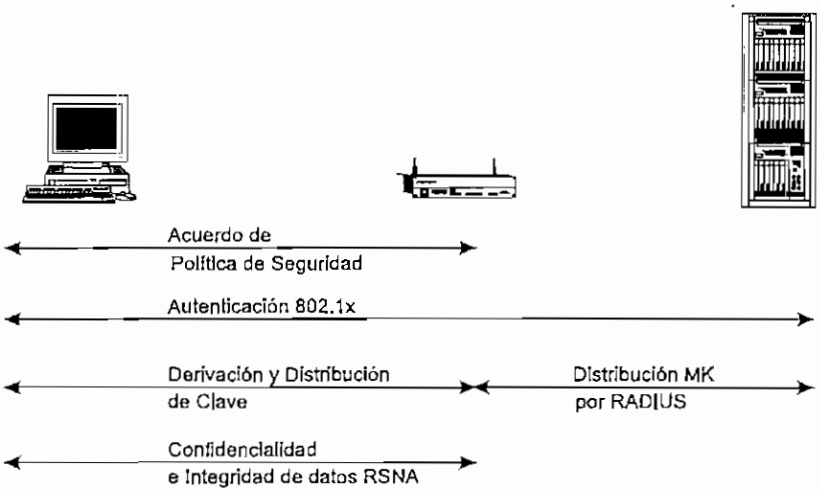



**Figura 1.35[59] Establecimiento de una comunicación segura con IEEE 802.11i**

Esta nueva arquitectura robusta para las redes inalámbricas se llama *Robust Security Network* (RSN) y utiliza autenticación 802.1X, distribución de claves robustas y nuevos mecanismos de integridad y privacidad.

Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica.

Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transitoria de seguridad – *Transitional Security Network* (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo a futuro.

[59] GUILLAUME Lehembre; Seguridad Wi-Fi – WEP, WPA y WPA2, Diciembre 2005.

Si el proceso de autenticación o asociación entre estaciones utiliza *handshake* de 4 vías, la asociación recibe el nombre de RSNA (*Robust Security Network Association*). El establecimiento de un contexto seguro de comunicación se muestra en la Figura 1.35.

Las fases de dicho establecimiento de una comunicación segura son:

- Acuerdo sobre la política de seguridad a emplear: métodos de autenticación soportados, protocolo de seguridad para el tráfico *unicast* o *multicast* (CCMP, TKIP) y soporte para la pre–autenticación antes de cambiar de AP en la misma red.
- Autenticación 802.1X.
- Derivación y distribución de las claves, incluyendo una clave maestra común MK *Master Key*, manipulada por el Servidor RADIUS.
- Confidencialidad e integridad de los datos RSNA.

Finalmente cabe notar que los equipos en los que se vaya a implementar este complejo mecanismo de seguridad, requerirán un hardware potente para realizar sus algoritmos, lo cual es importante, puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporarlo.

### 1.8.8 PARÁMETROS PARA ELABORAR LAS POLÍTICAS DE SEGURIDAD

Generar la seguridad en una red requiere establecer un conjunto de reglas, regulaciones y políticas que no dejan nada al azar.

El primer paso para garantizar la seguridad de los datos es implementar las políticas que establecen los matices de la seguridad y ayudan al administrador y a los usuarios a actuar cuando se producen modificaciones, esperadas como no planificadas, en el desarrollo de la red.

#### 1.8.8.1 Prevención

La mejor forma de diseñar las políticas de seguridad de los datos es optar por una perspectiva preventiva. Los datos se mantienen seguros cuando se evita el acceso no autorizado.

Un sistema basado en la prevención requiere que el administrador conozca todas las herramientas y métodos disponibles que permiten mantener la seguridad de los datos.

#### 1.8.8.2 Autenticación

Para acceder a la red, un usuario debe introducir un nombre de usuario y una contraseña válida. Dado que las contraseñas se vinculan a las cuentas de usuario, un sistema de autenticación de contraseñas constituye la primera línea de defensa frente a usuarios no autorizados.

Es importante no permitir un exceso de confianza en este proceso de autenticación engañándonos con una falsa idea de seguridad. La autenticación funciona sólo en una red basada en servidor, donde el nombre y contraseña de usuario debe ser autenticada utilizando para ello la base de datos de seguridad.

#### 1.8.8.3 Entrenamiento

Los errores no intencionados pueden implicar fallos en la seguridad. Un usuario de red perfectamente entrenado probablemente va a causar, de forma accidental, un número menor de errores que un principiante sin ningún tipo de experiencia, que puede provocar la pérdida de un recurso dañando o eliminando datos de forma definitiva.

El administrador debe asegurar que alguien que utiliza la red esté familiarizado con sus procedimientos operativos y con las tareas relativas a la seguridad.

#### 1.8.8.4 Mantenimiento de un Entorno de Red Operativo

El entorno físico donde reside una red es un factor importante a considerar en el mantenimiento de una red de equipos físicamente segura.

#### 1.8.8.5 Los Equipos y el Entorno

La mayor parte de los tipos de equipamiento electrónico, son rígidos y fiables, funcionan durante años con un pequeño mantenimiento.

Un proceso de deterioro lento, pero continuo puede generar problemas intermitentes, cada vez más frecuentes, hasta provocar un fallo catastrófico en el sistema. Cuando se planifica o mantiene una red, es importante pensar en términos de red global (completa), visible o no, y no sólo en los componentes locales que se ven cada día.

#### 1.8.8.6 Creación del Entorno Adecuado

Es responsabilidad del administrador de la red crear las políticas que gobiernen prácticas seguras alrededor del equipamiento de la red e implementar y gestionar el entorno de trabajo apropiado para la red, tomando en cuenta factores como: temperatura, humedad, y polvo del sitio donde se desea implementar la red, ya que pueden ocasionar el mal funcionamiento de los equipos.

#### 1.8.8.7 Factores Humanos

En el diseño de una red, podemos controlar muchos factores ambientales, como temperatura, humedad y ventilación.

Aunque es posible, desde un punto de vista teórico, la creación de un entorno físico adecuado para los equipos, la entrada en escena de las personas traerá consigo modificaciones ligadas a provocar impactos en la red.

#### 1.8.8.8 Factores Ocultos

Muchos aspectos de la red no están visibles y, por tanto, fuera de nuestro pensamiento.

Dado que diariamente no se pueden ver estos elementos ocultos, se supone que todo está correcto hasta que comienzan a generar problemas.

El cableado es uno de los componentes de red que puede provocar problemas, especialmente cables que se encuentran en el suelo. Los cables de un ático se pueden dañar fácilmente debido a un accidente durante las reparaciones de otros objetos del ático. Los roedores y bichos de todo tipo son otros factores ocultos,

estos invitados no deseados salen a cenar probablemente los materiales de red o los utilizan con propósitos de construcción.

#### 1.8.8.9 Factores Industriales

El trabajo del equipamiento de red en un entorno de producción presenta muchos desafíos. Las propiedades necesarias a controlar cuando se implementan las redes en un entorno de fabricación incluyen la presencia de: Ruido, Interferencia electromagnéticas (EMI), Vibraciones, Entornos explosivos y corrosivos, Trabajadores no especializados y sin entrenamiento adecuado.

Para minimizar los problemas que se derivan del funcionamiento de una red en un entorno industrial, se debe:

- Instalar el equipamiento de red en habitaciones separadas con ventilación externa.
- Utilizar cableado de fibra óptica, para reducir los problemas de interferencias eléctricas y corrosión del cable.
- Asegurar que todo el equipamiento está conectado a tierra de forma adecuada.
- Proporcionar el entrenamiento adecuado a todos los empleados que necesitan utilizar el equipamiento, para garantizar la integridad del sistema.

### 1.8.9 EQUIPAMIENTO DE SEGURIDAD

El primer paso en el mantenimiento de la seguridad de los datos es proporcionar seguridad física para el *hardware* de la red.

La magnitud de la seguridad requerida depende de:

- El tamaño de la empresa.

- La importancia de los datos.

- Los recursos disponibles para brindar seguridad.

## 1.8.10 MODELOS DE SEGURIDAD

Después de implementar la seguridad en los componentes físicos de la red, el administrador necesita garantizar la seguridad en los recursos de la red, evitando accesos no autorizados y daños accidentales o deliberados.

Las políticas para la asignación de permisos y derechos a los recursos de la red constituyen el corazón de la seguridad de la red. Se han desarrollado dos modelos de seguridad para garantizar la seguridad de los datos y recursos *hardware*.

### 1.8.10.1 Compartición Protegida por Contraseña

La implementación de un esquema para compartir recursos protegidos por contraseñas requiere la asignación de una contraseña a cada recurso compartido. Se garantiza el acceso a un recurso compartido cuando el usuario introduce la contraseña correcta. Los tipos de acceso pueden ser de solo lectura, y acceso total.

### 1.8.10.2 Permisos de Acceso

Esta seguridad implica la asignación de ciertos derechos usuario por usuario. Un usuario escribe una contraseña cuando entra en la red. El servidor valida esta combinación de contraseña y nombre de usuario y la utiliza para asignar o denegar el acceso a los recursos compartidos, comprobando el acceso al recurso en una base de datos de accesos de usuarios en el servidor.

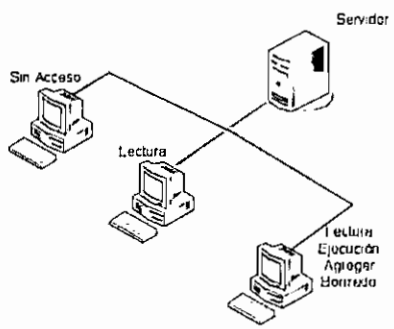



**Figura 1.36 Control de Acceso mediante permisos**

Este modelo es preferido en las grandes organizaciones, puesto que se trata de la seguridad más completa y permite determinar varios niveles de seguridad.

### 1.8.11 SEGURIDAD DE LOS RECURSOS

Después de autenticar a un usuario y permitir su acceso a la red, el sistema de seguridad proporciona al usuario el acceso a los recursos apropiados.

Los usuarios tienen contraseñas, pero los recursos tienen permisos. En este sentido, cada recurso tiene una barrera de seguridad. La barrera tiene diferentes puertas mediante las cuales los usuarios pueden acceder al recurso. Determinadas puertas permiten a los usuarios realizar más operaciones sobre los recursos que otras puertas. El administrador determina qué usuarios tienen acceso a qué puertas.

Algunos de los permisos de acceso habituales asignados a los directorios o archivos compartidos son: lectura, ejecución, escritura, borrado, sin acceso.

### 1.8.12 PERMISOS DE GRUPO

La forma más eficiente de realizarlo es mediante la utilización de grupos, especialmente en una organización grande con muchos usuarios y recursos.

Los permisos para los grupos funcionan de la misma forma que los permisos individuales. El administrador revisa los permisos que se requieren para cada cuenta y asigna las cuentas a los grupos apropiados.

### 1.8.13 MEDIDAS DE SEGURIDAD ADICIONALES

El administrador de la red puede incrementar el nivel de seguridad de una red de diversas formas.

#### 1.8.13.1 Cortafuegos (*Firewalls*)

Un cortafuegos es un sistema de seguridad, normalmente una combinación de *hardware* y *software*, que está destinado a proteger la red de una organización frente a amenazas externas que proceden de otra red, incluyendo Internet.

Los cortafuegos evitan que los equipos de red de una organización se comuniquen directamente con equipos externos a la red, y viceversa. En su lugar, todas las comunicaciones de entrada y salida se encaminan a través de un servidor *Proxy* que se encuentra fuera de la red de la organización.

Además, los cortafuegos auditan la actividad de la red, registrando el volumen de tráfico y proporcionando información sobre los intentos no autorizados de acceder al sistema.

Un servidor *Proxy* es un cortafuegos que gestiona el tráfico de Internet que se dirige y genera una red de área local (LAN). El servidor *proxy* decide si es seguro permitir que un determinado mensaje pase a la red de la organización.

#### 1.8.13.2 Auditoria

La revisión de los registros de eventos en el registro de seguridad de un servidor se denomina *auditoria*. Este proceso realiza un seguimiento de las actividades de la red por parte de las cuentas de usuario. La auditoria debería constituir un elemento de rutina de la seguridad de la red.

Los registros de auditoria muestran los accesos por parte de los usuarios (o intentos de acceso) a recursos específicos. La auditoria ayuda a los administradores a identificar la actividad no autorizada.

#### 1.8.13.3 Equipos sin Disco

Los equipos sin disco, como su nombre implica, no tienen unidades de disco o discos duros. Pueden realizar todo lo que hacen los equipos con unidades de disco, excepto almacenar datos en una unidad de disco local o en un disco duro. Los equipos sin disco constituyen una opción ideal para el mantenimiento de la seguridad puesto que los usuarios no pueden descargar datos y obtenerlos.

#### 1.8.13.4 Cifrado de Datos

Una utilidad de cifrado de datos cifra los datos antes de enviarlos a la red. Esto hace que los datos sean ilegibles, incluso para alguien que escucha el cable e

intenta leer los datos cuando pasan a través de la red. Cuando los datos llegan al equipo adecuado, el código para descifrar los datos cifrados decodifica los bits, trasladándolos a información entendible.

Los esquemas más avanzados de cifrado y descifrado automatizan ambos procesos. Los mejores sistemas de cifrado se basan en *hardware* y pueden resultar muy caros.

### 1.8.14 VIRUS INFORMÁTICOS

Los virus informáticos se han convertido en algo demasiado familiar en la vida diaria. Los virus son bits de programación de equipos o código, que se ocultan en los programas de equipos o en el sector de arranque de los dispositivos de almacenamiento, como unidades de disco duro o unidades de disco.

El propósito principal de un virus es reproducirse, así mismo, con tanta asiduidad como sea posible y, finalmente, destruir el funcionamiento del equipo o programa infectado. Una vez activado, un virus puede ser un simple anuncio o completamente catastrófico en su efecto.

### 1.8.15 EVITAR LA PÉRDIDA DE DATOS

Un desastre en un sitio se define como cualquier cosa que provoca la pérdida de los datos. Muchas organizaciones grandes tienen planes de recuperación de catástrofes que permiten mantener la operatividad y realizar un proceso de reconstrucción después de ocurrir una catástrofe natural como puede ser un terremoto o un huracán. Desgraciadamente no todas, incluyen un plan para recuperar la red. La recuperación frente a las catástrofes en una red va más allá del reemplazo de los dispositivos *hardware*, también se deben proteger los datos.

Cuando tiene lugar una catástrofe, el tiempo que se consume en la recuperación de los datos a partir de una copia de seguridad (si se dispone de ella), puede resultar una pérdida seria de productividad. No digamos si no se dispone de las correspondientes copias de seguridad. En este caso, las consecuencias son aún más severas, provocando posiblemente unas pérdidas económicas significativas.

Algunas formas de evitar o recuperar datos a partir de la pérdida de los mismos, son:

- Sistemas de copia de seguridad de cintas.
- Equipos de interconectividad con mecanismos de redundancia.
- Un sistema de alimentación ininterrumpida (SAI) mediante UPS[60] o planta eléctrica.
- Sistemas tolerantes a fallos.
- Discos y unidades ópticas.

### 1.8.16 RECUPERACIÓN FRENTE A CATÁSTROFES

El intento de recuperación frente a una catástrofe, independientemente de la causa, puede constituir una experiencia terrible. El éxito de la recuperación depende de la implementación frente a catástrofes y del estado de preparación desarrollado por el administrador de la red.

### 1.8.17 PREVENCIÓN DE CATÁSTROFES

La mejor forma de recuperarse frente a un desastre es, en primer lugar, evitarlo antes de que ocurra. Cuando se implementa la prevención de catástrofes se debe:

- Enfocar los factores sobre los que se tienen control.
- Determinar el mejor método de prevención.
- Implementar y forzar las medidas preventivas que se seleccionen.
- Comprobar continuamente nuevos y mejores métodos de prevención.
- Realizar un mantenimiento habitual y periódico de todas las componentes *hardware y software* de la red.

Recordar que el entrenamiento es la clave de la prevención de las catástrofes de tipo humano que pueden afectar a la red. No todas las catástrofes se pueden evitar. Cada jurisdicción tiene un plan de contingencia frente a catástrofes y se gastan muchas horas cada año en la preparación de este plan. Dado que cada

---

[60] *Unit Power Supply*

comunidad es diferente, los planes de recuperación tendrán en cuenta distintos factores.

Cuando se considera la protección frente a las catastro fes, necesitará un plan para el *hardware*, *software* y datos. Se pueden reemplazar las aplicaciones *software* y *hardware* y los sistemas operativos. Pero para realizar esto, es necesario, primero, conocer exactamente los recursos que se disponen. Realice un inventario de todo el *hardware* y *software*, incluyendo fecha de compra, modelo y número de serie.

Los componentes físicos de una red se pueden reemplazar fácilmente y, normalmente, están cubiertos por algún tipo de seguro, pero el problema se plantea con los datos que son altamente vulnerables a las catástrofes.

La única protección frente a las catástrofes que implican la pérdida de datos es implementar un método de copias de seguridad o más de uno de los descritos anteriormente. Almacene las copias de seguridad en un lugar seguro, como puede ser una caja de seguridad de un banco, lejos del sitio donde se ubica la red.

Para conseguir una recuperación total frente a cualquier catástrofe, necesitará:

- Realizar un plan de recuperación.
- Implementar el plan y comprobarlo.

# CAPÍTULO 2

# DISEÑO DE LA RED HÍBRIDA

# 2. DISEÑO DE LA RED HÍBRIDA

## 2.1 ESTADO ACTUAL DEL FUNCIONAMIENTO DE LA CLÍNICA

La Clínica Durán es propiedad del Dr. Juan José Durán, se encuentra ubicada en el sector Cashapamba en la parte Nor - Occidental de la ciudad de Ambato en la Av. Pasteur 1315 e Italia.

La Clínica Durán desarrolla sus actividades en un edificio que cuenta con 5 pisos. Los dos primeros pisos están construidos en su totalidad, mientras que los tres restantes se encuentran parcialmente construidos, y serán concluidos en su totalidad en un futuro a largo plazo.

En la planta baja se encuentra operando: Emergencia, Farmacia, Caja de Información, Camillero, Sala de Espera, Consulta Externa, Eco, Pediatría, Tomografía, Rayos X y Cabina.

En el primer piso se tienen: Suites, Contabilidad y Administración, Sala de Espera, Enfermería, Esterilización, Estación de Enfermería, Vestidor Enfermeras, Preparación de Ropa, Termo cuna, Vestidor de Médicos, Sala de partos, recuperación y quirófanos.

En el segundo piso se encuentra funcionando: Suites, Utilería, Odontología, Sala de Espera, y en el área por construir, se ubican los tendederos.

En el tercer piso se dispone de: Habitaciones, Dormitorio de Residentes, Bodega de Farmacia, Sala de Espera, y en el área restante por construir, funcionan las lavanderías de la clínica.

Finalmente en el cuarto piso se tiene: Cocina, Comedor de Médicos y Terraza.

### 2.1.1 ESTRUCTURA ACTUAL DE LA RED Y MANEJO DE INFORMACIÓN

La infraestructura actual de la clínica cuenta con varios puntos de red y un equipo de interconectividad (*switch*) marca 3COM, modelo LS Banda Base de 24 puertos 10/100 Mbps, puerto MDI/MDIX y no administrable.

El cableado estructurado actual fue elaborado sin cumplir ningún estándar, por lo cual la edificación no dispone de un Cuarto de Comunicaciones, y no garantiza actualmente, un adecuado funcionamiento de la red.

En la red de datos se tiene funcionando únicamente el sistema contable. Se tienen ciertos archivos y carpetas compartidos a nivel de administrador y de usuario simple. La clínica no dispone de un software para atención médica, manteniendo toda su información de pacientes en fichas médicas y en hojas de cálculo.

### 2.1.2 CONSIDERACIONES GENERALES DE DISEÑO

Previo a la realización del diseño, es necesario determinar los factores que establezcan el correcto funcionamiento de la red híbrida, los cuales se analizan a continuación.

#### 2.1.2.1 Desvanecimiento por Múltiples Trayectorias

Este fenómeno se presenta cuando una señal de RF tiene más de un camino entre un receptor y un transmisor, lo que provoca que múltiples señales distorsionen la señal original y la degraden.

Para el presente proyecto, este factor es considerado en ambientes *indoor*, ya que podría ocasionar alteraciones de la información que viaja a través de la red, perdiendo su confiabilidad, y afectando a lugares críticos de la clínica, que requieren de la misma permanentemente, como es el caso de Emergencia.

#### 2.1.2.2 Diversidad

En un ambiente de múltiples caminos, se tienen puntos nulos donde no existe señal, los cuales se encuentran en el contorno del área que se quiere cubrir con la red, ocasionados por el entorno mismo.

Para recibir la señal de manera adecuada es necesario moverse del punto nulo. Se aprovecha de este factor, para garantizar que los mismos se ubiquen en

aquellos sitios donde se encuentran los equipos médicos que podrían interferir con la red a diseñar, y así garantizar su funcionamiento adecuado.

Es por esto que se introduce el concepto de antenas duales, con lo cual si una antena está en un punto nulo, la otra no lo está y se garantiza el adecuado funcionamiento de la red.

### 2.1.2.3 Áreas de Cobertura y Velocidad de Conexión

En las comunicaciones inalámbricas se presenta una contraposición, ya que, entre mayor es el área de cobertura, menor es la velocidad a la cual se establece la conexión, como se muestra en la Figura 2.1 (IEEE 802.11g). Para equilibrar este factor, se incrementa la ganancia de las antenas, sin embargo esto ocasiona mayor interferencia entre canales adyacentes.

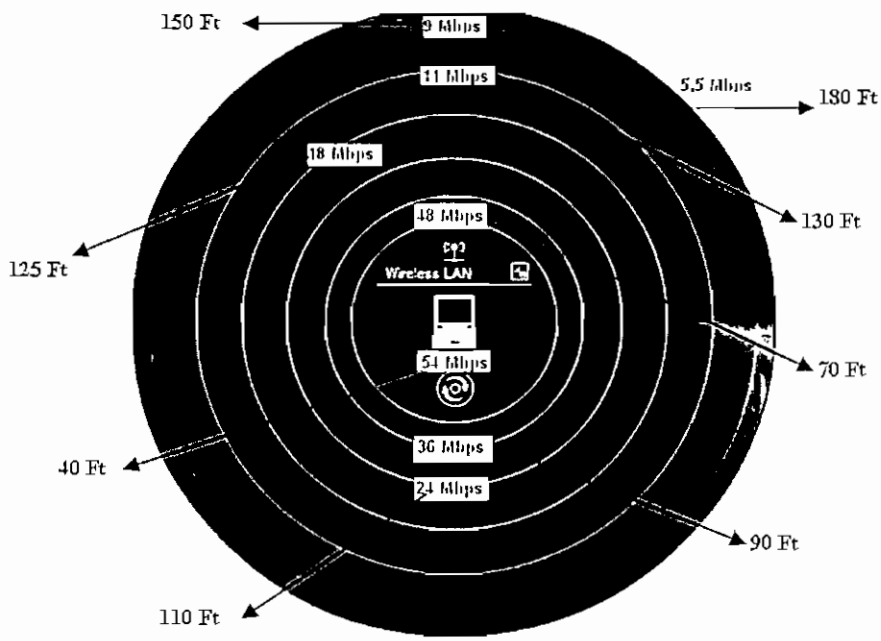



Figura 2.1 Áreas de Cobertura y Velocidades de Conexión para IEEE 802.11g

### 2.1.2.4 Escalabilidad

Este factor permite emplear canales que no se interfieran entre sí, con la finalidad de aumentar la velocidad de conexión; así por ejemplo se puede emplear 3 canales no adyacentes de IEEE 802.11g, y alcanzar una velocidad teórica de 162 Mbps (54 Mbps x 3).

#### 2.1.2.5 Reflexión y Refracción

Para mantener un nivel aceptable de la señal, se deben considerar los materiales de construcción de la edificación y del mobiliario.

Existen objetos que provocan que la señal se refracte, permitiendo su paso; mientras que otros la reflejan, desvaneciéndola e incluso llegando a perderla.

#### 2.1.2.6 Ancho de Banda

El ancho de banda de la red híbrida, es uno de los parámetros de mayor importancia a la hora de plasmar un diseño, ya que permite realizar su adecuado dimensionamiento.

Para este proyecto, se ha considerado la utilización de aplicaciones de software básicas y propias de la clínica, y el software cero papel para el manejo de la información de la misma.

#### 2.1.2.7 Usuarios a Servir

El número de usuarios a servir, está determinado por las necesidades de la clínica. Para elaborar un diseño acertado se debe considerar la cantidad de usuarios a servir por cada AP y un porcentaje de crecimiento futuro de la red.

#### 2.1.2.8 Seguridades

La clínica no dispone de ningún mecanismo, ni políticas de seguridad a nivel de transmisión de información. En una red inalámbrica es indispensable que se disponga de niveles mínimos de seguridad.

#### 2.1.2.9 Equipos de Medición de Signos Vitales

En este establecimiento se realiza la medición de los signos vitales de los pacientes, en forma manual y se los almacena de igual manera. Para optimizar este proceso, se emplearán sensores de medición, que se acoplen adecuadamente al resto del diseño de la red híbrida.

## 2.2 ANÁLISIS DE REQUERIMIENTOS Y EVALUACIÓN DEL SITIO DE DISEÑO

El presente diseño se lo elabora considerando las dificultades que implica tener equipos médicos trabajando en la misma banda de frecuencia que la red inalámbrica.

El diseño se divide en dos partes: la cableada y la inalámbrica. Para la parte cableada se considerará el equipo de interconectividad del cual dispone la clínica, siempre y cuando se ajuste a los requerimientos del diseño; para la parte inalámbrica, se analizarán las características de los equipos de interconectividad disponibles y las redes inalámbricas cercanas al sitio de diseño, que podrían ocasionar interferencia con la red.

Adicionalmente se plantean dos diseños para la red sensores, que interactuará con la red inalámbrica, y se selecciona el más adecuado acorde a los requerimientos de manejo de información de la clínica y su disponibilidad en el mercado.

### 2.2.1 ANÁLISIS DE REQUERIMIENTOS

El edificio de la Clínica Durán, presta sus servicios las 24 horas del día, realizando desde consultas médicas hasta operaciones de alto riesgo, por tanto es imprescindible el adecuado funcionamiento de todos los componentes de comunicaciones.

Se considera necesario un equipo con características de Servidor, para mantener el manejo de la información centralizado (topología estrella), el cual puede disponer adicionalmente del servicio DNS[1], para mantener perfiles de usuario de la red y hacer uso de sus recursos.

Para elaborar adecuadamente el diseño de la red, se analizan en detalle los requerimientos del sitio y de los usuarios, tal como se muestra a continuación.

---

[1] *Domain Name Server* mediante *Active Directory*

#### 2.2.1.1 Cuarto de Comunicaciones

La clínica no dispone de un cuarto de comunicaciones, debido a la falta de planificación en lo que a comunicaciones se refiere, previo a la construcción del edificio.

Por esta razón, se plantea una solución adecuada y económica, que radica en disponer de un espacio apropiado en el primer piso (Departamento de Contabilidad y Administración), para colocar un pequeño RACK de comunicaciones y dar servicio a los usuarios de la red.

Cabe notar que se elige el mencionado sitio, por disponer de la seguridad física adecuada para los equipos, y del acceso restringido del personal al mismo.

Para llevar a cabo este procedimiento, se cumplirán las normativas y especificaciones dadas mediante el estándar ANSI/EIA/TIA 568B, de tal modo que se mejore la administración y funcionamiento de la red.

#### 2.2.1.2 Usuarios por Departamento

Los usuarios que emplearán la red híbrida a diseñar son: empleados administrativos, personal médico, y propietarios de la Clínica Durán, sin embargo esta consideración es teórica.

Para obtener la información real de los usuarios a servir y evitar errores de dimensionamiento, se realizó una visita a la clínica, determinándose el número de usuarios real por departamento, y clasificándolas por piso dentro de la edificación.

Acorde a lo que se establece en la tabla 2.1, se determina que el número de usuarios entre pacientes, y personal médico y administrativo de la clínica que utilizarán la red, en condiciones normales está en aproximadamente 44.

Sin embargo, el dueño de la institución, supo manifestar, que hay ocasiones en las que se tienen médicos foráneos atendiendo en la misma y éstos requerirán acceder a la información de la red, por lo tanto, se deja un 10% de crecimiento, llegando a tener un máximo de 49 usuarios en la red.

| Piso | Departamento | Número de Usuarios |
|---|---|---|
| PLANTA BAJA | Emergencia | 1 |
| | Farmacia | 1 |
| | Información | 1 |
| | Camillero | ---- |
| | Sala de Espera | ---- |
| | Consulta Externa | 3 |
| | Eco | 1 |
| | Pediatría | 1 |
| | Monitoreo | 1 |
| | Rayos X | ---- |
| | Tomografía | ---- |
| | Cabina | 2 |
| PRIMER PISO | Suite 1 | 1 |
| | Suite 2 | 1 |
| | Suite 3 | 1 |
| | Suite 4 | 2 |
| | Contabilidad y Adm. | 4 |
| | Utilería | ---- |
| | Sala de Espera | ---- |
| | Enfermería | 2 |
| | Termo-cuna | 1 |
| | Vestidor Enfermería | ---- |
| | Estación Enfermería | ---- |
| | Esterilización | ---- |
| | Prep. Ropa | ---- |
| | Vestidor Médicos | 1 |
| | Preparación | 1 |
| | Sala de Partos | 1 |
| | Quirófano 1 | 1 |
| | Quirófano 2 | 1 |
| | Recuperación | 2 |
| SEGUNDO PISO | Suite 5 | 1 |
| | Suite 6 | 2 |
| | Suite 7 | 1 |
| | Suite 8 | 2 |
| | Odontología | 1 |
| | Sala de Espera | ---- |
| | Utilería | ---- |
| TERCER PISO | Habitación 9 | 1 |
| | Habitación 10 | 1 |
| | Habitación 11 | 1 |
| | Habitación Residentes | 3 |
| | Bodega de Farmacia | 1 |
| | Sala de Espera | ---- |
| | Utilería | ---- |
| TOTAL DE USUARIOS | | 44 |

Tabla 2.1 Usuarios de la Red de la Clínica Durán

### 2.2.1.3 Cálculo del Ancho de Banda y Selección de Estándares

Para determinar la velocidad de trabajo necesaria y suficiente para la red, se ha determinado que el número de usuarios sea de 44 no simultáneos, en condiciones normales.

Se define que el Ancho de Banda necesario para cada aplicación a ejecutarse sobre la red, en base a los resultados brindados por el Administrador de Tareas de Windows, es el siguiente:

- Sistema contable (900 Kbps).
- Sistema de atención médica cero papel (850 Kbps).
- Procesador de palabras, Hoja de cálculo, *Power Point* (250 Kbps).
- Sistema de control de medicamentos para la farmacia (200 Kbps).
- Correo electrónico (10 Kbps).
- Acceso a Internet con Banda Ancha (64 kbps).
- Compartición de archivos (1 Mbps).
- Enciclopedias médicas (50 Kbps).

Entonces, considerando la situación más crítica (44 usuarios utilizando simultáneamente todas las aplicaciones), se determina que cada usuario utilizará como máximo 3.3 Mbps, teniendo:

$$V = \#\ \text{usuarios}^* \ V\ \text{individual} \qquad \textbf{Ecuación 2.1 AB total de la red}$$

$$V = 44 * 3.3\ (\text{Mbps}) = 145.2\ (\text{Mbps})$$

Esta velocidad es ideal, por lo cual se ha tomado un grado de utilización del 10%[2] de la capacidad total (Regla 10 a 1), debido a que generalmente no todos los usuarios acceden paralelamente a todas las aplicaciones, con lo cual se tiene que la capacidad necesaria y suficiente para el funcionamiento adecuado de la red, es de 14.5 Mbps.

Para la parte cableada, se requiere elaborar el diseño con un estándar acorde a la velocidad mínima establecida, a la topología y a la disponibilidad económica de la

[2] SINCHE Soraya MSc, Apuntes de Clase de Redes de Área Local Inalámbricas.

clínica, por tanto se selecciona *Fast Ethernet*, ya que permite velocidades entre 10 y 100 Mbps, y emplea como medio de transmisión el cable UTP categoría 6. Se selecciona este tipo de cable, para permitir el funcionamiento adecuado a futuro de nuevas aplicaciones.

Este medio de transmisión ha sido definido para trabajar con la topología deseada, aprueba los estándares de cableado estructurado necesarios para obtener una certificación y es relativamente económico, en relación con los medios de transmisión que emplea este estándar.

Para el caso de la red de sensores, se cuenta con 4 nodos (presión, temperatura, ritmo cardíaco, y pulso) en la red, se considera que el ancho de banda a emplearse es de alrededor de 1 MHz (IEEE 802.15.1) por cada uno de ellos. Debido a que la información obtenida de los sensores es crítica (signos vitales de los pacientes), se ve la necesidad de transmitirla a tiempo real, razones por las cuales se debe escoger la mejor tecnología que se ajuste a estos parámetros.

Las redes cableada, inalámbrica y de sensores deben estar interconectadas entre ellas formando la red híbrida; para lo cual la conexión entre la primera y la segunda, se realiza a través de un puerto de los equipos de interconectividad, y la conexión entre la segunda y la tercera, al tener como medio de transmisión al aire, debe emplear la misma banda de frecuencias, y hacerlo a través de una tarjeta dual.

Para la red inalámbrica, en base a los requerimientos de velocidad obtenidos, se decide que el estándar a emplear sea IEEE 802.11g, ya que permite trabajar con velocidades de hasta 54 Mbps, superando lo necesario, y emplea la banda de frecuencias de 2.4 GHz, que es la adecuada para la interconexión con los estándares para redes de sensores inalámbricas, disponibles actualmente. Por tanto se descarta la utilización de IEEE 802.11a e IEEE 802.11b.

### 2.2.2 EVALUACIÓN DEL TERRENO

La clínica tiene un área total de 377 (37.2 x 10.13) $m^2$, y se desea garantizar la cobertura de los siguientes lugares: habitaciones, contabilidad y administración,

farmacia, información, enfermería, salas de espera, emergencia y consulta externa.

#### 2.2.2.1 Materiales de Construcción de la Clínica

Al realizar la inspección de la clínica, se obtuvieron los siguientes resultados en cuanto a materiales:

- Puertas de madera y vidrio.
- Armarios de aglomerado.
- Pisos de baldosa.
- Mesones de mármol.
- Paredes internas de bloque (40 cm ó 20 cm de grosor).
- En Tomografía y Rayos X, se dispone de paredes de 60 cm de grosor hechas de bloque macizo.
- Quirófanos, Sala de Partos y Recuperación totalmente herméticos.
- Vidrios de 5 líneas.
- Focos y lámparas fluorescentes.

## 2.3 PROCEDIMIENTO DE DISEÑO

Para realizar el diseño de la red se ha utilizado el siguiente procedimiento:

a) Levantamiento de Planos acorde con la infraestructura arquitectónica actual.
b) Determinación de las áreas que van a ser cubiertas por la red inalámbrica y aquellas que por razones de interferencia causada por el equipo médico, empleen la red cableada, garantizando la seguridad de los pacientes y a la vez la integridad de la información.
c) Análisis de interferencia.
d) Análisis de las características de los AP disponibles en mercado, y selección de la mejor opción acorde a los requerimientos planteados.
e) Determinación del número de AP requeridos para el diseño.
f) Pruebas de calidad de la señal, para determinar la correcta ubicación de los Puntos de Acceso.

g) Diseño de la red de sensores inalámbricos *Zigbee* y *Bluetooth*, a interactuar con la red cableada e inalámbrica.
h) Selección de uno de los diseños de la red de sensores elaborados, acorde a los requerimientos de Ancho de Banda de la clínica y la disponibilidad del equipo en el mercado.
i) Elaboración del diseño de cableado estructurado de voz/datos, considerando para los puntos de datos sólo aquellas zonas propensas a interferencia.
j) Establecimiento de los materiales y equipos necesarios, acorde al diseño planteado.

Se considera para el diseño de la red inalámbrica, únicamente los equipos médicos mencionados por el personal de la clínica.

Adicionalmente, se aclara que actualmente no se dispone del ascensor, pero el diseño incluye las posibles complicaciones que puede ocasionar éste.

Para la red cableada se ha asignado en el primer piso, un espacio de 2 $m^2$ para ubicar el RACK, debido a que en este sitio se dispone de una abertura por la cual se puede llegar a todos los pisos.

Para el diseño de la red de sensores, se ha tomado en cuenta únicamente las áreas de Consulta Externa y Emergencia, debido a la gran necesidad de monitoreo clínico en éstas. Sin embargo, si se requiere de la misma en otras áreas, se la puede reubicar, siempre y cuando se considere puntualmente las recomendaciones de interferencia con otros equipos, dadas por los fabricantes de los sensores.

## 2.4 POLÍTICAS DE SEGURIDAD

En el capítulo anterior se realizó un estudio de seguridad de las redes en general, a partir de lo cual se ve la necesidad de emplear mecanismos de seguridad y reglas o políticas adecuadas, para el buen funcionamiento de la red.

### 2.4.1 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD

Una política de seguridad, y el cumplimiento de ella, es fundamental dentro de la operación de una red, a continuación se definen las políticas de seguridad necesarias para el correcto funcionamiento de la red, acorde al servicio que brinda la institución.

a) La red será de una misma marca en cuanto a equipos de interconectividad y tarjetas de red inalámbricas; esto para que el intruso tenga que trabajar con un modelo compatible al nuestro.
b) Los Puntos de Acceso estarán colocados permanentemente, en los sitios designados acorde al diseño, en cajas adecuadamente ventiladas y aseguradas.
c) *El switch* se ubica en el primer piso, en el Armario de Comunicaciones, permaneciendo encendido siempre.
d) Los sensores ubicados en Consulta Externa, se encenderán únicamente cuando se requiera atender al paciente, previo a la cancelación de la cita médica.
e) Las claves por defecto en los equipos de interconectividad son cambiadas, y manipuladas por el administrador de la red, siendo de su completa responsabilidad el uso de las mismas.
f) Implementación de autentificación bidireccional.
g) Control y filtrado de direcciones MAC e identificadores de red, para restringir los adaptadores y los equipos de interconectividad que se puedan conectar a la red.
h) Seguridad mediante servidor de autenticación *RADIUS* trabajando con IEEE 802.1x - WEP. El tamaño de las cuatro claves creadas es de 128 bits en formato ASCII.
i) Las claves WEP serán cambiadas cada dos meses por el Administrador de la red. Adicionalmente se proporcionara una guía sobre la creación y administración de las llaves.
j) Educación a los usuarios de la red, para que mantengan la confidencialidad de las claves y eviten compartir información crítica para la organización.
k) Identificación de quienes puede usar la WLAN en la clínica y quienes no.

l) Identificación de los lugares en los cuales se tendrá acceso a Internet.
m) Identificación del personal encargado del mantenimiento de los APs y las estaciones de trabajo, por parte de los encargados de la clínica.
n) Descripción del tipo de información que puede ser enviada sobre los enlaces inalámbricos.
o) La información almacenada en las BDD, será respaldada cada fin de semana, y entregada en un CD o DVD según corresponda, al administrador de la red.
p) En caso de sucesos de pérdidas de dispositivos, se dispone de un fondo económico para alquilar o reemplazar el mismo.
q) Se agregarán usuarios a la red únicamente con autorización del administrador de la red o el gerente de la institución.
r) La frecuencia de utilización de estas políticas es permanente, y se rige para todos los usuarios de la red.

## 2.5 SELECCIÓN DE EQUIPOS Y ELEMENTOS

La elaboración del diseño de la red híbrida, se la ha separado en tres partes principales: parte cableada, parte inalámbrica y sensores. Para realizar esta selección de equipos y elementos, es necesario analizar los requerimientos de ancho de banda definidos anteriormente, y en base a ello determinar los equipos disponibles en el mercado, que satisfagan las exigencias mínimas del mismo.

En el mercado se encuentran disponibles una variedad de equipos y elementos para redes, sin embargo se deben considerar únicamente aquellos que brinden confiabilidad, en cuanto a utilización y garantía y ser compatibles tecnológicamente entre ellos.

### 2.5.1 RED CABLEADA

Conforme a los requerimientos establecidos en el ítem 2.2.1.3[3], es necesario disponer de un equipo de interconectividad, que trabaje a una velocidad mínima de 14 Mbps, con cable UTP categoría 6, y que realice segmentación y aislamiento

[3] Cálculo del Ancho de Banda y Selección de Estándares

de estaciones de alto tráfico por disponer de un servidor. No se ve la necesidad de disponer de una VLAN[4] ya que se dispone de un solo dominio y todos los usuarios pertenecen a una única función departamental.

Por lo cual se concluye que el equipo de interconectividad apropiado para el presente diseño, debe ser un *switch* de capa 2.

Entonces luego de analizar las características del equipo[5] de interconectividad del que dispone la clínica, y compararlas con las requeridas, se decide utilizar el mismo, ya que satisface las necesidades planteadas.

#### 2.5.1.1 Tarjeta de Red

Las tarjetas de interconexión con la red cableada, deben estar acorde al estándar de trabajo del equipo de interconectividad elegido, y a la velocidad mínima establecida en 14 Mbps.

Es por ello que las tarjetas de red a emplear, son las que disponen los computadores de la clínica, las cuales son marca ADVANTAGE/CNET, PCI, *Ethernet* 10/100 Mbps.

#### 2.5.1.2 Elementos

Los elementos a emplear para la red cableada se resumen en la Tabla 2.2.

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | *Patch Panel* | 48 Puertos RJ45 categoría 6 |
| 2 | RACK | Mural MUPM de 10" categoría 6 |
| 3 | Cable UTP | Categoría 6 de 4 pares |
| 4 | Conectores | Tipo RJ45 |
| 5 | Canaletas | Tamaño: 2 metros, Capacidad: 2 cables UTP categoría 6 de 4 pares. |
| 6 | Tubería | Tipo PVC de _", con codos y uniones. |
| 7 | *Patch Cords* | De 3 pies, categoría 6. |

Tabla 2.2 Elementos requeridos para la red cableada.

[4] Redes LAN Virtuales
[5] Equipo descrito en el ítem 2.1.1 Estructura Actual y Manejo de Información de la Red.

## 2.5.2 RED INALÁMBRICA

Acorde a los requerimientos establecidos en el ítem 2.2.1.3[6] para la red inalámbrica, es necesario optar por un equipo de interconectividad inalámbrico, que trabaje a una velocidad mínima de 14 Mbps, disponga de un puerto *Ethernet* 10/100 Mbps, trabaje en la banda de frecuencias de 2.4 GHz, y soporte hasta 49 usuarios simultáneamente, acorde al ítem 2.2.1.2[7].

El equipo debe proveer un rango de cobertura promedio de 37 m, acorde al área de la clínica descrito en el ítem 2.2.2[8].

Adicionalmente, en base a lo planteado en las políticas de seguridad, se ve la necesidad de que los equipos y elementos soporten los mecanismos de seguridad establecidos.

Adicionalmente, el equipo debe disponer de administración vía Navegador Web, *Telnet*, o HTTP, para ser configurado.

Luego de examinar los equipos disponibles en el mercado, se han seleccionado como posibles marcas para los equipos a: 3COM, *Lynksys*, DLINK y *Avantec*, descartándose las 2 últimas opciones por razones de soporte técnico y garantía.

A continuación se presentan la descripción y características, de los dos equipos de interconectividad inalámbricos, que cumplen los requerimientos definidos, acorde a las marcas seleccionadas.

### 2.5.2.1 Puntos de Acceso

#### *2.5.2.1.1 Punto de Acceso 3Com OfficeConnect Wireless 108 Mbps 11g*

El punto de Acceso 3Com® con capacidad PoE[9] y certificación Wi-Fi constituye una solución para extender el acceso móvil a los recursos de la red cableada, o para crear redes con multitud de características para las pequeñas y medianas

---

[6] Cálculo del Ancho de Banda y Selección de Estándares.
[7] Usuarios por Departamento
[8] Evaluación del Terreno
[9] *Power Over Ethernet*

empresas, oficinas remotas o temporales, de forma segura y rentable. Una de las características más atractivas de este equipo, es la sensibilidad en recepción, cuyos valores se resumen en la Tabla 2.3.

| 802.11g | | 802.11b | |
|---|---|---|---|
| 108 Mbps | -68 dBm | 11 Mbps | -85 dBm |
| 48 Mbps | -73 dBm | 5,5 Mbps | -89 dBm |
| 36 Mbps | -78 dBm | 2 Mbps | -90 dBm |
| 24 Mbps | -82 dBm | 1 Mbps | - 93 dBm |
| 18 Mbps | -83 dBm | | |
| 12, 11, 9 Mbps | -88 dBm | | |
| 6 Mbps | -90 dBm | | |

**Tabla 2.3 Sensibilidad en recepción del AP 3COM *Office Connect Wireless***

Las especificaciones de este producto se detallan a continuación:

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | Interfaces | RJ-45, Puerto *Ethernet* 10 BASE-TX/100 Base-TX, DB9 hembra. |
| 2 | Usuarios | Hasta 64 simultáneamente, bajo IEEE 802.11b/g. |
| 3 | Compatibilidad | Certificación Wi-Fi, IEEE 802.11b/g, IEEE 802.3, IEEE 802.3af, IEEE 802.1X, IEEE 802.1Q, AES[10], WPA, WEP, HTTP, SNMP. |
| 4 | Velocidades | 802.11b: 11, 5.5, 2, y 1 Mbps.<br>802.11g: 6, 9, 12, 18, 24, 36, 48, 54, y 108Mbps. |
| 5 | Alcance | Para IEEE 802.11b/g hasta 100 m INDOOR. |
| 6 | Antena | Extraible con ganancia de 2 dB. y conector RP-SMA. |
| 7 | Seguridad | WPA, AES, TKIP, WEP de 64/128/152 bits, 802.1X con EAP-TLS, EAP-TTLS, y PEAP, WPA-PSK, Filtrado MAC, VLAN 802.1Q, AAA de cliente RADIUS. |
| 8 | Administración | Línea de Comando, Interfaz de Navegador Web o HTTP o S-http, SNMP, *Access Point Discovery, Syslog y Firmware* actualizable. |
| 9 | Rendimiento | Super G de 108 Mbps, *Clear Channel Select*, Ráfaga de Paquetes, Cambio dinámico de velocidad. |
| 10 | Indicadores LED | Alimentación, actividad LAN, estado, actividad inalámbrica. |
| 11 | Alimentación | 24 VDC, 300 mA. |
| 12 | Banda de Frecuencias | 802.11b/g 2.4 -- 2.4835 GHz |
| 13 | Esquema de Modulación | 802.11b DSSS, 802.11g OFDM – DSSS |
| 14 | Protocolo Acceso al medio | CSMA/CA |

**Tabla 2.4 Características del AP 3COM *Office Connect Wireless***

[10] Sistema de Encripción Asimétrica

*2.5.2.1.2 Punto de Acceso LinkSys*

Linksys es una división de los equipos *CISCO Systems Works*, lo cual garantiza confiabilidad y un adecuado funcionamiento.

El Punto de Acceso seleccionado de entre la gama que ofrece el fabricante mencionado es el *Wireless - G Access Point WAP54G*.

Sus características de mayor relevancia se resumen a continuación:

| Item | Nombre | Descripción |
|---|---|---|
| 1 | Interfaces | Puerto Ethernet 10/100 MDI/MDIX |
| 2 | Usuarios | Hasta 60 simultáneamente, bajo IEEE 802.11b/g. |
| 3 | Compatibilidad | IEEE 802.11b/g, IEEE 802.3, IEEE 802.3u. |
| 4 | Velocidades | 802.11b: 11, 5.5, 2, y 1 Mbps.<br>802.11g: 6, 9, 12, 18, 24, 36, 48, y 54 Mbps. |
| 5 | Alcance | Para IEEE 802.11b/g hasta 76 m INDOOR, -74 dBm |
| 6 | Antena | Extraible con ganancia de 2 dB. y conector RP-SMA. |
| 7 | Seguridad | Filtrado MAC, WEP 64/128, WPA RADIUS. |
| 8 | Administración | Interfaz de Navegador Web o HTTP o S-HTTP. |
| 10 | Indicadores LED | Alimentación, actividad LAN, actividad inalámbrica. |
| 11 | Alimentación | 24 VDC, 300 mA. |
| 12 | Banda de Frecuencias | 802.11b/g 2.4 – 2.4835 GHz |
| 13 | Esquema de Modulación | 802.11b DSSS, 802.11g OFDM - DSSS |
| 14 | Seguridad Rápida | Crea una conexión inalámbrica con WPA |

Tabla 2.5 Características del AP *Linksys* WAP54G

### 2.5.2.2 Selección del Punto de Acceso

Para realizar la selección del AP, se procede a presentar un cuadro comparativo de las características de los equipos mencionados, y las requeridas para el presente diseño, en la tabla 2.6.

Como se puede apreciar a continuación, las especificaciones del Punto de Acceso 3COM en cuanto a cobertura y mecanismos de seguridad, son mejores respecto del otro equipo, ya que al permitir mayor cobertura, se emplean menos APs para cubrir el área planteada, y el alto nivel de seguridad que provee, permite garantizar que la información de la red no sea atacada.

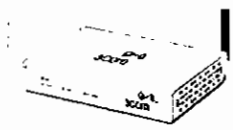
| Ítem | Requerimientos Mínimos del Proyecto[11] | AP 3COM  | AP LINKSYS  |
|---|---|---|---|
| Velocidad | 14 Mbps | IEEE 802.11 b/g hasta 108 Mbps | IEEE 802.11 b/g hasta 54 Mbps |
| Banda de Frecuencia | 2.4 GHz | 2.4 GHZ | 2.4 GHZ |
| Usuarios | 49 | 64 Simultáneamente | 60 Simultáneamente |
| Seguridad | Filtrado MAC WEP IEEE 802.1x con RADIUS | WPA, AES, TKIP, WEP de 64/128/152 bits, 802.1X con EAP-TLS, EAP-TTLS, y PEAP, WPA-PSK, Filtrado MAC, VLAN 802.1Q, AAA de cliente RADIUS. | Filtrado MAC, WEP 64/128, WPA RADIUS. |
| Cobertura | 37 m en interiores | 100m en Interiores | 76 m en Interiores |
| Administración | Navegador Web, *Telnet*, HTTP | Navegador Web o HTTP o S-http, SNMP, *Access Point Discovery, Syslog* y Firmware actualizable | Interfaz de Navegador Web o HTTP o S-HTTP |
| Niveles de Potencia | - 14.8 dBm[12] | - 83 dBm | -64 dBm |
| Precio | - | $156.95 | $74.87 |

Tabla 2.6 Comparativa de características de los APs

Una de las principales desventajas del primer equipo respecto del segundo, es su costo, pero este se ve recompensado por sus características en cuanto a potencia, rendimiento, y administración.

[11] 2.2.1.3 Cálculo del Ancho de Banda y Selección de Estándares - 2.5.2.1. Punto de Acceso
[12] Acorde a parámetros de potencia establecidos en el estándar IEEE 802.11g (40 dBm a 100m).

Luego de analizar las características de mayor relevancia de los APs, para satisfacer los requerimientos del diseño planteado, y compararlas, se ha seleccionado el Punto de Acceso 3COM, ya que pese a su costo, permite emplear un menor número de éstos debido a su cobertura. Adicionalmente, se debe mencionar que los mecanismos de seguridad del AP seleccionado, están acorde al nivel de seguridad y confiabilidad requeridas para la información manipulada.

### 2.5.2.3 Tarjeta de Red Inalámbrica

La tarjeta de red inalámbrica a seleccionar, debe trabajar a una velocidad mínima de 54 Mbps, en la banda de frecuencia de 2.4 GHz, rango de operación de 37.2[13] metros, y mecanismos de seguridad acorde al Punto de Acceso y a las políticas de seguridad. Analizadas las tarjetas disponibles en el mercado, se selecciona la recomendada por el fabricante, para el AP escogido, ya que cumple con las características requeridas.

#### *2.5.2.3.1 Tarjeta de Red Inalámbrica 3COM*

La tarjeta inalámbrica seleccionada para el Punto de Acceso propuesto, es el Adaptador Compacto USB 3Com® *OfficeConnect® Wireless* 54Mbps 11g. Sus características se resumen en la tabla 2.7 y su imagen en la Figura 2.2.

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | Tipo de Bus | USB 2.0 |
| 2 | Velocidad | IEEE 802.11b: 1, 2, 5.5 y 11 Mbps<br>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps |
| 3 | Banda de Frecuencia | 2.4 – 2.4835 GHz |
| 4 | Técnica de Modulación | IEEE 802.11b: DSSS/CCK; IEEE 802.11g: DSSS/CCK, OFDM |
| 5 | Protocolo de Acceso al Medio | CSMA/CA |
| 6 | Canales de Operación | 1-11 América, 1-14 Japón, 1-13 Europa |
| 7 | Rango de Operación | Con obstáculos: 100 m, sin obstáculos: 400 m |
| 8 | Antena | Tipo PCB |
| 9 | Seguridad | WPA, IEEE 802.11i |
| 10 | Estándares | IEEE 802.11b/g, IEEE 802.3, IEEE 802.11i |
| 11 | Potencia de Salida | IEEE 802.11b: 19 dBm<br>IEEE 802.11g: 15 dBm (48 y 54 Mbps) y 17 dBm (resto) |
| 12 | Precio | $41 (dólares) |

**Tabla 2.7 Características del Adaptador Compacto USB 3COM**

[13] Dato basado en 2.2.2 Evaluación del Terreno

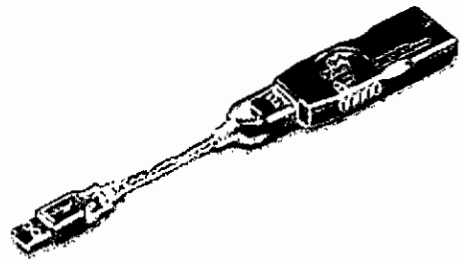


Figura 2.2 Adaptador Compacto USB 3COM

### 2.5.3 RED DE SENSORES

Para este ítem, se considera únicamente la inclusión de sensores de medición de: pulso, ritmo cardíaco, presión, y temperatura.

Para la selección de los sensores, es necesario tomar en cuenta factores como: disponibilidad en el mercado, precisión, tiempo de duración de la batería, capacidad de procesamiento y compatibilidad entre ellos.

Se toman en cuenta exclusivamente los sensores que trabajen con los estándares *Bluetooth* y *ZigBee*, por ser los de mayor auge y aceptación en el mercado, y a la vez de permitir interconectividad con el estándar de la red inalámbrica planteado en el ítem 2.2.1.3[14].

La red de sensores que se pretende construir debe de cumplir características muy concretas, las cuales se mencionan a continuación:

- La primera de ellas, es que debe abarcar áreas específicas y canalizar toda la información recogida en los sensores hacia una estación base de almacenamiento global de datos.
- La segunda, es que el consumo de potencia de los sensores debe ser muy bajo, para permitir una alimentación a batería que permita su funcionamiento de forma autónoma.
- Y por último, la latencia en la comunicación debe ser lo mas pequeña posible, ya que la sensorización de variables médicas presenta limitaciones críticas.

[14] Cálculo del Ancho de Banda y Selección de Estándares

A partir de estas especificaciones se concluye que la red es semi-estática, sin movimiento crítico de los nodos, con lo cual existe una red con multitud de nodos enlazados de forma inalámbrica, capaces de canalizar la información hasta una estación base, que será el origen/destino de todas las transferencias de información en la red.

Las métricas de evaluación de una WSN[15] y un Nodo Sensor, se muestran a continuación:

| Evaluación WSN | Evaluación Nodo Sensor |
|---|---|
| Tiempo de Vida | Energía |
| Cobertura | Flexibilidad |
| Costo y Facilidad de Instalación | Robustez |
| Tiempo de Respuesta | Seguridad |
| Precisión y Frecuencia de Mediciones | Comunicación |
| Seguridad | Computación - Sincronización |
| | Tamaño y Coste |

**Tabla 2.8 Métricas de evaluación para diseñar una WSN**

Previo a la selección de los elementos de la red de sensores, se deben considerar los parámetros de la Tabla 2.8, y su disponibilidad en el mercado.

### 2.5.3.1 Elementos *ZigBee*[16]

En una red de sensores *ZigBee*, se requieren dos elementos básicos: el Nodo Coordinador y los sensores (Nodo Sensor).

Actualmente, los principales marcas de plataformas para redes de nodos inalámbricos, son: *Wins, Smart Dust, iPAQ, y Berkeley MICA Mote.*

Las principales características de dichas plataformas, se resumen en la Tabla 2.9.

En el mercado, la plataforma de mayor aceptación por sus características, costos y disponibilidad, es *MICA Mote*, es por ello que se la ha seleccionado para la realización del diseño *ZigBee* de este proyecto.

---

[15] *Wireless Sensor Network*
[16] *Wireless Sensor Networks* – Investigación, María Soledad Escolar Díaz, 2005.

| | *Wins NG 2.0* | *iPAQ* | *Berkeley MICA Mote* | *Smart Dust* |
|---|---|---|---|---|
| Costo (USD) | 100 | 100 | 10 | <1 |
| Tamaño ($cm^3$) | 5300 | 600 | 40 | 0.002 |
| Peso (g), con batería | 5400 | 350 | 70 | 0.002 |
| Capacidad batería (KJ) | 300 | 35 | 15 | <15 |
| Sensores | No incluye | Luz y micrófono | Varios | No incluye |
| Marca de CPU | *Hitachi* SH4 | *StrongARM o Xscale* | *Atmega 103L* | Menor |
| Memoria | 32 MB RAM<br>32 MB flash | 64 MB RAM<br>32 MB flash | 4 KB RAM<br>128 KB flash | < 4 KB RAM |
| Sistema Operativo | Linux | WinCE o Linux | *TinyOS* | - |
| Radio de Cobertura | 100 m | 100 m | 30 m | 10m |

**Tabla 2.9 Comparación de Plataformas para Nodos *ZigBee***

El funcionamiento de la arquitectura *MICA*, radica en el Micro Controlador, hacia el cual se dirigen todas las operaciones de: memoria, co-procesador, receptor identificador, y conector.

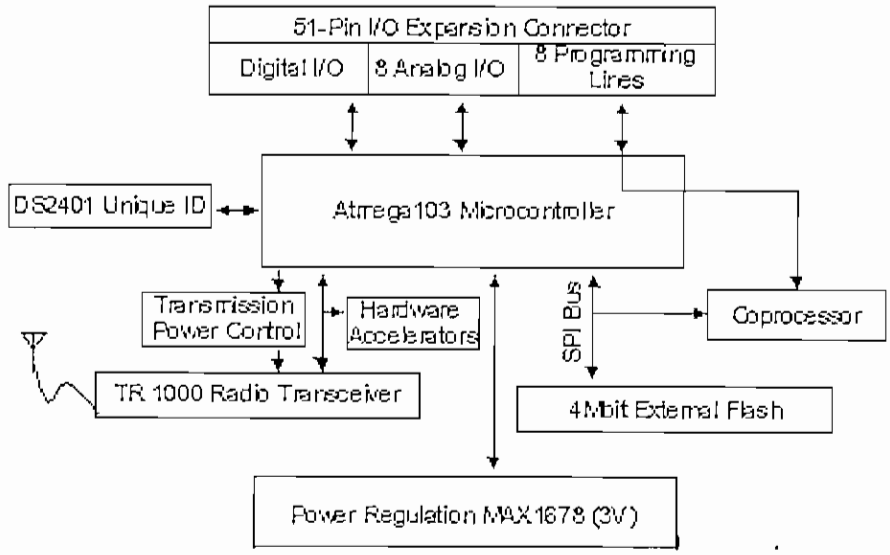



**Figura 2.3 Arquitectura MICA**

Incluye un acelerador de hardware, que trabaja en conjunto con el receptor de radio y el microcontrolador. Adicionalmente dispone de un regulador de voltaje, de 3 V. La arquitectura de *MICA* se presenta en la Figura 2.3.

Las plataformas Motes dotan de procesamiento de datos y comunicación al nodo sensor, generalmente incluyen: un par de baterías AA, un CPU, una memoria Flash, una memoria separada para datos/programas, una placa para colocar los sensores (Ej. Luz, humedad, presión, etc.), radio para comunicación con otros Motes, y un conversor analógico-digital.

Existen varios tipos de *Motes*, sus características se resumen a continuación:

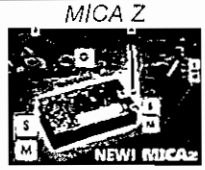
| Ítem | *MICA 2*  | *MICA Z*   | *TELOS*  |
|---|---|---|---|
| Tiempo en modo *Wakeup* | 0.2 ms | 0.2 ms | 0.006 ms |
| Tiempo en modo *Sleep* | 30 ms | 30 ms | 2 ms |
| Tiempo en modo *Active* | 33 ms | 33 ms | 3 ms |
| Potencia de Transmisión | 21 mW | 45 mW | 45 mW |
| Velocidad | 19 kbps | 250 kbps | 250 kbps |
| Voltaje de trabajo | 2.5V min | 2.5V min | 1.8V min |

**Tabla 2.10 Características de MOTES**

Mica2 provee muy bajas velocidades de transmisión. *Telos* incluye los sensores en la placa, pero aún no se dispone de un modelo con sensores médicos. Mica Z provee las características adecuadas para trabajar con sensores médicos, sin embargo no se dispone en el mercado de éstos.

Por lo tanto, se concluye que de existir módulos de tipo médico *ZigBee*, se seleccionaría Mica Z.

Los sensores que se conectan a la plataforma Nodo Coordinador *Mica Z*, tienen la siguiente estructura: medidores de variables y el puerto de interfaz paralelo.

En la Figura 2.4 se muestra un ejemplo de un sensor *Zigbee* (MTS300/310), capaz de detectar aceleración, luminosidad, micrófono, sonido, magnetómetro, y temperatura.

El interfaz con el *Mote*, se lo realiza mediante el puerto paralelo, cuya descripción de pines se muestra en el Anexo 2A.

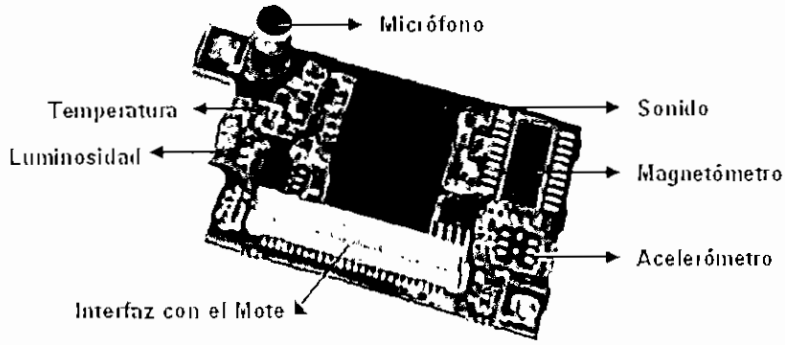



Figura 2.4 Sensor *ZigBee* MTS300/310

Para la interconexión de la red de sensores con un PC o una red, se requiere de un *gateway*. Existen dos tipos de *gateways*: *Ethernet* y Serial (RS – 232), los cuales se muestran en las siguientes gráficas.

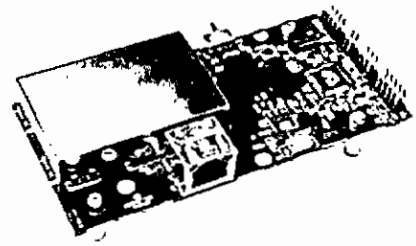


Figura 2.5 *Gateway* MIB600. *Ethernet* (TCP/IP)

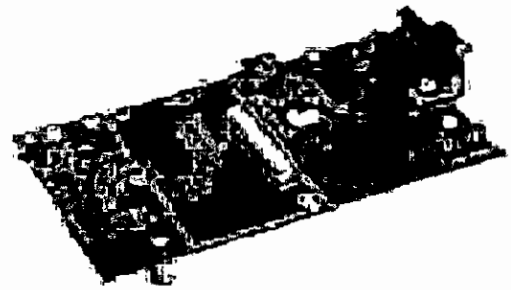


Figura 2.6 *Gateway* MIB510. Serial (RS-232)

Finalmente se requiere de una estación base o *STARGATE*, para realizar la recolección y almacenamiento de los datos obtenidos por los sensores. El *Stargate* es un sistema embebido basado en el procesador *Intel XScale* y el sistema operativo Linux.

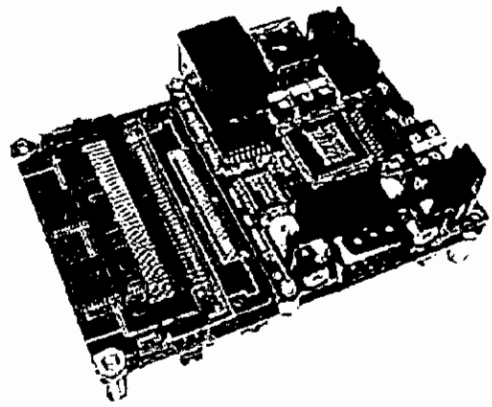


Figura 2.7 *Stargate* Completo

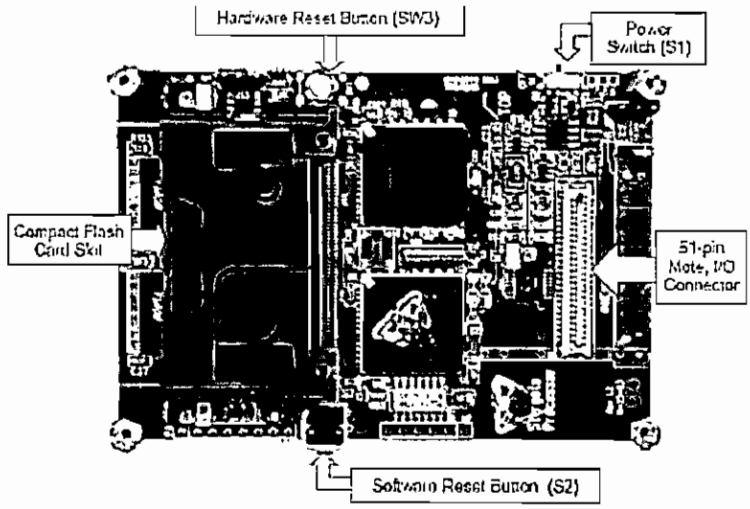



Figura 2.8 Parte 1 del *Stargate*

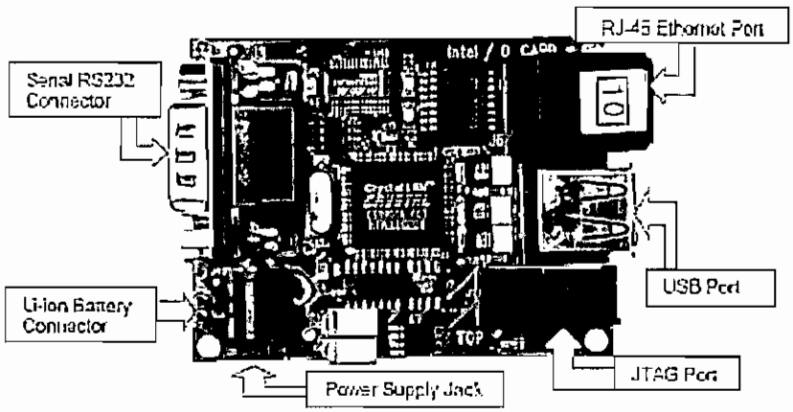



Figura 2.9 Parte 2 del *Stargate*

El *Stargate*, tiene las siguientes características:

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | Procesador | Intel PXA255 XScale RISC de 32 bits, 400 MHz |
| 2 | Chíp | SA1111 Strong ARM para Gestión I/O |
| 3 | RAM | Tipo dinámica, 64 MB |
| 4 | Slots | 1 PCMCIA |
| 5 | Sincronización | Reloj tiempo real |
| 6 | Compatibilidad | MICA2, MICAz, conector de expansión GPIO/SSp de 51 pines. |
| 7 | Pin 51 | Empleado para: puerto 10BASE-T, USB, RS-232, DB-9, y alimentación externa. |

Tabla 2.11 Características del *Stargate*

Adicionalmente, se debe mencionar que para trabajar con los *Motes: Mica, Mica2, Micadot, Micaz, Telos*, la Universidad de *Berkeley* ha creado el sistema operativo *TinyOS (Tiny Microthreading Operating System)*, el cual fue diseñado específicamente para sensores en red, con el objetivo de llenar el vacío existente entre las capacidades de *hardware* y el sistema completo.

Las funciones del *TinyOs* son: enrutamiento, conversor analógico-digital, identificación de un nodo, reserva de memoria, conversión serie-paralelo, pila de comunicación, radio, *Active Messages*, logs del sistema, reloj del sistema, energía del sistema, resetear el sistema, generador de números aleatorios, leds del sistema, conversión de datos (Int a Leds, a Radio y viceversa), y gestión de errores CRC.

### 2.5.3.2 Elementos *Bluetooth*

El campo médico ha empezado a involucrarse con esta tecnología en lo que a monitoreo médico se refiere, existiendo diversos equipos en estudio y prototipos de prueba, sin embargo la gran mayoría de ellos no están disponibles aún en el mercado.

El equipo de interconectividad a seleccionar, debe permitir la conexión múltiple de hasta 4 sensores, una cobertura promedio de 4.6[17] metros, y trabajar en la banda

[17] Dimensión del área de consulta externa medida acorde a planos de la clínica.

de frecuencias de 2.4 GHz, a velocidades de 850 Kbps (acorde al sistema de atención médica cero papel[18]).

A continuación se detallan los sensores médicos disponibles a la venta para el diseño de la red, así como el equipo de interconexión de los mismos, que se ajustan a los requerimientos especificados.

#### *2.5.3.2.1 Punto de Acceso Bluetooth*

El Punto de Acceso *Bluetooth* DBT-900AP permite habilitar el paso hacia una red LAN para usuarios que trabajan con equipos *Bluetooth* tales como *notebooks* o PDA's. Además admite la conexión en red de múltiples usuarios, hasta 7 simultáneamente de forma inalámbrica y una cobertura de hasta 20 metros.

Figura 2.10 Punto de Acceso *Bluetooth* DLINK DBT-900AP

Entre sus principales características se distinguen:

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | Estándar | *Bluetooth* v1.1 (PAN *Profile Compliant*) |
| 2 | Puertos | RJ-45, 100BASE-TX |
| 3 | Cobertura | Hasta 20 metros |
| 4 | Antena | Externa giratoria, dipolo con ganancia 2 dBi |
| 5 | Frecuencia | 2.400 – 2.4835 GHz |
| 6 | Modulación | FHSS - GFSK[19] |
| 7 | Potencia de Salida | 6 a +4 dBm |

Tabla 2.12 Características del AP *Bluetooth* DLINK DBT-900AP

[18] Dato obtenido del ítem 2.2.1.3 Cálculo del Ancho de Banda y Selección de Estándares
[19] *Gaussian Frequency Shift Keying*

### *2.5.3.2.2 Pulso – Oxímetro Bluetooth NONIN AVANT-4100*[20]

Se emplea este dispositivo para este trabajo, por ser el único disponible en el mercado acorde a las necesidades planteadas en el ítem 2.5.3[21].

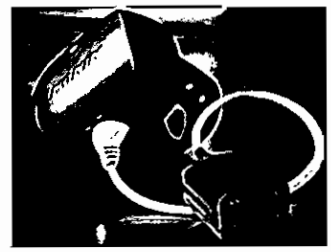


**Figura 2.11 Pulso – Oxímetro *Bluetooth* NONIN AVANT-4100**

El módulo de paciente *Avant 4100* tipo muñequera de *Nonin* con tecnología inalámbrica *Bluetooth*, permite transmitir los datos de SpO2[22], frecuencia de pulso y pletismografía, a través de un receptor *Bluetooth*, a un dispositivo compatible configurado para utilizar esta tecnología.

El módulo del paciente incorpora una radio *Bluetooth* con un alcance aproximado de 9 metros de radio esférico. Las especificaciones técnicas del equipo se detallan en la siguiente tabla:

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | % SpO2 | Limite saturación de oxigeno: 0- 100% |
| 2 | Frecuencia de Pulso | De 18 a 300 pulsos por minuto |
| 3 | Longitud de Onda | Roja 660 nm |
| 4 | Potencia de Salida | 3 mW (nominal) |
| 5 | Alimentación | Interna: 2 baterías AA de 1.5 V |
| 6 | Antena | Tipo F invertida, ganancia 2 dB |
| 7 | Protocolo | *Bluetooth* v1.1 |
| 8 | Alcance | 9 metros en interiores. |
| 9 | Topología | Punto – Punto |
| 10 | Modulación | FHSS |
| 11 | Ancho de Banda | 1 MHz |

**Tabla 2.13 Características del Pulso – Oxímetro NONIN**

[20] www.nonin.com
[21] Red de Sensores
[22] SpO2 Límite de Saturación de Oxígeno en la Sangre

El sensor realiza la medición de parámetros de pulso y ritmo cardíaco, mediante la emisión de luz de diodos (LED *Light Emitting Diodes)*.

El sensor genera dos ondas de luz de: 600-750 nm (R rojo) y 850-1000 nm (IR infrarrojo), dichas ondas son absorbidas constantemente por hemoglobinas, huesos, grasa, piel y uñas.

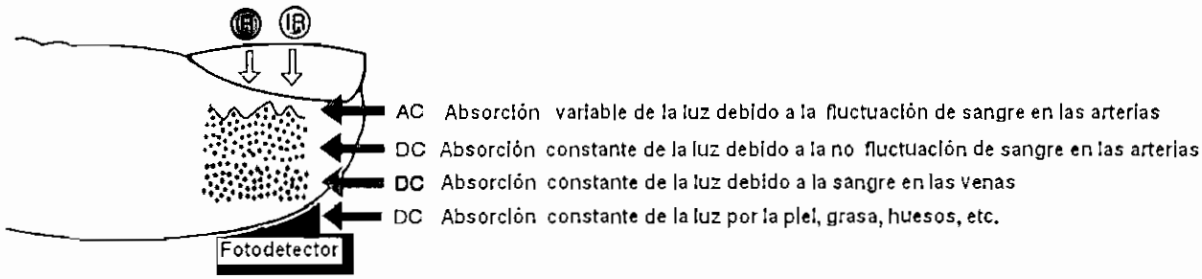



**Figura 2.12 Proceso de medición de Pulso y Ritmo Cardíaco**

El fotodetector en el sensor, mide la luz roja/infrarroja transmitida, considerando que la hemoglobina oxigenada absorbe más la luz infrarroja, con lo cual la luz roja atraviesa, ocurriendo lo contrario con la hemoglobina desoxigenada. La luz absorbida por las dos ondas, se convierte en un valor numérico de SpO2, en base a una tabla o curva de calibración previamente definida.

En pacientes saludables, típicamente un R/IR de 0.5 equivale al 100% de SpO2. Se considera como valores normales de SpO2 a un rango entre 94 y 100%.

Todos los Pulso-Oxímetros, requieren una señal de pulso, ya que su amplitud viene dada por la fluctuación de la sangre en las arterias, y ésta permite determinar la curva de comportamiento del corazón.

Para realizar la transmisión de los datos obtenidos por el sensor inalámbrico, se emplea el puerto serial. Los formatos de datos con los que se transmiten las mediciones, vienen dados por:

- **Formato de Datos 1**

  Se transmiten tres bytes de datos por cada segundo, los cuales vienen dados de acuerdo a la siguiente figura:

| Byte 1: STATUS | | | | | | | |
|---|---|---|---|---|---|---|---|
| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
| 1 | SNSD | OOT | LPRF | MPRF | ARTF | HR8 | HR7 |
| **Byte 2: HEART RATE** | | | | | | | |
| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
| 0 | HR6 | HR5 | HR4 | HR3 | HR2 | HR1 | HR0 |
| **Byte 3: SpO2 RATE** | | | | | | | |
| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
| 0 | SP6 | SP5 | SP4 | SP3 | SP2 | SP1 | SP0 |

**Figura 2.13 Formato de Datos 1 del Pulso Oxímetro**

- SNSD (*Sensor Disconected*): sensor desconectado.
- OOT (*Out of track*): fuera de seguimiento.
- LPRF (*Low Perfusion*): calidad de señal baja.
- MPRF (*Marginal Perfusion*): calidad de señal media baja.
- ARTF (*Artifact*): indica la condición del dispositivo.
- HR8 – HR0 (*Heart Rate*): Pulso promediado durante 4 latidos.
- SP6 – SP0 (*SpO2*): Nivel de saturación de oxígeno en sangre promediado durante 4 latidos, no limitado en velocidad de cambio.

Este formato de paquete, es el que trasmite por defecto el sensor; pero si llegase a existir algún problema en la conexión, se usa el formato de datos 2.

- **Formato de Datos 2**

Una trama consiste de 5 bytes, un paquete está formado por 25 tramas, y se trasmiten 3 paquetes (75 tramas) por cada segundo.

De estos 5 bytes, los bytes 2 y 4 son los que permiten determinar los datos de medición de los sensores. El byte 5 permite realizar la comprobación de la trama recibida, mediante la suma módulo 256 de los 4 *Bytes* anteriores [(Byte1)+ (Byte2)+ (Byte3)+ (Byte4) módulo 256], esto para evitar inconsistencias en los datos. El byte 1 permanece constante.

La Figura 2.14 muestra descripción de la trama descrita.

PAQUETE

| | Byte 1 | Byte 2 | Byte 3 | Byte 4 | Byte 5 |
|---|---|---|---|---|---|
| 1 | 01 | STATUS | PLETH | HR MSB | CHK |
| 2 | 01 | STATUS | PLETH | HR LSB | CHK |
| 3 | 01 | STATUS | PLETH | SpO2 | CHK |
| 4 | 01 | STATUS | PLETH | SREV | CHK |
| 5 | 01 | STATUS | PLETH | reserved | CHK |
| 6 | 01 | STATUS | PLETH | reserved | CHK |
| 7 | 01 | STATUS | PLETH | reserved | CHK |
| 8 | 01 | STATUS | PLETH | BTS | CHK |
| 9 | 01 | STATUS | PLETH | SpO2-D | CHK |
| 10 | 01 | STATUS | PLETH | SpO2 Fast | CHK |
| 11 | 01 | STATUS | PLETH | SpO2 B-B | CHK |
| 12 | 01 | STATUS | PLETH | reserved | CHK |
| 13 | 01 | STATUS | PLETH | reserved | CHK |
| 14 | 01 | STATUS | PLETH | E-HR MSB | CHK |
| 15 | 01 | STATUS | PLETH | E-HR LSB | CHK |
| 16 | 01 | STATUS | PLETH | E-SpO2 | CHK |
| 17 | 01 | STATUS | PLETH | E-SpO2-D | CHK |
| 18 | 01 | STATUS | PLETH | reserved | CHK |
| 19 | 01 | STATUS | PLETH | reserved | CHK |
| 20 | 01 | STATUS | PLETH | HR-D MSB | CHK |
| 21 | 01 | STATUS | PLETH | HR-D LSB | CHK |
| 22 | 01 | STATUS | PLETH | E-HR-D MSB | CHK |
| 23 | 01 | STATUS | PLETH | E-HR-D LSB | CHK |
| 24 | 01 | STATUS | PLETH | reserved | CHK |
| 25 | 01 | STATUS | PLETH | reserved | CHK |

**Figura 2.14 Formato de Datos 2 del Pulso - Oxímetro**

La descripción del byte 2 se detalla como sigue:

| Byte 2: STATUS | | | | | | | |
|---|---|---|---|---|---|---|---|
| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
| 1 | SNSD | ARTF | OOT | SNSA | RPRF | GPRF | SYNC |

**Figura 2.15 Formato del Byte 2 de la Trama de Datos 2 del Pulso Oxímetro**

- SNSD (*Sensor Disconected*): Una ausencia de señal determina que el sensor está desconectado.
- OOT (*Out of track*): Fuera de Seguimiento.
- SNSA (*Sensor Alarm*): Los datos recibidos no pueden ser procesados para su análisis.
- RPRF (*Red Perfusion*): Calidad de señal baja.
- GPRF (*Green Perfusion*): Calidad de señal alta.
- ARTF (*Artifact*): indica la condición del dispositivo.
- Formato Genérico del paquete HR.

| HR MSB | x | x | x | x | x | x | HR8 | HR7 |
|---|---|---|---|---|---|---|---|---|

| HR LSB | x | HR6 | HR5 | HR4 | HR3 | HR2 | HR1 | HR0 |
|---|---|---|---|---|---|---|---|---|

- Formato Genérico del paquete SpO2.

| SpO2 | x | SP6 | SP5 | SP4 | SP3 | SP2 | SP1 | SP0 |
|---|---|---|---|---|---|---|---|---|

- HR: pulso promediado durante 4 latidos, en modo estándar.
- SpO2: nivel de saturación de oxígeno en sangre promediado durante 4 latidos, en modo estándar.
- HR–D: pulso promediado durante 4 latidos, en modo *display*.
- SpO2-D: nivel de saturación de oxígeno en sangre promediado durante 4 latidos, en modo *display*.
- SpO2 Fast: nivel de saturación de oxígeno en sangre promediado durante 4 latidos, no limitado en velocidad de cambio y en modo estándar.
- SpO2 B-B: nivel de saturación de oxígeno en sangre, no limitado en velocidad de cambio, sin promediar y en modo estándar.
- E-HR: pulso promediado durante 8 latidos,
- en modo estándar. promedio de 8 valores en modo estándar.
- E-SpO2: promedio de 8 valores en modo estándar.
- E-HR-D: pulso promediado durante 8 latidos, en modo *display*.
- E-SpO2-D: nivel de saturación de oxígeno en sangre promediado durante 8 latidos, en modo display.
- PLETH: Amplitud de pulso pletismográfico.
- SREV: Nivel de revisión del *Firmware* del Oxímetro.
- BTS: estado de la batería, 01= baja; 00= crítica.

CHK: Checksum = (Byte 1) + (Byte 2) + (Byte 3) + (Byte 4) módulo 256.

Siendo:

- Modo estándar: Valores actualizados con cada latido.
- Modo *display*: Valores actualizados cada 1,5 seg.

*2.5.3.2.3 Sensor de Temperatura*

Este sensor está incluido en una camiseta, la cual funciona mediante *Bluetooth*, percibiendo sensaciones como la temperatura corporal de la persona, y las transmite a un dispositivo receptor *Bluetooth*, como un PC, una PALM o un celular.

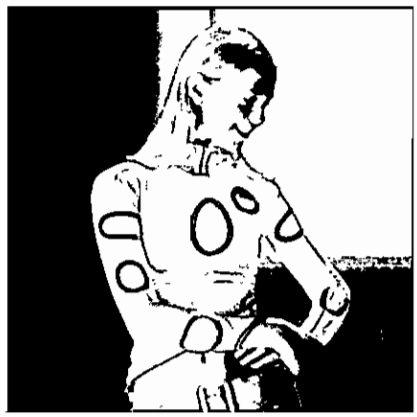


**Figura 2.16 Camiseta *Bluetooth Hug Shirt***

Esta camiseta se llama *Hug Shirt* y es lavable, no tóxica y funciona en cualquier ancho de banda (900 Mhz, 1800 Mhz y demás) y con baterías recargables.

Otra de las soluciones disponibles en el mercado, en cuanto a sensores de temperatura, son los *panties Bluetooth*. Estos *panties* pueden darle su ubicación, temperatura y latidos del corazón, enviando los datos obtenidos por los sensores hacia una PC, o un dispositivo de mano.

**Figura 2.17 Panties *Bluetooth***

Su esquema de componentes se muestra en la figura.

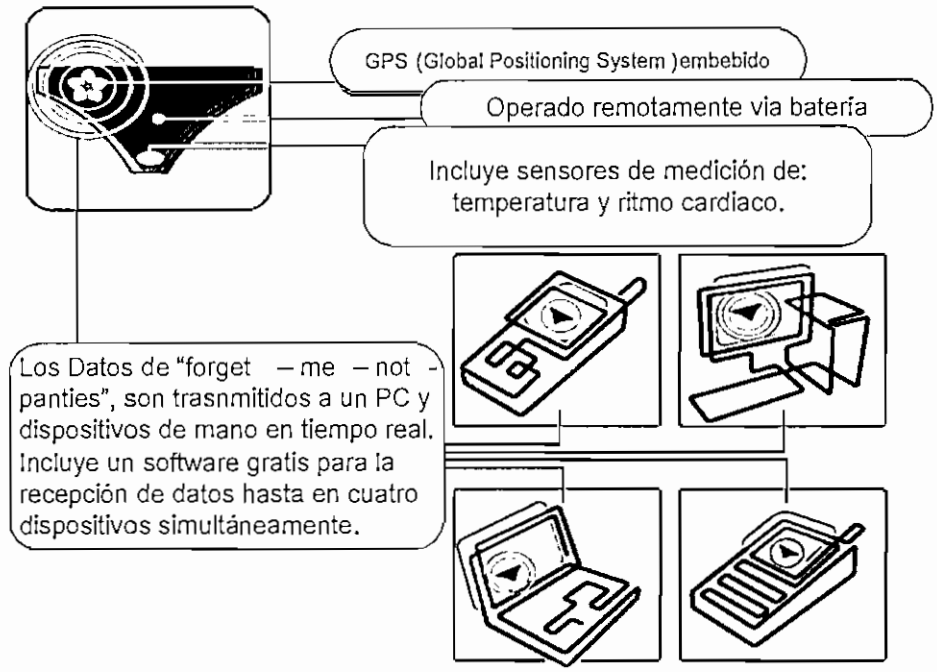



**Figura 2.18 Componentes del Panty *Bluetooth*.**

*2.5.3.2.4 Sensor de Presión*

Este sensor aún no se encuentra disponible en el mercado, sin embargo se considera que si a futuro se lo implementará, y éste trabajará con un formato de trama equivalente al del Pulso – Oxímetro, puede ser agregado a la red de sensores *Bluetooth*.

## 2.5.4 ELEMENTO DE INTERCONEXIÓN DE LA RED HÍBRIDA

En este proyecto se trabaja principalmente con tres tecnologías. *Ethernet* 10/100 Mbps para la red cableada, 802.11g para la red inalámbrica y *Bluetooth* para la red sensores.

La tarjeta PCI *dual wireless*, combina 2 populares tecnologías inalámbricas, WLAN 802.11g y *Bluetooth* v1.2. Permite conectar cualquier dispositivo B*luetooth*, ya sea PDA, celular, etc. a la red, y a la vez transferir datos mediante 802.11g.

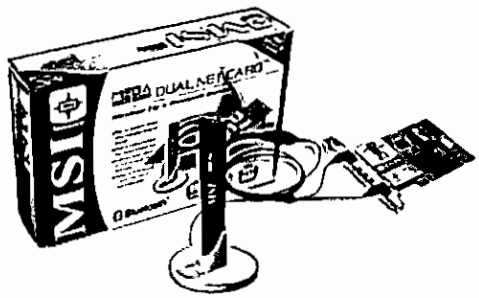



Figura 2.19 Tarjeta Dual MSI *Bluetooth*/IEEE 802.11g.

Sus principales características se resumen a continuación:

| Ítem | Nombre | Descripción |
|---|---|---|
| 1 | Frecuencia | 2.4 – 2.4835 GHz (14 canales) |
| 2 | Velocidades | IEEE 802.11g (Auto – *fallback*): 54, 48, 36, 24, 18, 12, 9, y 6 Mbps.<br>IEEE 802.11b (Auto – *fallback*): 1, 2, 5.5 y 11 Mbps. |
| 3 | Potencia de canal | EIRP < = 20 dB |
| 4 | Seguridad | WEP 64/128 bits |
| 5 | Interfaz | *Wireless* LAN PCI |
| 6 | *Bluetooth* | v1.1 |
| 7 | *Throughput* | Hasta 723 Kbps (Canales de Datos) |
| 8 | Modulación | FHSS |
| 9 | Antena | Hasta 3 dBi |

Tabla 2.14 Características Tarjeta Dual MSI *Bluetooth*/IEEE 802.11g

## 2.6 INGENIERÍA DE DETALLE DEL DISEÑO PROPUESTO

En esta sección se detalla el procedimiento de ingeniería seguido para la elaboración del diseño.

La red híbrida propuesta para la Clínica "Durán" de la ciudad de Ambato, alberga alrededor de 44 usuarios y se la clasifica como una red mediana con pocas perspectivas de crecimiento. Adicionalmente, se considera configurar los mecanismos de seguridad: WEP, filtrado MAC, y servidor *RADIUS*, en los equipos y dispositivos a utilizarse para la solución.

### 2.6.1 LEVANTAMIENTO DE PLANOS

El personal de la clínica, por medio de su propietario, realizó la entrega de los planos del edificio en papel, luego de lo cual, se hizo una visita al lugar para

comprobar y realizar las actualizaciones correspondientes, y ejecutar la digitalización de los mismos. (Anexo 2A).

### 2.6.2 DETERMINACIÓN DE REDES INALÁMBRICAS CERCANAS

Para la realización del diseño híbrido, se efectuó un análisis previo de las interferencias existentes, dadas por las redes inalámbricas cercanas a la edificación, así como de los equipos médicos que trabajan en la misma banda de frecuencia.

A continuación se resume mediante tablas los resultados de dicho análisis. Las tablas y gráficas que respaldan los datos para el resto de la edificación, se muestran en el Anexo 2B.

**Planta Baja**

| NORTE | | | SUR | | |
|---|---|---|---|---|---|
| Red | Canal | V (Mbps) | Red | Canal | V (Mbps) |
| EMMAPA 03 | 6 | 11 | EMMAPA 03 | 6 | 11 |
| PLASTIWAN | 11 | 11 | | | |

**Tabla 2.15** Redes Inalámbricas cercanas a la Planta Baja por Norte y Sur

| ESTE | | | OESTE | | |
|---|---|---|---|---|---|
| Red | Canal | V (Mbps) | Red | Canal | V (Mbps) |
| EMMAPA 03 | 6 | 18 | EMMAPA 03 | 6 | 11 |
| PLASTIWAN | 11 | 18 | | | |
| SPEEDY | 3 | 18 | | | |
| CEN | 8 | 11 | | | |
| WAVELAN | 8 | 18 | | | |

**Tabla 2.16** Redes Inalámbricas cercanas a la Planta Baja por Este y Oeste

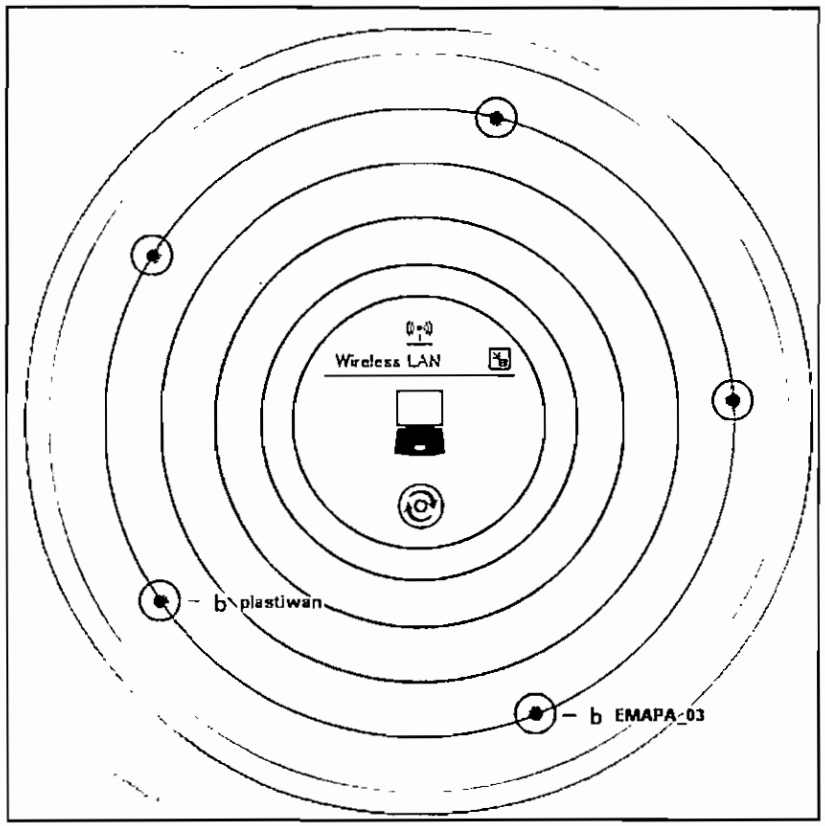



Figura 2.2a Norte

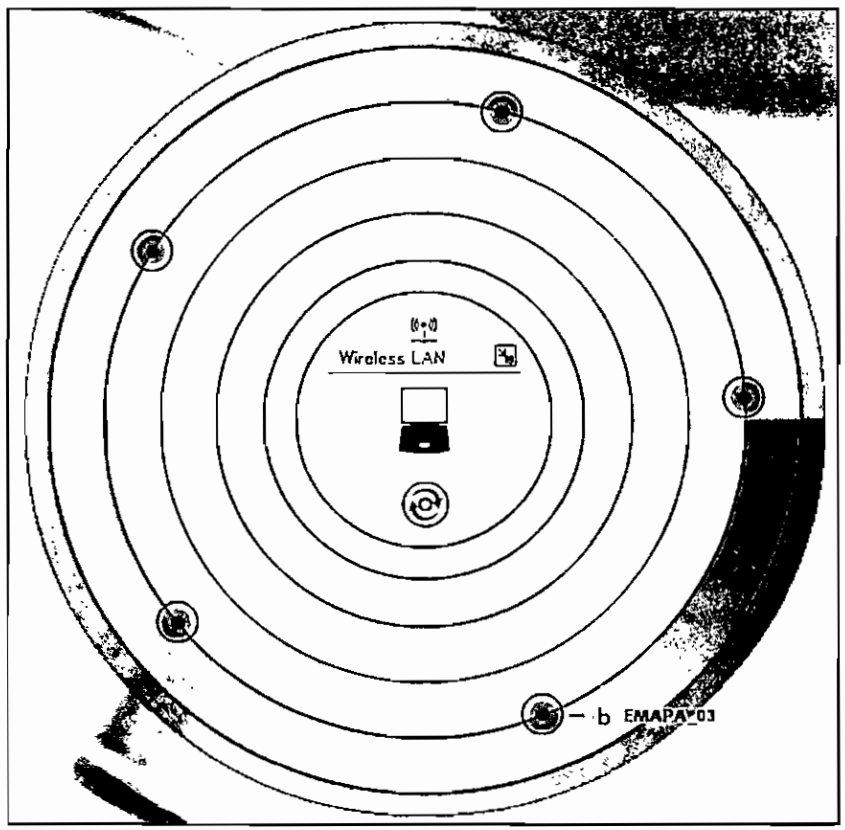



Figura 2.2b Sur

Figura 2.20 Redes inalámbricas cercanas a la Planta Baja

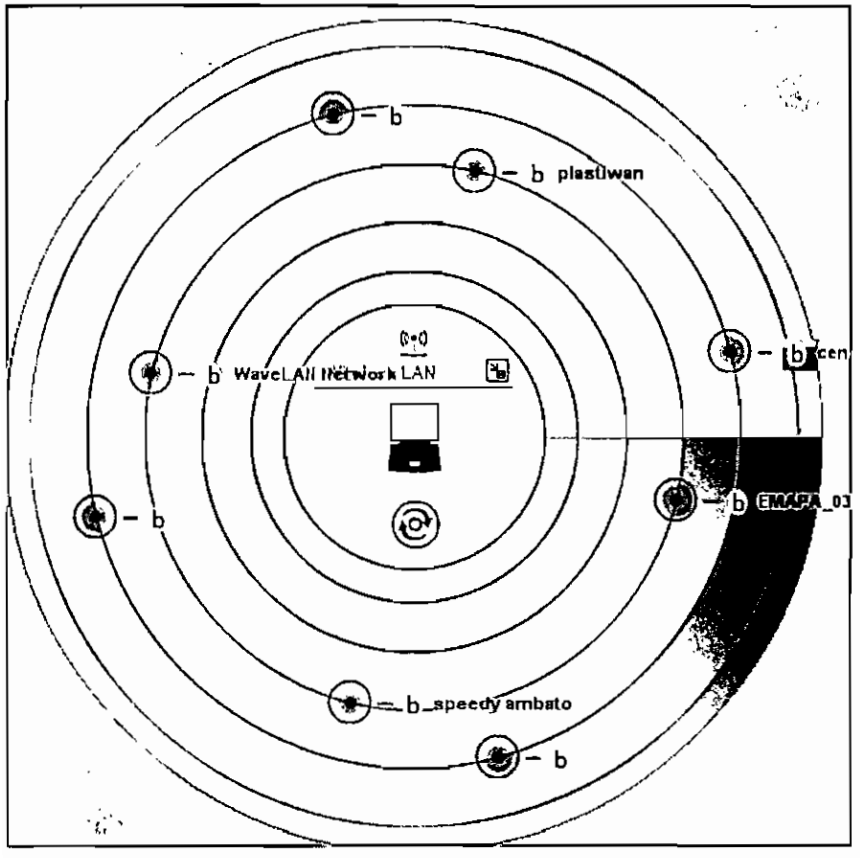



Figura 2.3a Este

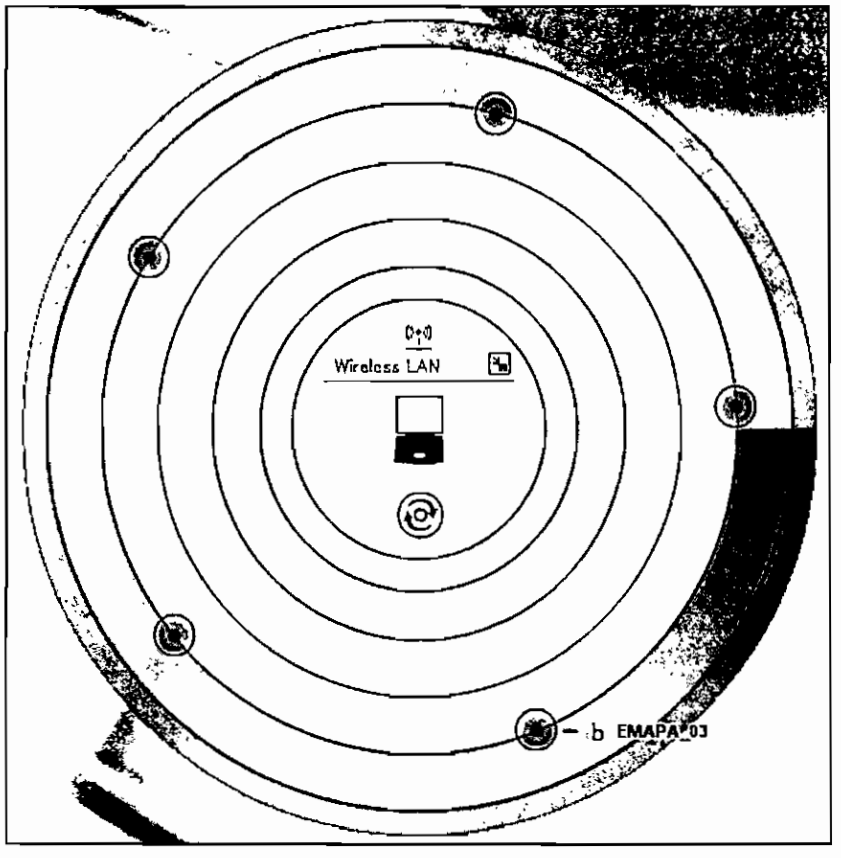



Figura 2.3b Oeste

Figura 2.21 Redes inalámbricas cercanas a la Planta Baja

### 2.6.3 PRUEBAS DE CALIDAD DE SEÑAL

Para el diseño de la red inalámbrica, se realizó un análisis previo de la calidad de señal en los puntos críticos, respecto a diversas ubicaciones del AP, mediante el programa demo *Odyssey Client Manager* Versión 4.32[23].

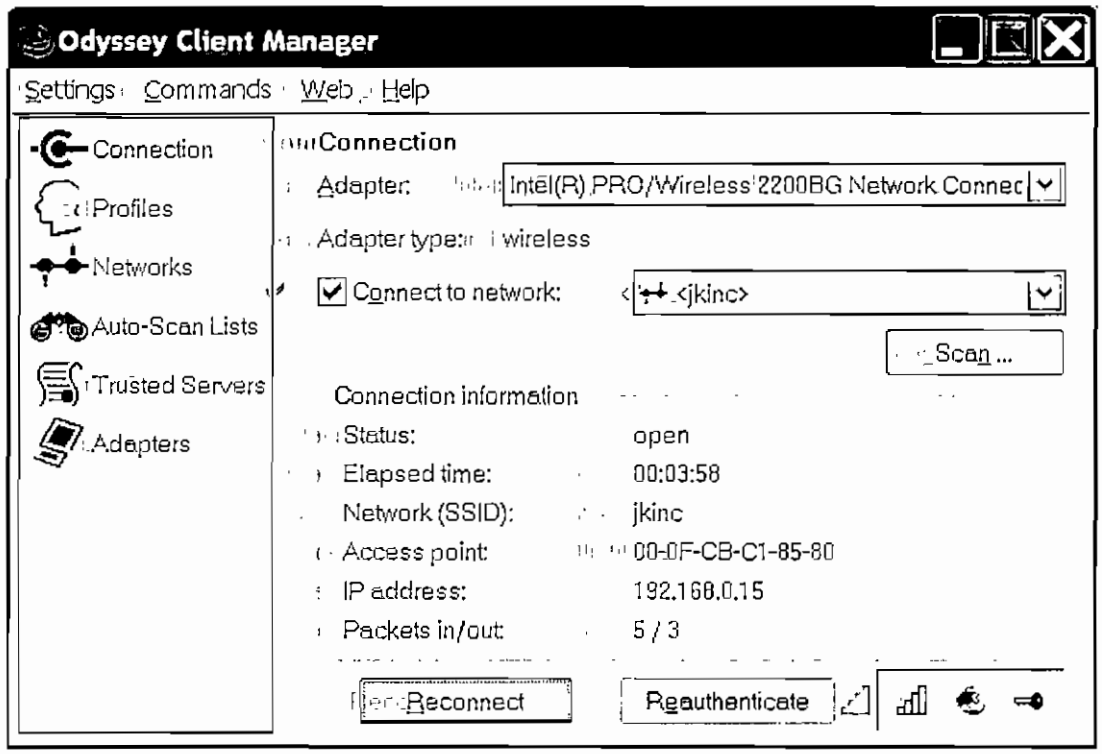



**Figura 2.22 Pantalla de Configuración del Software de Pruebas de Cobertura**

Acorde a las pruebas de ubicación del AP a lo largo de la edificación, se concluye que se requieren dos equipos de interconectividad para cubrir las áreas planteadas, y que el mejor sitio para ubicarlos es la Sala de Espera de la Planta Baja y el Segundo Piso.

A continuación se muestra una gráfica ejemplo de cobertura del AP ubicado en uno de los sitios seleccionados, respecto a Farmacia (Planta Baja).

Las gráficas de resultados de calidad de la señal, para todas las localidades, se encuentran en el Anexo 2C.

[23] www.funksoftware.com

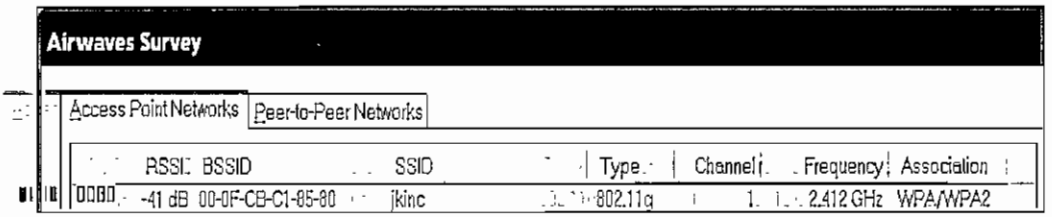



**Figura 2.23 Prueba de Cobertura en Farmacia**

### 2.6.4 DISEÑO DE LA RED INALÁMBRICA

Para el diseño de la red inalámbrica, se consideran el número de computadores que van a acceder a la misma, y los puntos de acceso necesarios para servir a dichos usuarios, acorde al estándar seleccionado en el ítem 2.2.1.3[24].

Se toma en cuenta también, que la edificación incluye un ascensor y equipos médicos que interfieren con la red.

IEEE 802.11g trabaja con 3 canales (1, 6, y 11), y un ancho de banda de 22 MHz[25] por cada uno de ellos.

Acorde a las pruebas de cobertura y calidad de señal realizadas en el edificio, se decide setear al AP1 para que trabaje en el canal 11, y al AP2 en el canal 1, obteniendo cerca de un 10% de superposición de celdas.

#### 2.6.4.1 Número de Adaptadores PCI Inalámbricos

Después de realizar la visita en la Clínica Durán de la ciudad de Ambato, se determinó el número de usuarios de la red que harán uso de una computadora de escritorio.

El número de PCI inalámbricos necesarios, se detalla en la siguiente tabla y acorde a cada piso.

---

[24] Cálculo del Ancho de Banda y Selección de Estándares
[25] SINCHE, Soraya, Redes LAN Inalámbricas

| | LUGAR | Número de Usuarios |
|---|---|---|
| PLANTA BAJA | Emergencia | 2 |
| | Farmacia | 1 |
| | Información | 1 |
| | Camillero | ----- |
| | Sala de Espera | ----- |
| | Consulta Externa | 3 |
| | Eco | 1 |
| | Pediatria | ---- |
| | Monitoreo | ---- |
| | Rayos X | ---- |
| | Tomografía | ----- |
| | Cabina | ---- |
| PRIMER PISO | Suite 1 | 1 |
| | Suite 2 | 2 |
| | Suite 3 | 1 |
| | Suite 4 | 2 |
| | Contabilidad y Adm. | 4 |
| | Utileria | ---- |
| | Sala de Espera | ---- |
| | Enfermeria | 2 |
| | Termo-cuna | 1 |
| | Vestidor Enfermeria | ---- |
| | Estación Enfermería | ---- |
| | Esterilización | ---- |
| | Prep. Ropa | ---- |
| | Vestidor Médicos | ---- |
| | Preparación | ---- |
| | Sala de Partos | ---- |
| | Quirófano 1 | ---- |
| | Quirófano 2 | ---- |
| | Recuperación | ---- |
| SEGUNDO PISO | Suite 5 | 2 |
| | Suite 6 | 1 |
| | Suite 7 | 1 |
| | Suite 8 | 2 |
| | Odontología | 1 |
| | Sala de Espera | ---- |
| | Utileria | ---- |
| TERCER PISO | Habitación 9 | 1 |
| | Habitación 10 | 1 |
| | Habitación 11 | 1 |
| | Habitación Residentes | 3 |
| | Bodega de Farmacia | 2 |
| | Sala de Espera | 2 |
| | Utileria | ---- |
| Total de Adaptadores PCI | | 36 |

Tabla 2.17 Adaptadores Inalámbricos

### 2.6.4.2 Ubicaciones de los Puntos de Acceso

Los puntos de acceso se encuentran distribuidos para cubrir las áreas en donde se requiere conexión, acorde a lo definido en la Tabla 2.1 y a las pruebas de calidad realizadas; a continuación se especifica la ubicación que tendrán los equipos (Tabla 2.18) y su cobertura teórica (Anexo 2D).

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| PLANTA BAJA | 1 | Sala de Espera | AP1 |
| PRIMER PISO | ---- | ---- | ---- |
| SEGUNDO PISO | 1 | Sala de Espera | AP2 |
| TERCER PISO | ---- | ---- | ---- |

Tabla 2.18 Ubicación de los Puntos de Acceso.

Los puntos de acceso se ubican en el techo de los pisos respectivos, lo cual permite a la señal llegar a todos los sitios de cobertura propuestos, sin que el material del ascensor debilite significativamente la señal a su paso por este sitio.

Adicionalmente se tabulan las distancias respecto del AP1 (ubicado en la Planta Baja) y AP2 (ubicado en el Segundo Piso) para brindar una idea de la cobertura global de la red inalámbrica.

| | LOCALIDAD | Distancia (m) |
|---|---|---|
| PLANTA BAJA | Emergencia | 13.85 |
| | Farmacia | 12.85 |
| | Información | 7.9 |
| | Camillero | 1 |
| | Sala de Espera | 13.6 |
| | Consulta Externa | 17.4 |
| | Eco | 16.1 |
| | Pediatría | 17.4 |
| | Monitoreo | 27.3 |
| | Rayos X | 31.9 |
| | Tomografía | 32 |
| | Cabina | 28.6 |

Tabla 2.19 Distancias respecto del AP1 en la planta baja

| | LOCALIDAD | Distancia (m) |
|---|---|---|
| PRIMER PISO | Suite 1 | 17 |
| | Suite 2 | 15 |
| | Suite 3 | 9.8 |
| | Suite 4 | 10.3 |
| | Contabilidad y Adm. | 11.35 |
| | Sala de Espera | 14.05 |
| | Enfermería | 15.90 |
| | Termo-cuna | 18.8 |
| | Vestidor Enfermería | 14.1 |
| | Estación Enfermería | 17.2 |
| | Esterilización | 20.8 |
| | Prep. Ropa | 16 |
| | Vestidor Médicos | 21.1 |
| | Preparación | 22.7 |
| | Sala de Partos | 26.9 |
| | Quirófano 1 | 31.1 |
| | Quirófano 2 | 25.6 |
| | Recuperación | 33.1 |

**Tabla 2.20 Distancias respecto del AP1 en el primer piso**

| | LOCALIDAD | Distancia (m) |
|---|---|---|
| SEGUNDO PISO | Suite 5 | 17 |
| | Suite 6 | 15 |
| | Suite 7 | 9.8 |
| | Suite 8 | 11.4 |
| | Odontología | 9.7 |
| | Sala de Espera | 13.3 |
| | Utilería | 1 |

**Tabla 2.21 Distancias respecto del AP2 en el segundo piso.**

| | LOCALIDAD | Distancia (m) |
|---|---|---|
| TERCER PISO | Habitación 9 | 17.4 |
| | Habitación 10 | 15.4 |
| | Habitación 11 | 10.2 |
| | Habitación Residentes | 11.8 |
| | Bodega de Farmacia | 10.1 |
| | Sala de Espera | 14.7 |
| | Utilería | 1.4 |

**Tabla 2.22 Distancias respecto del AP2 en el tercer piso**

Acorde a la información actual de la ubicación de los equipos médicos, que interfieren con la red inalámbrica, brindada por el personal de la clínica, se

emplean puntos de cableado estructurado en esos sitios, con lo cual se garantiza el adecuado funcionamiento de ambos.

### 2.6.5 DISEÑO DE LA RED DE SENSORES INALÁMBRICOS *ZIGBEE* Y *BLUETOOTH*

En este ítem se analizan dos posibles soluciones para el diseño de la Red de Sensores Inalámbricos (*WSN Wireless Sensor Networks*), contemplando en cada una de ellas sensores para la medición de pulso, ritmo cardíaco, presión y temperatura, acorde a su disponibilidad en el mercado.

Este diseño es únicamente para las áreas de Consulta Externa y Emergencia.

#### 2.6.5.1 Diseño *Zigbee*

*ZigBee* trabaja con velocidades comprendidas entre 20 kB/s y 250 kB/s y rangos de 10 a 75 metros, y puede funcionar en las bandas de 2,4 GHz, 868 MHz y 915 MHz. Puede estar formada por 65.000 nodos, agrupados en subredes de hasta 255 nodos.

Los sensores de *ZigBee* pueden armarse en topologías de red del tipo estrella, malla o mixta, como se estudió en el capítulo anterior. Después de la recolección de datos, éstos pueden ser manipulados por una computadora o ser transmitidos por otras tecnologías inalámbricas, como Wi-Fi o WiMAX.

La elección del protocolo de acceso al medio tiene grandes consecuencias sobre el consumo de potencia del sistema y la latencia de la red.

La topología en estrella que proporciona el estándar 802.15.4, puede ser aplicada a la red que se pretende diseñar, ya que existe un nodo de red que asume el papel de coordinador central (Nodo FFD), y es el encargado de manejar la adquisición y las rutas de comunicación entre los dispositivos.

El estándar 802.15.4 establece que el acceso al medio debe ser CSMA/CA, pero no proporciona ningún método para sincronizar los períodos de actividad e inactividad de los nodos y deja su diseño en manos de los usuarios.

Una clínica debe brindar atención médica permanente y oportuna, ya que unos pocos segundos pueden ser de valiosa importancia para salvar la vida de una persona.

Por tanto se plantea dejar a los nodos siempre en estado de actividad, pudiendo transmitir o recibir tramas en cualquier instante. Pero esta solución es muy costosa en términos de potencia consumida, aunque permitiría una comunicación con una latencia mínima que es lo que se desea tener.

Este planteamiento es realizable siempre y cuando en el mercado, se disponga de sensores que trabajen con baterías de larga duración (varios años). Es por lo tanto recomendable contemplar un tiempo de inactividad del nodo para reducir su consumo de potencia.

El elemento coordinador FFD para este proyecto, es una Placa Procesador/ Radio (Motes), que trabaja con un sensor con capacidad de recolección de datos.

Los sensores de tipo médico para este tipo de coordinadores, aun no se encuentran disponibles en el mercado, existiendo solamente prototipos[26] no disponibles para la venta. Además se requiere de un *gateway* para comunicarse con un PC, una LAN o el Internet.

En la siguiente figura se muestra un diagrama de los componentes de una red de sensores.

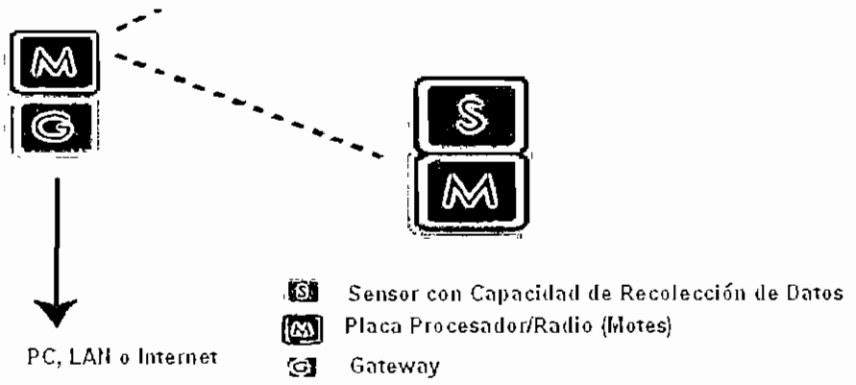



**Figura 2.24 Componentes de una red de sensores *ZigBee*.**

[26] Prototipos elaborados en la Universidad de *Harvard*.

El diseño realizado para las áreas de Consulta Externa y Emergencia, se muestra en la siguiente figura.


**Figura 2.25 Red de Sensores ZigBee**

### 2.6.5.2 Diseño Bluetooth

Una red de sensores inalámbricos *Bluetooth* puede ser implementada en dos topologías de red: *piconets* y *scatternets*.

Una picored puede tomar dos formas: la primera como diseño punto a punto, donde solo existe un maestro y un solo esclavo en la red; y la segunda como un diseño punto – multipunto, donde un maestro es conectado a muchos esclavos en la red.

La figura muestra una arquitectura punto – multipunto, donde el maestro llega a ser la cabeza de la picored y además sirve como controlador central.

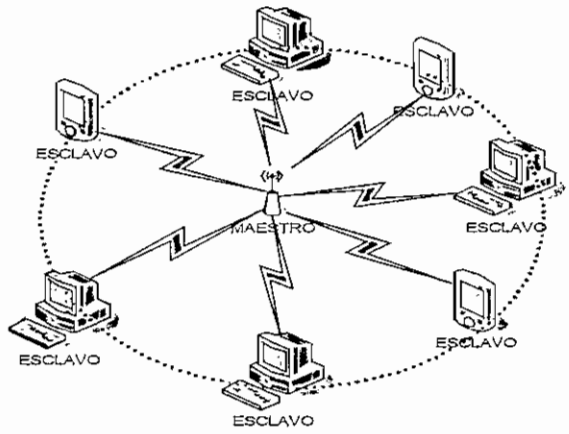



**Figura 2.26 Arquitectura de una Picored *Bluetooth***

Todos los dispositivos de una picored siguen el mismo patrón de salto de frecuencia y sincronismo proveído por el maestro, estableciéndose un enlace directo entre el maestro y el esclavo, pero no entre esclavos.

En una *scatternet*, el maestro de una picored sirve a los esclavos de otra picored, pero ningún dispositivo puede servir como maestro a dos picored. Cuando un esclavo de una picored desea comunicarse con otro esclavo de otra picored, ambos maestros deben involucrarse en el envío de paquetes.

Adicionalmente, es posible que un maestro pueda servir a un esclavo de dos picoredes.

En cada escenario, el Maestro/Esclavo actúa como un puente de red o un ruteador a través de las picoredes, sin embargo cuando se tienen escenarios multi-salto, se produce degradación de la señal debido a la interferencia de las picoredes adyacentes.

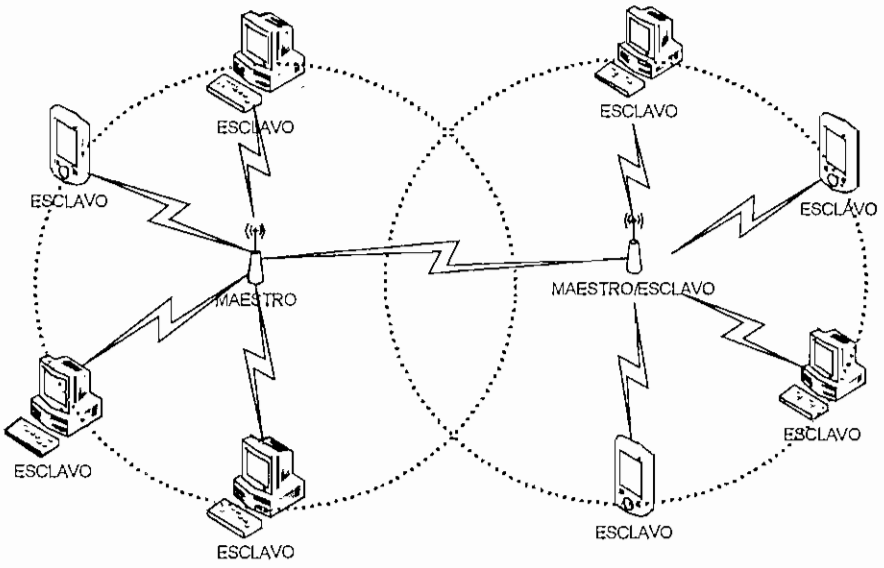



**Figura 2.27 Arquitectura de una *scatternet Bluetooth***

Para este proyecto, se plantea la utilización de la topología punto-multipunto, en la cual el dispositivo central es un AP *Bluetooth* y los esclavos son cada uno de los sensores que toman datos de los signos vitales.

Este esquema se presenta en la figura siguiente.

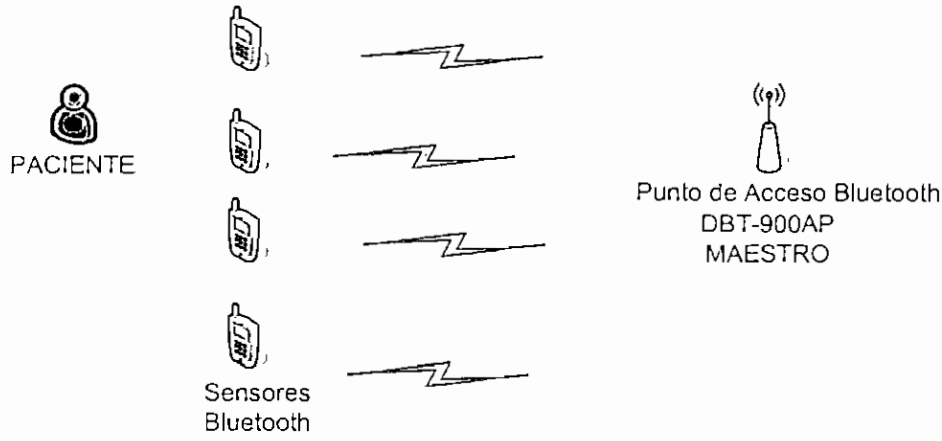



Figura 2.28 Esquema de la red de sensores *Bluetooth*

## 2.6.6 SELECCIÓN DE UNO DE LOS DISEÑOS DE LA RED DE SENSORES PROPUESTAS

Luego de plantear las dos posibles soluciones de diseño para la red de sensores, se analizan y comparan las características de ambas tecnologías acorde a las necesidades de la red, y se justifican los motivos por los cuales se descarta una de ellas.

En la siguiente tabla, se resume las características de mayor relevancia de *Bluetooth* y *ZigBee*.

| Estándar | Requerimientos Mínimos[27] | *Bluetooth* | *ZigBee* |
|---|---|---|---|
| Aplicación principal | WPAN | WPAN | Control y monitorización |
| Vida Batería (días) | 45 | 30 - 60 | 100 – 1000+ |
| Tamaño de la red (nodos) | 4 | 7 | 255 / 65000 |
| Velocidad (Kbps) | - | 720 Kbps | 250 Kbps |
| Cobertura (m) | 4.6 (m) | 10 (v 1.1) (m) | 1 – 100 (m) |

Tabla 2.23 Características de *Bluetooth* y *ZigBee*

*ZigBee* fue creado para control y monitorización, proporciona menos velocidad que *Bluetooth* y actualmente no admite voz ni vídeo, pero permite un mayor alcance. Adicionalmente *Bluetooth* esta introduciéndose en el campo de

[27] 2.5.3.2 *Elementos Bluetooth*

monitoreo, mediante estudios y prototipos propuestos y poniendo a disposición unos pocos dispositivos para ello.

*ZigBee* resulta ideal para redes estáticas, escalables, con muchos dispositivos, pocos requisitos de ancho de banda y uso infrecuente. Por otro lado, *Bluetooth* trabaja con pocos dispositivos, sin embargo permite que éstos puedan moverse y utilizarse frecuentemente.

*ZigBee* define sensores que incluyen baterías con autonomía muy elevada, ya que están programados para que solo se despierten durante frecuencias de segundo para realizar la emisión/recepción. En *Bluetooth* en cambio, los dispositivos deben permanecer despiertos y en posible movimiento, lo que origina un mayor consumo de batería.

En *ZigBee* no se define un protocolo de enrutamiento, lo que ocasiona que la estación base no alcance a todos los nodos de la red, por tanto cada uno de ellos debe actuar como *router* para encaminar los paquetes.

Como solución a este inconveniente, varios autores plantean una nueva topología llamada malla (*full mesh*) en combinación con la actualización dinámica de tabla de rutas, sin embargo esto introduce una mayor latencia en la red e implica que los dispositivos deban tener mayor capacidad de procesamiento.

Ambas tecnologías tienen un control centralizado del intercambio de la información, lo que introduce un único punto de falla, si el nodo central deja de funcionar, la red también lo hace.

Para este proyecto se requiere trabajar en tiempo real, lo que implica tener la menor latencia posible y con ello garantizar la disponibilidad de la información.

Las dos tecnologías definen adecuadamente en sus respectivos estándares, varios mecanismos de seguridad, pero los fabricantes de los dispositivos, al implementarlos no incluyen toda la pila del protocolo y ocasionan vulnerabilidades.

Después de realizar un análisis tanto a la tecnología *Bluetooth* como *ZigBee*, se ha decidido descartar la segunda por las siguientes razones:

- *ZigBee* tienen problemas de heterogeneidad con hardware, incompatibilidad, sistemas operativos diferentes. Ej.: una mote mica2 es incapaz de comunicarse con una *Mote MicaZ*.
- En *ZigBee* no existen protocolos estandarizados que permitan a las aplicaciones interoperar y peor aún APIs estándar para la portabilidad de las aplicaciones.
- En *ZigBee* la red es estática, por lo cual es inapropiada para este proyecto, ya que se requiere movilidad permanente de los nodos.
- Actualmente se dispone de plataformas base sobre las cuales trabajan los dispositivos de medición. En el mercado, se tienen a la venta sensores en los campos de: agricultura, ganadería, y control de edificios inteligentes; más no existen sensores de cuidado médico, éstos solo se hallan en proyectos de estudio y prototipos.
- Para este proyecto se requiere interconectar las redes 802.11g y la red de sensores, pero en el mercado se dispone solo de tarjetas duales para interconexión de redes 802.11g y *Bluetooth*.
- *ZigBee* introduce un alto grado de latencia, debido a que cada nodo debe actuar como enrutador, impidiendo trabajar en tiempo real.

Finalmente, la tecnología seleccionada es *Bluetooth*, ya que en este proyecto se desea trabajar con pocos nodos y alta velocidad de transmisión, además que se cuenta con los sensores médicos y los APIs adecuados para elaborar la aplicación.

### 2.6.7 DISEÑO DE LA RED CABLEADA

El diseño de la red cableada, se lo hace acorde al estándar seleccionado en el literal 2.2.1.3[28] y tomando en cuenta las ubicaciones de cada uno de los puestos de trabajo de los usuarios de la red; los cuales requieren puntos de voz para

[28] Cálculo del Ancho de Banda y Selección de Estándares

conexión telefónica y puntos de datos en el caso de estar en sitios críticos, donde el diseño de la red inalámbrica no es la solución adecuada.

En el diseño del cableado estructurado, se muestran las ubicaciones de los respectivos Puntos de Acceso, cuya conexión al *Rack* principal es cableada. Luego de la definición de ubicaciones, se realizan los cálculos para determinar los elementos a utilizarse en este proyecto. Finalmente, se presenta una tabla de resumen que muestra el contenido de esta sección.

### 2.6.7.1 Definición de Ubicaciones

En primera instancia, se debe definir las ubicaciones de los puntos que requieren la solución cableada como conexión, las cuales se muestran a continuación.

**PUNTOS VOZ PARA USUARIO**

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| PLANTA BAJA | 2 | Emergencia | PB-V001 - PB-V002 |
| | 1 | Farmacia | PB-V003 |
| | 2 | Información | PB-V004 - PB-V005 |
| | 1 | Consulta Externa | PB-V006 - PB-V007 - PB-V008 |
| | 1 | Eco | PB-V009 |
| | 1 | Sala de Sesiones | PB-V010 |
| | 1 | Cabina | PB-V011 |

**Tabla 2.24 Ubicación Puntos de voz Planta Baja**

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| PRIMER PISO | 1 | Suite 1 | P1-V001 |
| | 1 | Suite 2 | P1-V002 |
| | 1 | Suite 3 | P1-V003 |
| | 2 | Suite 4 | P1-V004 - P1-V005 |
| | 4 | Contabilidad y Admin | P1-V006 - P1-V007 - P1-V008 - P1-V009 |
| | 2 | Enfermería | P1-V010 - P1-V011 |
| | 1 | Termo-cuna | P1-V012 |
| | 1 | Vestidor Médicos | P1-V013 |
| | 1 | Preparación | P1-V014 |
| | 1 | Sala de Partos | P1-V015 |
| | 1 | Quirófano 2 | P1-V016 |
| | 1 | Quirófano 1 | P1-V017 |
| | 2 | Recuperación | P1-V018 - P1-V019 |

**Tabla 2.25 Ubicación Puntos de voz Primer Piso**

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| SEGUNDO PISO | 1 | Suite 5 | P2-V001 |
| | 1 | Suite 6 | P2-V002 |
| | 1 | Suite 7 | P2-V003 |
| | 1 | Suite 8 | P2-V004 |
| | 1 | Odontología | P2-V005 |
| | 2 | Sala de Espera | P2-V006 - P2-V007 |
| | 1 | Utilería | P2-V008 |

**Tabla 2.26 Ubicación Puntos de voz Segundo Piso**

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| TERCER PISO | 1 | Habitación 9 | P3-V001 |
| | 1 | Habitación 10 | P3-V002 |
| | 1 | Habitación 11 | P3-V003 |
| | 1 | Residentes | P3-V004 |
| | 1 | Bodega Farmacia | P3-V005 |
| | 2 | Sala de Espera | P3-V006 -P3-V007 |
| | 1 | Utilería | P3-V008 |

**Tabla 2.27 Ubicación Puntos de voz Tercer Piso**

## PUNTOS DATOS PARA USUARIO

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| PLANTA BAJA | 1 | Eco | PB-D001 |
| | 2 | Cabina | PB-D002 - PB-D003 |
| PRIMER PISO | 1 | Recuperación | P1-D001 |

**Tabla 2.28 Ubicación Puntos de DATOS de usuario**

## PUNTOS DE DATOS PARA CONEXIÓN DE PUNTOS DE ACCESO

| LOCALIDAD | CANTIDAD | UBICACIÓN | IDENTIFICADOR |
|---|---|---|---|
| PLANTA BAJA | 1 | Sala de Espera | AP1 |
| PRIMER PISO | ---- | ---- | ---- |
| SEGUNDO PISO | 1 | Sala de Espera | AP2 |
| TERCER PISO | ---- | ---- | ---- |

**Tabla 2.29 Ubicación Puntos de DATOS de los Puntos de Acceso**

### 2.6.7.2 Patch Cords

En el primer piso, se ubicará un pequeño armario de comunicaciones, el cual conectará un patch panel de 48 puertos (voz y datos). Hay 6 puntos de datos que serán conectados a sus respectivos *face plate* que llegarán a un *Switch* 3COM de 24 puertos existente en la clínica, por tanto se requiere 6 *patch cords* de 3 pies.

### 2.6.7.3 Número de Corridas

El número de corridas nos permite definir la cantidad de cable UTP a utilizarse en el diseño de cableado estructurado. Existen dos métodos para determinar el número de corridas: el método exacto o el método aproximado.

#### *2.6.7.3.1 Método Exacto*

Este método consiste en determinar la distancia desde cada punto de acceso hasta el closet de comunicaciones, considerando una reserva de 2 metros para las instalaciones, 0.50 m en las ubicaciones de puntos de acceso y 2.50 m en el closet de comunicaciones.

Los resultados que se obtuvo tanto para los puntos de usuario de datos que requieren una conexión cableada como los puntos de conexión de los Puntos de Acceso, se los muestra en la siguiente tabla, considerando distancias y reservas.

# DISEÑO DE CABLEADO ESTRUCTURADO PARA USUARIO (VOZ, DATOS)

## *PLANTA BAJA*

| | LUGAR | PUNTOS DE VOZ | NOMBRE | DISTANCIA (mt) | RESERVA (mt) | PUNTOS DE DATOS | NOMBRE | DISTANCIA (mt) | RESERVA (mt) |
|---|---|---|---|---|---|---|---|---|---|
| PLANTA BAJA | Emergencia | 1 | PB-V001 | 25,75 | 3 | ----- | | ---- | ----- |
| | Emergencia | 1 | PB-V002 | 17,55 | 3 | ----- | ----- | ----- | ----- |
| | Farmacia | 1 | PB-V003 | 25,8 | 3 | ----- | ----- | ---- | ----- |
| | Información | 1 | PB-V004 | 14,95 | 3 | ----- | ----- | ---- | ----- |
| | Información | 1 | PB-V005 | 16,26 | 3 | ----- | ----- | ----- | ----- |
| | Camillero | ----- | ---- | ---- | ----- | ---- | ---- | ---- | ----- |
| | Sala de Espera | ----- | ----- | ---- | ----- | ----- | ----- | ---- | ----- |
| | Consulta Externa | 1 | PB-V006 | 34,7 | 3 | ---- | ---- | ----- | ----- |
| | Consulta Externa | 1 | PB-V007 | 30,9 | 3 | ---- | ---- | ---- | ---- |
| | Consulta Externa | 1 | PB-V008 | 27,6 | 3 | ----- | ---- | ----- | ----- |
| | Eco | 1 | PB-V009 | 25,8 | 3 | 1 | PB-D001 | 25,8 | 3 |
| | Monitoreo | ----- | ---- | ---- | ----- | ----- | ---- | ----- | ----- |
| | Maquinaria | ---- | ---- | ---- | ----- | ----- | ---- | ----- | ----- |
| | Rayos X | ---- | ----- | ----- | ----- | ----- | ---- | ----- | ---- |
| | Tomografía | ----- | ---- | ---- | ----- | ----- | ---- | ----- | ---- |
| | Cabina | 1 | PB-V011 | 40,9 | 3 | 1 | PB-D002 | 41,4 | 3 |
| | Cabina | ----- | ---- | ----- | ----- | 1 | PB-D003 | 41,4 | 3 |
| | Pediatría | 1 | PB-V010 | 29,1 | 3 | ---- | ---- | ----- | ----- |
| | TOTALES | 11 | ---- | 289.31 | 33 | 3 | ----- | 108.6 | 9 |

Tabla 2.30 Cableado Estructurado para la Planta Baja

## *PRIMER PISO*

| | LUGAR | PUNTOS DE VOZ | NOMBRE | DISTANCIA (mt) | RESERVA (mt) | PUNTOS DE DATOS | NOMBRE | DISTANCIA (mt) | RESERVA (mt) |
|---|---|---|---|---|---|---|---|---|---|
| PRIMER PISO | Suite 1 | 1 | P1-V001 | 24 | 3 | ---- | | | |
| | Suite 2 | 1 | P1-V002 | 24 | 3 | ----- | | | |
| | Suite 3 | 1 | P1-V003 | 15,1 | 3 | ----- | | | |
| | Suite 4 | 1 | P1-V004 | 11,7 | 3 | ----- | | | |
| | Suite 4 | 1 | P1-V005 | 7,05 | 3 | ----- | | | |
| | Contab. y Adm. | 1 | P1-V006 | 14,95 | 3 | ----- | | | |
| | Contab. y Adm. | 1 | P1-V007 | 18,65 | 3 | ----- | | | |
| | Contab. y Adm. | 1 | P1-V008 | 7,8 | 3 | ----- | | | |
| | Contab. y Adm. | 1 | P1-V009 | 7,2 | 3 | ----- | | | |
| | Utilería | ---- | ----- | ---- | ---- | ----- | | | |
| | Sala de Espera | ---- | ----- | ---- | ---- | ----- | | | |
| | Enfermería | 1 | P1-V010 | 21,9 | 3 | ----- | | | |
| | Enfermería | 1 | P1-V011 | 22 | 3 | ----- | | | |
| | Termo-cuna | 1 | P1-V012 | 25,6 | 3 | ----- | | | |
| | Vestidor Enfermería | ----- | ----- | ----- | ---- | ----- | | | |
| | Estación Enfermería | ----- | ----- | ----- | ---- | ----- | | | |
| | Esterilización | ----- | ----- | ----- | ---- | ----- | | | |
| | Prep. Ropa | ----- | ----- | ----- | ---- | ----- | | | |
| | Vestidor Médicos | 1 | P1-V013 | 26,4 | 3 | ----- | | | |
| | Preparación | 1 | P1-V014 | 29,3 | 3 | ----- | | | |
| | Sala de Partos | 1 | P1-V015 | 35,3 | 3 | ----- | | | |
| | Quirófano 1 | 1 | P1-V017 | 42,7 | 3 | ----- | | | |
| | Quirófano 2 | 1 | P1-V016 | 37,1 | 3 | ----- | | | |
| | Recuperación | 1 | P1-V018 | 35,5 | 3 | 1 | P1-D001 | 41 | 3 |
| | Recuperación | 1 | P1-V019 | 41,1 | 3 | ----- | ---- | | |
| | **TOTAL** | **19** | ----- | **447.35** | **57** | 1 | ----- | 41 | **3** |

Tabla 2.31 Cableado Estructurado para el Primer

## *SEGUNDO PISO*

| | LUGAR | PUNTOS DE VOZ | NOMBRE | DISTANCIA (mt) | RESERVA (mt) | PUNTOS DE DATOS | NOMBRE | DISTANCIA (mt) | RESERVA (mt) |
|---|---|---|---|---|---|---|---|---|---|
| SEGUNDO PISO | Suite 5 | 1 | P2-V001 | 33,4 | 3 | ----- | ----- | ----- | ----- |
| | Suite 6 | 1 | P2-V002 | 33,7 | 3 | ----- | ----- | ----- | ----- |
| | Suite 7 | 1 | P2-V003 | 23,9 | 3 | ----- | ----- | ----- | ----- |
| | Suite 8 | 1 | P2-V004 | 25 | 3 | ----- | ----- | ----- | ----- |
| | Odontología | 1 | P2-V005 | 23 | 3 | ----- | ----- | ----- | ----- |
| | Sala Espera | 1 | P2-V006 | 11,5 | 3 | ----- | ----- | ----- | ----- |
| | Sala Espera | 1 | P2-V007 | 20,3 | 3 | ----- | ----- | ----- | ----- |
| | Utilería | ----- | ---- | ---- | ----- | ----- | ----- | ----- | ----- |
| TOTAL | | 7 | ---- | 170.8 | 21 | 0 | ---- | 0 | 0 |

**Tabla 2.32 Cableado Estructurado para el Segundo Piso**

## *TERCER PISO*

| | LUGAR | PUNTOS DE VOZ | NOMBRE | DISTANCIA (mt) | RESERVA (mt) | PUNTOS DE DATOS | NOMBRE | DISTANCIA (mt) | RESERVA (mt) |
|---|---|---|---|---|---|---|---|---|---|
| TERCER PISO | Habitación 9 | 1 | P3-V001 | 38,4 | 3 | ---- | ----- | ---- | |
| | Habitación 10 | 1 | P3-V002 | 38,7 | 3 | ----- | ----- | ---- | ----- |
| | Habitación 11 | 1 | P3-V003 | 28,9 | 3 | ----- | ----- | ----- | ----- |
| | Habitación R | 1 | P3-V004 | 33 | 3 | ----- | ----- | ----- | ----- |
| | Bodega Farmacia | 1 | P3-V005 | 28 | 3 | ----- | ----- | ----- | ---- |
| | Sala de Espera | 1 | P3-V006 | 16,5 | 3 | ----- | ----- | ----- | ----- |
| | Sala de Espera | 1 | P3-V007 | 25,3 | 3 | ----- | ----- | ----- | ----- |
| | Utilería | ---- | ---- | ---- | ---- | ----- | ----- | ----- | ---- |
| TOTAL | | 7 | ---- | 208.8 | 21 | 0 | ---- | 0 | 0 |

**Tabla 2.33 Cableado Estructurado para el Tercer Piso**

# DISEÑO DE CABLEADO ESTRUCTURADO CONEXIÓN DE PUNTOS DE ACCESO

| DISEÑO CABLEADO ESTRUCTURADO PUNTOS DE ACCESO | | | | |
|---|---|---|---|---|
| LOCALIDAD | NOMBRE | UBICACIÓN | DISTANCIA (m) | RESERVA (m) |
| PLANTA BAJA | AP1 | Sala de Espera | 25 | 3 |
| PRIMER PISO | ----- | ----- | ----- | ----- |
| SEGUNDO PISO | AP2 | Sala de Espera | 40 | 3 |
| TERCER PISO | ----- | ----- | ----- | ----- |
| TOTAL | | | 65 | 6 |

Tabla 2.34 Cableado Estructurado para los Puntos de Acceso

De las tablas se puede obtener totales tanto de puntos como de metros de cable:

| Ítem | Puntos de Voz | Puntos de Datos | Puntos interconexión APs | Total |
|---|---|---|---|---|
| Puntos | 44 | 4 | 2 | 50 |
| Cable (metros) | 1248.26 | 1616 | 71 | 1480.86 |

**Tabla 2.35 Totales de puntos y metros de cable**

Realizando el cálculo con la siguiente expresión:

N° rollos= Total metros/ 305 m

**Ecuación 2.2 Cálculo Número de Rollos**

N° rollos= 1480.86/ 305 m

N° rollos = 4.85

Entonces se tiene que se utilizarán 5 rollos de cable UTP.

*2.6.7.3.2 Método Aproximado*

Para determinar la cantidad de rollos a utilizarse, usando el método aproximado, se debe seguir el siguiente procedimiento:

Primero se determinan las distancias críticas:

- Distancia al punto más lejano (dmax).
- Distancia al punto más cercano (dmin).

Los valores determinados son:

dmax = 41.4 m.

dmin= 7.05 m.

Se debe sumar y dividir para 2 ambos valores de distancia, añadir un 10% de holgura, y 2.5 m para la terminación.

$$D' = \frac{d\max + d\min}{2}$$

**Ecuación 2.3 Cálculo de distancias D'**

$$D' = \frac{41.4m + 7.05m}{2} \longrightarrow \text{D'= 24.23 m}$$

Se calcula el D", de la siguiente manera:

$$D'' = D' + 10\% + 2.5$$

**Ecuación 2.4 Cálculo de distancias D"**

$$D'' = 24.23 + 2.42 + 2.5 \longrightarrow D'' = 29.15$$

El número de corridas Q, se obtiene dividiendo el número total de metros que tiene el rollo para D". Se debe aproximar el resultado, al inmediato inferior debido a que no se deben tener corridas incompletas.

$$Q = \frac{305}{D''}$$

**Ecuación 2.5 Cálculo Número de Corridas**

$$Q = \frac{305}{29.15} = 10.464$$

La cantidad de bobinas o rollos, se calculan de la siguiente forma:

$$R = \frac{\#salidas}{Q}$$

**Ecuación 2.6 Cálculo cantidad de rollos**

$$R = \frac{50}{10.464} = 4.78 rollos \approx 5 rollos$$

El número de salidas se calcula tomando en cuenta todos los valores de puntos de servicio que se van a tener, ya sea: voz, datos, puntos de acceso.

Del valor obtenido se tiene que se debe utilizar 5 rollos de cable UTP cat. 6. Se puede concluir que ambos métodos no difieren.

#### 2.6.7.4 Armario de Comunicaciones

Para esta solución, por ser un cableado de pocas salidas de usuario, se va a disponer de un pequeño armario de comunicaciones para todo el diseño, en el constarán: 1 *Switch* 3COM de 24 puertos, 1 *Patch Panel* de 48 puertos.

Se tendrá un total de 2 HU[29] de dimensión:

1 HU=1.75 pulgadas

2 HU= 3.50 pulg.

#### 2.6.7.5 Canaletas

Las distancias estimadas para la canalización de vistas de pared, se detallan en la siguiente tabla:

| Piso | Total Canaleta Metálica (m) | Total Canaleta Plástica (m) |
|---|---|---|
| Planta Baja | 46.1 | 19.75 |
| Primer Piso | 42.3 | 46.83 |
| Segundo Piso | 29.15 | 13.9 |
| Tercer Piso | 29.15 | 13.9 |
| TOTAL | **146.7** | **108.58** |

**Tabla 2.36 Cantidad total de canaletas.**

En el Anexo 2E se puede apreciar el diseño completo de la red cableada, y en el Anexo 2F un esquema de funcionamiento de la red hibrida en su totalidad.

### 2.6.8 RESUMEN DE REQUERIMIENTOS

La lista de requerimientos a utilizarse en el diseño de cableado estructurado cat. 6, para este proyecto, se detallan en la siguiente tabla:

[29] Unidad de *Rack*.

| Ítem | Descripción | Cant. |
|---|---|---|
| A | **RED INALAMBRICA 802.11g** | |
| A.1 | PUNTO DE ACCESO 3COM OFFICECONNECT WIRELESS 108 MBPS 11G. | 1 |
| A.2 | ADAPTADOR DE RED USB | 36 |
| B | **RED DE SENSORES *BLUETOOTH*** | |
| B.1 | PUNTO DE ACCESO *BLUETOOTH* | 2 |
| B.2 | TARJETA DE RED DUAL | 2 |
| B.3 | SENSOR DE PULSO *BLUETOOTH* | 2 |
| B.4 | SENSOR DE RITMO CARDIACO *BLUETOOTH* | 2 |
| B.5 | SENSOR DE TEMPERATURA *BLUETOOTH* | 2 |
| B.6 | SENSOR DE PRESIÓN *BLUETOOTH* | 2 |
| C | **RED CABLEADA** | |
| 1 | **SISTEMA HORIZONTAL** | |
| 1.1 | PATCH CORD 3 PIES | 6 |
| 1.2 | JACK RJ45 Cat. 6 | 12 |
| 1.3 | CABLE UTP 4 PARES Cat. 6 (metros) | 1409,86 |
| 1.4 | PATCH PANEL MODULAR 48 PUERTOS | 1 |
| 1.5 | RACK MURAL MUPM DE 10" Cat. 6 | 1 |
| 1.6 | MATERIALES MENORES(AMARRAS PLASTICAS, TORNILLOS, ETC) | 1 |
| 2 | **CANALETAS PLASTICAS** | |
| 1.1 | CANALETA METALICA 16X10 (metros) | 146,7 |
| 1.2 | CANALETA DE 2 m PARA 2 CABLES UTP Cat. 6 TIPO PANDUIT (metros) | 108,58 |
| 1.3 | ACCESORIOS CANALETAS | 100 |
| 1.4 | MATERIALES MENORES (ANILLADO PLASTICO, TORNILLOS, tacos, ETC) | 1 |
| 3 | **TRABAJOS DE INSTALACION Y PUESTA EN MARCHA** | |
| 3,2 | INSTALACION CANALETA (metros) | 255,28 |
| 3,3 | INSTALACION Y CONFIGURACION | 1 |
| 3,4 | PUNTO DE CABLEADO ESTRUCTURADO CAT 6 | 50 |
| 3,5 | PLANOS AS BUILT | 4 |
| 3,6 | Certificación Puntos Cat. 6 | 50 |
| 3.7 | DIRECCION TECNICA | 1 |

**Tabla 2.37 Resumen de Requerimientos para elaborar la red hibrida.**

## 2.7 COSTOS DEL DISEÑO DE LA RED HÍBRIDA

Para la realización del presupuesto necesario para el diseño de la red hibrida propuesto, se analizan: costos de los equipos y elementos, costo de instalación y configuración, y el costo de mano de obra.

### 2.7.1 PRESUPUESTO

Las siguientes tablas, se resume la cantidad y precios de los equipos y elementos necesarios para el diseño planteado.

| Ítem | Descripción | Cant. | V Unit. | V Total |
|---|---|---|---|---|
| A | RED INALAMBRICA 802.11g | | | |
| A.1 | PUNTO DE ACCESO 3COM OFFICECONNECT WIRELESS 108 MBPS 11G POE. | 2 | $ 156,95 | $ 313,90 |
| A.2 | ADAPTADOR DE RED USB | 36 | $ 41 | $ 1.476,00 |
| A.3 | LICENCIA SERVIDOR RADIUS | 1 | $ 2.350 | $ 2.350,00 |
| A.4 | LICENCIA CLIENTE RADIUS | 44 | $ 50 | $ 200,00 |
| | | SUBTOTAL | | $ 4.339,90 |
| | | IVA | | $ 520,79 |
| TOTAL | | | | $ 4.860,69 |

Tabla 2.38 Presupuesto para elaborar la red inalámbrica

| Ítem | Descripción | Cant | V Unit. | V Total |
|---|---|---|---|---|
| B | RED DE SENSORES BLUETOOTH | | | |
| B.1 | PUNTO DE ACCESO BLUETOOTH | 2 | $ 75,25 | $ 150,50 |
| B.2 | TARJETA DE RED DUAL | 2 | $ 39,75 | $ 79,50 |
| B.3 | SENSOR DE PULSO BLUETOOTH | 2 | $ 275,00 | $ 550,00 |
| B.4 | SENSOR DE RITMO CARDIACO BLUETOOTH | 2 | $ 275,00 | $ 550,00 |
| B.5 | SENSOR DE TEMPERATURA BLUETOOTH | 2 | N/D | N/D |
| B.6 | SENSOR DE PRESIÓN BLUETOOTH | 2 | N/D | N/D |
| | | SUBTOTAL | | $ 1.330,00 |
| | | IVA | | $ 159,60 |
| TOTAL | | | | $ 1.489,60 |

Tabla 2.39 Presupuesto para elaborar la red de sensores

| Ítem | Descripción | Cant | V Unit. | V Total |
|---|---|---|---|---|
| C | RED CABLEADA | | | |
| 1 | SISTEMA HORIZONTAL | | | |
| 1.1 | PATCH CORD 3 PIES | 6 | $ 4,26 | $ 25,56 |
| 1.2 | JACK RJ45 Cat. 6 | 12 | $ 0,50 | $ 6,00 |
| 1.3 | CABLE UTP 4 PARES Cat. 6 (metros) | 1409,86 | $ 0,34 | $ 479,35 |
| 1.4 | PATCH PANEL MODULAR 48 PUERTOS | 1 | $ 36,36 | $ 36,36 |
| 1.5 | RACK MURAL MUPM 10" Cat. 6 | 1 | $ 170,85 | $ 170,85 |
| 1.6 | MATERIALES MENORES(AMARRAS PLASTICAS, TORNILLOS, ETC) | 1 | $ 80,00 | $ 80,00 |
| 2 | CANALETAS PLASTICAS | | | |
| 2.1 | CANALETA METALICA 16X10 (metros) | 146,7 | $ 0,80 | $ 117,36 |
| 2.2 | CANALETA 2 m (2 CAB. UTP Cat. 6) TIPO PANDUIT (metros) | 108,58 | $ 0,30 | $ 32,57 |
| 2.3 | ACCESORIOS CANALETAS | 100 | $ 0,42 | $ 42,00 |
| 2.4 | MATERIALES MENORES ( ANILLADO PLASTICO, TORNILLOS, tacos tirafondos, ETC) | 1 | $ 100,00 | $ 100,00 |
| | | SUBTOTAL | | $1090,06 |
| | | IVA | | $ 130,80 |
| TOTAL | | | | $ 1.220,86 |

Tabla 2.40 Presupuesto para elaborar la red cableada

| Ítem | Descripción | Cant | V Unit. | V Total |
|---|---|---|---|---|
| D | TRABAJOS DE INSTALACION Y PUESTA EN MARCHA | | | |
| D.1 | INSTALACION CANALETA (metros) | 255,28 | $ 1,00 | $ 255,28 |
| D.2 | INSTALACION Y CONFIGURACION | 1 | $ 300,00 | $ 300,00 |
| D.3 | PUNTO DE CABLEADO ESTRUCTURADO CAT 6 | 50 | $ 10,00 | $ 500,00 |
| D.4 | PLANOS AS BUILT | 4 | $ 80,00 | $ 320,00 |
| D.5 | Certificación Puntos Cat 6 | 50 | $ 6,00 | $ 300,00 |
| D.6 | DIRECCION TECNICA | 1 | $ 400,00 | $ 400,00 |
| | | SUBTOTAL | | $ 2.075,28 |
| | | IVA | | $ 249,03 |
| TOTAL | | | | $ 2.324,31 |

Tabla 2.41 Presupuesto de mano de obra para red cableada

| Ítem | Descripción | V Total |
|---|---|---|
| 1 | Red Inalámbrica | $ 4.860,69 |
| 2 | Red de Sensores | $ 1.489,60 |
| 3 | Red cableada | $ 1.081,43 |
| 4 | Trabajos y puesta en marcha | $ 2.324,31 |
| | SUBTOTAL | $ 9.756,03 |
| | IVA | $ 1.170,72 |
| TOTAL | | $ 10.926,75 |

Tabla 2.42 Presupuesto para elaborar la red híbrida

# CAPÍTULO 3

# DESARROLLO DE LA APLICACIÓN EN JAVA

# 3. DESARROLLO DE LA APLICACIÓN EN JAVA

Actualmente se emplea a la informática como una herramienta de ayuda para eventos o cálculos repetitivos, que conforme se van haciendo más complejos acorde al avance de la ciencia y la tecnología, simplifican las tareas del ser humano.

La aplicación de la informática en la medicina introduce un significativo ahorro de tiempo y errores, siendo un punto clave la automatización en los procesos de obtención, intercambio, manejo y almacenamiento de la información.

Se ha seleccionado esta plataforma de programación, por ser gratuita y proveer los paquetes de comunicación serial requeridos por los sensores seleccionados en el capítulo 2.

## 3.1 CARACTERÍSTICAS FUNDAMENTALES DE JAVA[1]

SUN es el creador del estándar Java2, el cual incluye tres diferentes entornos para desarrollo y ejecución de aplicaciones, estos son J2SE, J2EE y J2ME.

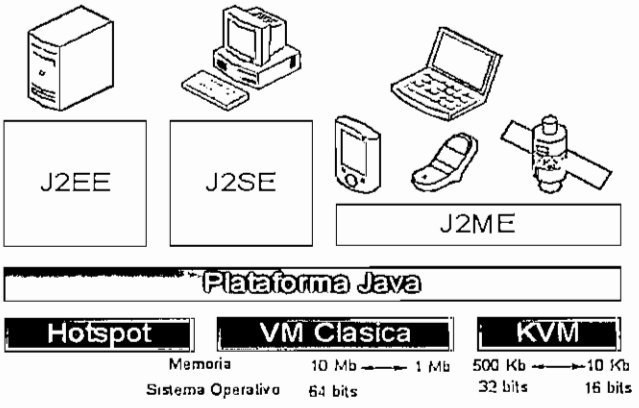



**Figura 3.1 Arquitectura de la plataforma Java 2 de Sun**

J2SE (*Java 2 Standard Edition*) es la base de la tecnología Java, permite el desarrollo de *applets*[2] y aplicaciones independientes (*standalone*).

[1] http://java.sun.com
[2] Aplicaciones que se ejecutan en un navegador Web (mini aplicaciones).

J2EE (*Java 2 Enterprise Edition*) está basado en J2SE, pero añade una serie de características necesarias en entornos empresariales, relativos a redes, acceso a datos y entrada/salida, que requieren mayor capacidad de proceso, almacenamiento y memoria. La decisión de separarlos es debida a que no todas estas características son necesarias para el desarrollo de aplicaciones estándar.

J2EE cubre necesidades más amplias que J2SE, sin embargo, se hace evidente la necesidad de un subconjunto de J2SE para entornos más limitados, la respuesta de SUN es J2ME (*Java 2 Micro Edition*).

### 3.1.1 CARACTERÍSTICAS DEL LENGUAJE JAVA

Java es un lenguaje simple, orientado a objetos, distribuido, interpretado, sólido, seguro, de arquitectura neutral, portable, de alto desempeño, multihilo y dinámico.

- **Simple**: Si bien Java es bastante parecido al lenguaje de programación C++, Java ha eliminado las complejidades innecesarias de C++ en lo que a POO[3] se refiere, facilitando y reduciendo el costo del desarrollo de software. Entre las principales características con las que no se cuenta en Java son: no soporta punteros, no permite sobrecarga de operadores, y no ofrece herencia múltiple. Sin embargo dispone de un sistema automático de asignación y liberación de memoria (recolector de basura), eliminando las instancias de objetos que han dejado de ser utilizadas en un programa, despreocupándose así de la destrucción de los mismos y evitando la sobrecarga de la memoria RAM[4].
- **Orientado a Objetos**: en Java los objetos agrupan en estructuras encapsuladas, tanto sus datos, como los métodos (o funciones) que manipulan esos datos, permitiendo su reutilización.
- **Distribuido**: Java proporciona una colección de clases para su uso en aplicaciones de red, que permiten abrir *sockets*, establecer y aceptar conexiones con servidores o clientes remotos, facilitando así la creación de aplicaciones distribuidas.

[3] Programación Orientada a Objetos.
[4] Memoria de Acceso Aleatorio.

- **Interpretado**: el compilador Java traduce cada fichero fuente de clases a código de bytes (*Bytecode*[5]), que puede ser interpretado por todas las máquinas que den soporte a un visualizador que funcione con Java. El *Bytecode* no es específico de una máquina determinada, por lo que no se compila y enlaza como en el ciclo clásico, sino que se interpreta.
- **Sólido**: en Java no es posible escribir en áreas arbitrarias de memoria ni realizar operaciones que corrompan el código, ya que fue diseñado para crear software altamente fiable, mediante comprobaciones en compilación y en tiempo de ejecución.
- **Seguro**: la máquina virtual de Java, al ejecutar el código java, realiza comprobaciones de seguridad, además el propio lenguaje carece de características inseguras, como por ejemplo los punteros.
- **Arquitectura Neutral**: Java está diseñado para soportar aplicaciones que serán ejecutadas en los más variados entornos de red, desde Unix a Windows NT, pasando por *Mac* y estaciones de trabajo, sobre arquitecturas distintas y con sistemas operativos diversos. Para acomodar requisitos de ejecución tan variados, el compilador de Java genera los *Bytecodes*, diseñados para transportar el código eficientemente a múltiples plataformas de hardware y software.
- **Portable**: la indiferencia a la arquitectura representa sólo una parte de su portabilidad. Además, Java especifica los tamaños de sus tipos de datos básicos y el comportamiento de sus operadores aritméticos, de manera que los programas son iguales en todas las plataformas. Estas dos últimas características se conocen como la *Máquina Virtual Java* (JVM).
- **Alto Rendimiento**: al ser código interpretado, la ejecución no es tan rápida como el código compilado para una plataforma particular, por lo que, cuando se necesitan capacidades de proceso intensivas, pueden usarse llamadas a código nativo y así proporcionar un grado de eficiencia aceptable.
- **Multihilos**: existen aplicaciones que sólo pueden ejecutar una acción a la vez, en cambio Java soporta sincronización de múltiples hilos de ejecución (*multithreading*) a nivel de lenguaje, que son especialmente útiles en la

[5] Formato intermedio indiferente a la arquitectura.

creación de aplicaciones de red distribuidas. Así, mientras un hilo se encarga de la comunicación, otro puede interactuar con el usuario, mientras otro presenta una animación en pantalla y otro realiza cálculos.

- **Dinámico**: el lenguaje Java y su sistema de ejecución en tiempo real son dinámicos en la fase de enlazado. Las clases sólo se enlazan a medida que son necesitadas. Se pueden enlazar nuevos módulos de código bajo demanda, procedente de fuentes muy variadas, incluso desde la Red.

## 3.2 DESCRIPCIÓN DE PAQUETES Y COMANDOS DE JAVA PARA LA COMUNICACIÓN CON SENSORES BLUETOOTH

### 3.2.1 J2ME

J2ME está enfocada a la aplicación de la tecnología Java en dispositivos electrónicos con capacidades computacionales y gráficas muy reducidas, tales como teléfonos móviles, PDAs o equipos inteligentes.

J2ME se basa en los conceptos de configuración y perfil. Una configuración describe las características mínimas en cuanto a la configuración hardware y software.

Existen 2 configuraciones definidas en J2ME: *Connected Limited Device Configuration* (CLDC) enfocada a dispositivos con restricciones de procesamiento y memoria, y *Connected Device Configuration* (CDC) enfocada a dispositivos con mayores recursos en cuanto a procesamiento.

La configuración que usa J2ME frecuentemente es la CLDC, la cual define:

- Características del lenguaje Java incluidas.
- Funcionalidad a ser incluida en la máquina virtual Java.
- Los requerimientos de hardware de los dispositivos.
- Las APIs[6] necesarias para el desarrollo de aplicaciones en móviles.

[6] *Application Programming Interfaces*

Un perfil define las características del dispositivo de forma más específica. Hay varios perfiles, pero los más importantes en referencia a J2ME son de: acceso genérico, identificación de servicio, puerto serial, acceso a LAN, sincronización y dispositivo de información móvil (MIDP).

### 3.2.2 APIs JAVA PARA BLUETOOTH

El desarrollo de aplicaciones que permiten el acceso y control sobre dispositivos que soporten Bluetooth en J2ME, se lo realiza bajo la especificación de Java JSR[7]-82, el cual esconde la complejidad del protocolo Bluetooth detrás de varios APIs que permiten centrarse en el desarrollo, en vez de los detalles de bajo nivel de Bluetooth.

Estos APIs para Bluetooth están orientados para dispositivos que cumplan las siguientes características:

- Al menos 512 KBytes de memoria libre (ROM y RAM). Las aplicaciones necesitan memoria adicional para almacenarse.
- Conectividad a la red inalámbrica Bluetooth.
- Que tengan una implementación del J2ME CLDC.

#### 3.2.2.1 JSR 82

Define un API estándar no propietario, que puede ser usado en todos los dispositivos que implementen J2ME, por consiguiente utiliza los APIs J2ME y el entorno de trabajo CLDC/MIDP.

El API ofrece las siguientes capacidades:

- Registro de servicios.
- Descubrimiento de dispositivos y servicios.
- Establecimiento de conexiones RFCOMM[8], L2CAP[9] y OBEX[10] entre dispositivos.

---

[7] *Java Specification Revision*
[8] *Radio Frecuency Communication*
[9] *Logical Link Control and Adaptation Protocol*

- Envío y recepción de datos (no soporta comunicaciones de voz).
- Manejo y control de conexiones.
- Seguridad a dichas actividades.

Las aplicaciones de Java para Bluetooth utilizan tres paquetes esenciales:

- *javax.bluetooth*, que conforma las especificaciones básicas del estándar Bluetooth.
- *javax.obex*, realiza el intercambio de objetos (transferencia de datos) entre dispositivos.
- *javax.comm*, para OEMs[11] Bluetooth que se comunican emulando un puerto serial.

Para la programación de un API, se deben contemplar cinco funciones principales, basadas en la operación del protocolo Bluetooth:

1. Inicializar los parámetros de comunicación: velocidad de transmisión, puerto de comunicación y establecimiento del modo de descubrimiento de dispositivos.
2. Establecer la definición de los dispositivos para etiquetarlos como locales o remotos.
3. Llevar a cabo el descubrimiento de los dispositivos en la red.
4. Realizar el registro y descubrimiento de los servicios disponibles en la red.
5. Envío y recepción de datos.

Los dispositivos Bluetooth que implementen este API permiten que múltiples aplicaciones se estén ejecutando concurrentemente.

El Centro de Control Bluetooth (BCC *Bluetooth Control Center*) es un conjunto de capacidades, que permiten al usuario o al OEM resolver peticiones conflictivas de aplicaciones, definiendo valores específicos para ciertos parámetros de la pila Bluetooth.

---

[10] Protocolo para transferencia de archivos simples entre dispositivos móviles
[11] *Original Equipment Manufacturer*

### 3.2.3 Paquete javax.bluetooth

En una comunicación Bluetooth existe un dispositivo que ofrece un servicio (servidor) y varios dispositivos que acceden a él (clientes).

Un cliente Bluetooth debe realizar las siguientes acciones:

- Búsqueda de dispositivos Bluetooth al alcance de la aplicación que estén en escucha para iniciar una conexión.
- Búsqueda de servicios por cada dispositivo.
- Una vez encontrado un dispositivo que ofrece el servicio deseado, se establece la conexión con el mismo.
- Ya establecida la conexión se inicia la comunicación.

Por otro lado, un servidor Bluetooth debe realizar las siguientes operaciones:

- Crear una conexión servidora.
- Especificar los atributos del servicio.
- Abrir las conexiones clientes.

#### 3.2.3.1 Clases Básicas

Dado que los dispositivos inalámbricos son móviles, necesitan un mecanismo que permita encontrar, conectar, y obtener información sobre las características de los mismos, el API de Bluetooth permite realizar todas estas tareas, mediante las siguientes clases:

**a.** Clase *LocalDevice*: un objeto *LocalDevice* representa al dispositivo local. Este objeto es el punto de partida de cualquier operación que se vaya a llevar a cabo en este API. La información del dispositivo que se puede obtener a través de este objeto es la siguiente: dirección Bluetooth, alias o "*friendly-name*", y modo de conectividad[12]. Adicionalmente obtiene la única instancia existente de esta clase, llamando al método *getLocalDevice()*.

[12] Forma en que el dispositivo esta o no visible para otros dispositivos.

**b.** Clase *DeviceClass*: el método *getDeviceClass()* devuelve un objeto de tipo *DeviceClass*. Este tipo de objeto describe el tipo de dispositivo, a través del cual se conoce si se trata de un teléfono, un ordenador, un elemento de medición, etc.

**c.** Clase *UUID* (*Universally Unique Identifier*): representa identificadores únicos universales, que no son mas que enteros de 128 bits identificando protocolos y servicios. Se puede crear un objeto UUID a partir de un *String* o de un entero largo, representado en hexadecimal.

#### 3.2.3.2 Búsqueda de Dispositivos y Servicios

La búsqueda de dispositivos y servicios son tareas que solamente realizan los dispositivos clientes, dichas tareas se realizan mediante las siguientes clases:

**a.** Clase *DiscoveryAgent*: la búsqueda de dispositivos y servicios Bluetooth se la realiza mediante un objeto *DiscoveryAgent*. Este objeto es único y se lo obtiene a través del método *getDiscoveryAgent()* del objeto *LocalDevice*:

```
DiscoveryAgent búsqueda = LocalDevice.getLocalDevice().getDiscoveryAgent();
```

Para descubrir dispositivos, se tiene el método *startInquiry()* para poner al dispositivo en modo de búsqueda (*inquiry*), y el método *retrieveDevices*[13] para obtener la información de dispositivos previamente encontrados. Además provee del método *cancelInquiry()* para cancelar una operación. Para realizar una o varias búsquedas de dispositivos se emplea *searchServices()*, el cual devuelve un entero que identifica cada una de ellas, su formato es:

```
public int searchServices
(int[] attrSet, UUID[] uuidSet, RemoteDevice btDev, DiscoveryListener discListener)
```

**b.** Interfaz *DiscoveryListener*: este interfaz permite a una aplicación especificar un evento en el *listener* que reaccione ante eventos de búsqueda de dispositivos. Cuando un nuevo servicio es descubierto, se llama al método *servicesDiscovered()*, y cuando la transacción ha sido

[13] Array de dispositivos *PREKNOWN* o *CACHED* (Dispositivos descubiertos en búsquedas anteriores).

completada o cancelada se llama a *serviceSearchCompleted()*. Este último método recibe como argumentos: *INQUIRY_COMPLETED*, *INQUIRY_ERROR* o *INQUIRY_TERMINATED*, dependiendo de cada caso.

c. Clase *DataElement*: ésta clase se encarga de encapsular los tipos de datos disponibles para describir un atributo de servicio Bluetooth. Esta clase además presenta un interfaz que permite construir y recuperar valores de un atributo de servicio.
d. Interfaz *ServiceRecord*: describe un servicio Bluetooth a los clientes. Contiene el pares (atributo ID[14], valor). El atributo ID es un entero sin signo de 16 bits, y valor es de tipo *DataElement*. Además, este interfaz tiene un método *populateRecord()* que permite recuperar los atributos de servicio deseados (pasando como parámetro al método, el ID del atributo deseado).

#### 3.2.3.3 Registro del Servicio

Un servidor Bluetooth tiene las siguientes funciones:

1. Crear un *Service Record* que describa el servicio ofrecido por el servidor.
2. Añadir el *Service Record* al SDDB[15] del servidor, para avisar a los clientes potenciales de este servicio.
3. Registrar las medidas de seguridad Bluetooth asociadas a un servicio.
4. Aceptar conexiones de clientes que requieran el servicio ofrecido.
5. Actualizar el *Service Record* en el SDDB del servidor si un servicio cambia.
6. Quitar o deshabilitar el *Service Record* en el SDDB del servidor cuando el servicio no está disponible.

#### 3.2.3.4 Modos Conectable y No Conectable

En el modo conectable, un dispositivo escucha periódicamente intentos de iniciar una conexión de un dispositivo remoto, mientras que en el modo no-conectable, no lo hace.

---

[14] Identificador de Atributo
[15] *Service Discovery Data Base*

Para el correcto funcionamiento de una aplicación servidora, es necesario que el dispositivo servidor esté en modo conectable. En la implementación de *acceptAndOpen()*, ésta debe asegurarse que el dispositivo local esté en modo conectable.

Aunque un dispositivo esté en el modo no-conectable, puede iniciar un intento de conexión. Por esto, un dispositivo en modo no-conectable puede ser un cliente, pero no un servidor.

Por lo tanto la implementación no necesita pedir al dispositivo que se ponga en modo conectable si no tiene ningún *ServiceRecord* en su SDDB.

#### 3.2.3.5 Comunicación

Para usar un servicio en un dispositivo Bluetooth remoto, el dispositivo local debe comunicarse usando el mismo protocolo que el servicio remoto.

El API *javax.bluetooth* permite usar dos mecanismos de conexión: SPP (Perfil del Puerto Serie ) y L2CAP (Protocolo de Adaptación y Control Lógico del Enlace ). Mediante SPP se obtiene un *InputStream* y un *OutputStream*, mientras que con L2CAP se envían y reciben *arrays* de bytes.

Para abrir cualquier tipo de conexión se emplea la clase *javax.microedition.io.Connector*. En concreto se debe usar el método estático *open()*, el cual en su versión más sencilla requiere un parámetro *String* que contendrá el Localizador Uniforme de Recurso (URL *Uniform Resouce Locator*), con los datos necesarios para realizar la conexión.

La URL será diferente dependiendo si se desea ser cliente o servidor de una conexión L2CAP o SPP.

#### 3.2.3.6 Comunicación Cliente

A través del método *getConnectionURL()*de un objeto *ServiceRecord* se obtiene la URL necesaria para realizar la conexión. Este método requiere dos

argumentos, el primero indica si se debe autenticar y/o cifrar la conexión. Los posibles valores de este primer argumento son:

- *ServiceRecord.NOAUTHENTICATE_NOENCRYPT*: no autenticación, no cifrado.
- *ServiceRecord.AUTHENTICATE_NOENCRYPT*: autenticación, no cifrado
- ServiceRecord.AUTHENTICATE_ENCRYPT: autenticación y cifrado.

El segundo argumento, es un *booleano* que especifica si el dispositivo será maestro (*true*) o bien no importa si es maestro o esclavo (*false*).

#### *3.2.3.6.1 Comunicación Cliente SPP*

Para realizar la conexión, se utiliza el método *Connector.open()*, el cual devuelve un objeto distinto según el tipo de protocolo usado, que en el caso de un cliente SPP devolverá un *StreamConnection*.

A partir del *StreamConnection* se pueden obtener los flujos de entrada y de salida:

```
StreamConnection con = (StreamConnection) Connector.open(url);
OutputStream out = con.openOutputStream();
InputStream in = con.openInputStream();
```

#### *3.2.3.6.2 Comunicación Cliente L2CAP:*

En una conexión L2CAP al llamar al método *Connector.open(),*este devuelve un objeto *L2CAPConnection*, con el cual se pueden leer bytes a través de *receive()* o enviarlos mediante *send()*. Ambos requieren como parámetro un *array* de bytes.

En una conexión L2CAP el tamaño de los *arrays* de bytes leídos y los recibidos están limitados a un tamaño máximo. Los tamaños límite se establecen mediante parámetros en la URL.

Para saber el tamaño máximo de los arrays recibidos se emplea *getRecieveMTU()* y para saber el tamaño máximo de los *arrays* que se envían se utiliza *getTransmitMTU()*.

#### 3.2.3.7 Comunicación Servidor

Para ofrecer un servicio a través de Bluetooth, es necesario poner al dispositivo en modo visible, a través de la clase *LocalDevice*.

Para crear una conexión servidora se requiere pasarle una URL al método *Connector.open()*, del mismo modo que para realizar conexiones clientes. La diferencia está en que se debe crear la conexión e indicar que se desea ser servidor, mostrando a "*localhost*" como *host* en la URL. De este modo la URL deberá comenzar por "*btspp://localhost:*" o por "*btl2cap://localhost:*".

Además del *host* de la URL, se debe indicar el UUID que identifica el servicio y posteriormente el nombre del servicio.

Al pasar una URL de este tipo al método *Connector.open()*, éste devuelve un "*notifier*", que en el caso de SPP será un objeto *StreamConnectionNotifier* y en el caso de L2CAP será un objeto *L2CAPConnectionNotifier*. Estos objetos permiten escuchar las conexiones entrantes de los clientes.

Una vez creado el "*notifier*", se deben especificar los atributos del servicio que presta el dispositivo servidor, los cuales están almacenados en un *ServiceRecord*.

Una vez obtenido el ServiceRecord se establecen los atributos mediante el método *setAttributeValue()* al que se le pasa un identificador numérico y un objeto *DataElement* que representará el valor del atributo de servicio. En este punto ya se pueden escuchar las conexiones clientes a través de *acceptAndOpen()*, del siguiente modo:

```
StreamConnection conn = notifier.acceptAndOpen();
L2CAPConnection conn = notifier.acceptAndOpen();
```

Una vez que se tiene el objeto *StreamConnection* o *L2CAPConnection*, el servidor ya puede comunicarse con los clientes.

### 3.2.4 Paquete javax.obex

Éste es totalmente independiente del paquete *javax.bluetooth*, es decir, en una aplicación OBEX no se utiliza ninguna de las clases de *javax.bluetooth*.

OBEX es un protocolo que se usa generalmente para la transferencia de archivos, muy similar a HTTP. Trabaja intercambiando mensajes entre cliente-servidor, que consisten en un conjunto de cabeceras y opcionalmente un cuerpo de mensajes.

En este protocolo el cliente envía comandos al servidor (*CONNECT, PUT, GET, DELETE, SETPATH, DISCONNECT*) junto con algunas cabeceras de mensaje, y en ocasiones un cuerpo de mensaje (únicamente para el comando PUT). Las cabeceras de mensaje están encapsuladas en un objeto *HeaderSet* y el cuerpo de mensaje se lee/escribe mediante un *Input/OutputStream* respectivamente.

El servidor por su parte recibirá los comandos del cliente y responderá con un código de respuesta indicando el éxito o no de la petición, y además enviará una serie de cabeceras de mensaje con información adicional y un cuerpo de mensaje en caso de tratarse de una respuesta al comando GET.

El comando *CONNECT* es necesario para completar el inicio de la sesión. El comando *PUT* envía datos del cliente al servidor y el comando *GET* a la inversa.

El comando *DELETE* sirve para eliminar un recurso del servidor, el comando *SETPATH* sirve para crear directorios y navegar por ellos, y finalmente el comando *DISCONNECT* sirve para cerrar la conexión.

#### 3.2.4.1 Clases Básicas

**a.** Clase *HeaderSet*: representa las cabeceras de un mensaje, enviado tanto por un cliente, como por un servidor. Las cabeceras de mensaje se guardan como pares (clave, valor), en los que la clave es un número entero; es decir, las cabeceras de mensaje se identifican numéricamente.

   Los identificadores numéricos son utilizados en los métodos *setHeader()* y *getHeader()* para establecer y obtener respectivamente una cabecera de mensaje. Mediante el método *getHeaderList()* se obtiene un array con todos los identificadores de las cabeceras que guarda un objeto *HeaderSet*.

Los mensajes enviados por el servidor tienen adicionalmente un código de respuesta que indica si tuvo éxito la petición o en caso de no tenerlo cuál fue el motivo, este código es almacenado en el objeto *HeaderSet*. El código de respuesta es un número entero que se obtiene a través del método *getResponseCode()*, los posibles valores que puede tomar están reflejados como variables estáticas de la clase *ResponseCodes*.

**b.** Clase *Operation*: un objeto de la esta clase, encapsula las cabeceras y el cuerpo del mensaje. Las cabeceras de mensaje se guardan en un objeto *HeaderSet* que se obtiene mediante *getReceivedHeaders()*. Para enviar datos se emplea un objeto *OutputStream*, el cual se lo obtiene mediante *openOutputStream()*. En el caso de que se desee recibir datos, se emplea un *InputStream*, obtenido con *openInputStream()*.

#### 3.2.4.2 Conexión Cliente

Una conexión cliente OBEX viene encapsulada en forma de un objeto *ClientSession*.

Para obtener un objeto *ClientSession* se utiliza el método *Connector.open()*, al cual se le pasa una URL del tipo "obex:// discover.0210;ias=NombreServicio". Una vez obtenido el objeto *ClientSession* se llama al método *connect()*.

Ahora ya se pueden efectuar las operaciones *DELETE, PUT, GET, y SETPATH* a través de los métodos *delete()*, *put()*, *get()* y *setPath()* respectivamente, los mismos que requieren un parámetro de tipo *HeaderSet*.

Los métodos *get()* y *put()* devuelven un objeto de tipo *Operation*, el cual encapsula un mensaje completo: código de respuesta, cabeceras de mensaje y cuerpo del mensaje.

Cuando se ejecuta una llamada al método *get()* se debe leer el cuerpo del mensaje usando *openInputStream()*; mientras que cuando se ejecute una llamada al método *put()*, se debe escribir en el cuerpo del mensaje usando *openOutpuStream()*.

El método *setPath()* requiere adicionalmente dos argumentos de tipo booleano. El primer argumento si es *true* indica que se quiere navegar al directorio padre del directorio indicado por la cabecera *HeaderSet.NAME* (cd..). El segundo argumento indica si se debe crear o no el directorio en caso de que no exista. Para finalizar la conexión se llama al método *disconnect()* que también requiere un argumento de tipo *HeaderSet*.

#### 3.2.4.3 Conexión Servidor

Una conexión servidora viene encapsulada en un objeto *SessionNotifier*, para obtenerlo se utiliza el método *Connection.open()* pasándole una URL del tipo "irdaobex://localhost.0010;ias=NombreServicio".

A través del objeto *SessionNotifier* (objeto *listener*), se escuchan las conexiones cliente mediante *acceptAndOpen()*, el cual requiere que se le pase un parámetro de tipo *ServerRequestHandler*.

Cada vez que un cliente envíe un comando *CONNECT, GET, PUT, DELETE o DISCONECT* se llamará a los métodos *onConnect()*, *onGet()*, *onPut()*, *onDelete()* u *onDisconnect()* respectivamente. A excepción de los métodos *onGet()* y *onPut()* el resto tienen dos argumentos de tipo *HeaderSet*. El primero representa las cabeceras que envió el cliente y el segundo las cabeceras a ser enviadas al cliente.

Los métodos *onGet()* y *onPut()* requieren un cuerpo de mensaje, razón por la cual se les pasa un único argumento de tipo *Operation*.

Todos estos métodos a excepción de *onDisconnect()* devuelven un código de respuesta representado por un valor entero.

### 3.2.5 Paquete javax.comm

El API COMM es una extensión de Java que permite el acceso mediante software al puerto serial, puerto paralelo, y al modo SPP.

Las principales características de este paquete son:

- Listado de puertos.
- Configuración del puerto (velocidad, bits de parada, bits de paridad, y bits de datos).
- Acceso al estándar EIA/TIA-232 mediante las señales DTR, CD, CTS, RTS y DSR.
- Transferencia de Datos sobre puertos RS-232.
- Opciones de control de flujo si el dispositivo lo soporta.

Los pasos a seguir para elaborar una aplicación que maneje el puerto de un dispositivo son:

1. Proporcionar al API de Comunicaciones Java, control sobre alguno de los dispositivos (antes de usar un dispositivo, el API debe conocerlo).
2. Abrir el dispositivo y acondicionar la línea a los parámetros de trabajo que se requiera.
3. Escribir o leer algunos datos siguiendo el protocolo especificado para el dispositivo.
4. Cerrar el puerto.

#### 3.2.5.1 Inicialización del API con Puertos Serie

Los puertos a emplear no deben ser necesariamente inicializados, ya que al arrancar el API, realiza una búsqueda de los puertos disponibles en la máquina en que se ejecuta y los va incorporando automáticamente.

Sin embargo, se recomienda inicializar los puertos serie que se vayan a utilizar en la aplicación, ya que existen puertos que no emplean la nomenclatura convencional, por lo cual es necesario agregar código para configurarlos y así garantizar su funcionamiento adecuado.

Para inicializar un puerto no convencional, se emplea la clase *CommPort*, como se muestra en el siguiente ejemplo:

```
// Registro del dispositivo OEM
CommPort OEM = new javax.comm.solaris.SolarisSerial( "OEM","/dev/OEM" );
CommPortIdentifier.addPort( OEM,CommPortIdentifier.PORT_SERIAL );
```

### 3.2.5.2 Apertura y Configuración de Dispositivos

Luego de registrar e inicializar los puertos deseados, se procede a añadirlos, fijar sus características de configuración y finalmente abrirlos.

Para añadir un dispositivo serial, se emplea la clase *SerialPort*, tomando en cuenta que esta instancia debe ser inicializada con un valor *null*, para evitar posibles errores de configuración y transmisión.

El segundo paso a seguir, es asignar un identificador para el dispositivo serie añadido, mediante el método *getPortIdentifier* de la clase *CommPortIdentifier.*

```
CommPortIdentifier idPuerto = CommPortIdentifier.getPortIdentifier(dispositivo);
```

Una vez obtenido el identificador del dispositivo serial con el que se va a trabajar, se procede a abrirlo mediante el método *openPort* de la clase *SerialPort*, pasando como argumentos, el puerto serie a emplear y el tiempo máximo de espera para abrirlo.

```
puertoSerie = (SerialPort)idPuerto.openPort( "PuertoSerie",timeout );
```

La configuración del dispositivo serial con el que se desea trabajar, se lo hace mediante el método *SerialPortParams* de la clase *SerialPort,* enviando como argumentos:

```
puertoSerie.setSerialPortParams( 9600,SerialPort.DATABITS_8,
        SerialPort.STOPBITS_1,SerialPort.PARITY_NONE );
```

- Velocidad del dispositivo en baudios.
- Número de bits por carácter.
- Bits de parada.
- Bits de paridad.

Adicionalmente se pueden configurar parámetros para realizar control de flujo (*SetFlowControl*), para el modo de recepción de los datos (*enableRcv*), y para el tiempo de espera antes de cerrar un puerto por inactividad (*enableRcvTimeout*), como se muestra a continuación:

```
puertoSerie.setFlowcontrolMode( SerialPort.FLOWCTRL_NONE );
puertoSerie.enableRcv..;
puertoSerie.enableRcvTimeout( timeout );
```

Finalmente se deben definir dos canales o *streams* para manejar los datos de lectura y escritura en el dispositivo conectado a este puerto, mediante los métodos *getInputStream* y *getOutputStream* de la clase *SerialPort* respectivamente.

```
InputStream entrada = null;
OutputStream salida;
salida = puertoSerie.getOutputStream();
entrada = puertoSerie.getInputStream();
```

### 3.2.5.3 Escritura y Lectura de Datos

En el caso del API de Comunicaciones Java, la lectura y escritura no se diferencia en nada de cualquier llamada a métodos para realizar dichas tareas; esto en cuanto a la utilización de objetos derivados de *streams*.

Para escribir, se puede realizar:

```
try {
  salida.write( arraySalida,0,longitud );
```

Y para la lectura de datos, es suficiente con:

```
try {
  int b = entrada.read()
```

### 3.2.5.4 Cierre de Puertos

El cierre de un puerto es un paso sumamente importante porque el API de Comunicaciones Java siempre intenta proporcionar acceso exclusivo a los dispositivos, y si algún canal no se cierra, no estará disponible para otras aplicaciones.

Si se desea utilizar un dispositivo para múltiples usuarios sobre un mismo puerto serie, es necesario emplear un protocolo que permita multiplexar la información proveniente de cada uno de ellos.

```
try {
  entrada.close();
  salida.close();
  } ...
```

## 3.3 DISEÑO DEL INTERFAZ GRÁFICO

En este capítulo se presenta el proceso de desarrollo empleado para elaborar la aplicación, y en base a este se describen los parámetros a utilizar en el interfaz gráfico.

Para la realización de este diseño se ha considerado el óptimo, el Proceso Unificado de Desarrollo de Software (PUDS), ya que provee una metodología apropiada para elaborar aplicaciones orientadas a objetos, y satisface los requerimientos de atención médica de la clínica, como se detalla más adelante.

### 3.3.1 PROCESO UNIFICADO DE DESARROLLO DE SOFTWARE[16]

Es una metodología que posee un conjunto de actividades necesarias para transformar los requisitos de un conjunto de usuarios en un sistema. Proporciona un marco de trabajo genérico que puede aplicarse para una gran variedad de sistemas, diferentes áreas de aplicación, diferentes tipos de organizaciones, diferentes niveles de aptitud y diferentes tamaños de proyectos.

Está basado en componentes, que se interconectan a través de interfaces adecuadamente definidas. Utiliza el Lenguaje Unificado de Modelado (UML *Unified Modeling Language*), para definir los esquemas del modelo. Este proceso se resume en tres características: dirigido por casos de uso, centrado en la arquitectura y con un ciclo de vida iterativo e incremental, sin una de las cuales se reduciría drásticamente el valor de este proceso.


**Figura 3.2 Proceso de Desarrollo de Software[17]**

[16] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, 2000.

### 3.3.1.1 Dirigido por Casos de Uso

Un caso de uso es un fragmento de funcionalidad del sistema, que proporciona al usuario[18] un resultado deseado. Los casos de uso representan los requisitos prácticos y en conjunto con los actores, constituyen el modelo de casos de uso que describe la funcionalidad completa del sistema.

Los casos de uso guían el proceso de desarrollo en las etapas de diseño, implementación y prueba. Son desarrollados al mismo tiempo que la arquitectura del sistema, de tal modo que ésta influye en la selección de los casos de uso.

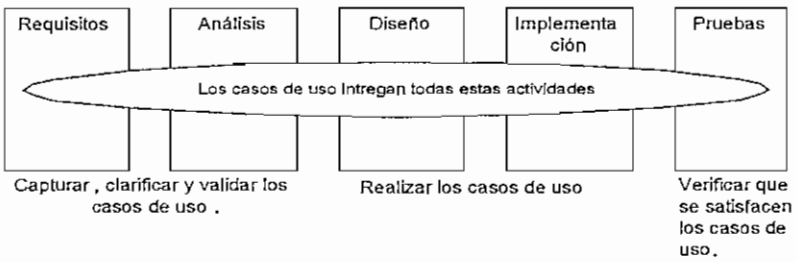



**Figura 3.3 Casos de Uso**[19]

### 3.3.1.2 Centrado en la Arquitectura

La arquitectura de software, incluye los aspectos estáticos y dinámicos de mayor relevancia en un sistema, y surge de las necesidades de la empresa y la percepción de los usuarios.

Los factores determinantes que influyen en la selección de la arquitectura son: plataforma de ejecución, bloques de construcción reutilizables, consideraciones de implantación, sistemas heredados y requisitos no funcionales (Ej. rendimiento y fiabilidad).

Cada software es creado para cumplir un fin y tiene su propia arquitectura; que debe ser diseñada para permitir cambios futuros, acorde a las necesidades de los

---

[17, 19] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, Pag 4, 37.

[18] Ser humano, máquinas o sistemas.

usuarios. Dicha arquitectura debe trabajar en base al conocimiento de los casos de uso claves del sistema, es decir evolucionan en paralelo.

Cada caso de uso seleccionado, se especifica en detalle y se lo realiza en términos de subsistemas, clases y componentes, como se describe más adelante.

#### 3.3.1.3 Iterativo e Incremental

Al elaborar un sistema, es conveniente dividirlo en pequeños proyectos, considerados como iteraciones, las cuales deben seleccionarse y ejecutarse en forma planificada para obtener los resultados esperados que da como resultado un incremento.

Las iteraciones hacen referencia a pasos en el flujo de trabajo, y los incrementos, al crecimiento del software. Para seleccionar una iteración, se lo hace en base al tratamiento de un grupo de casos de uso, de tal modo que se amplía la utilidad del sistema y se pueden apreciar acertadamente los riesgos de mayor relevancia.

En cada iteración, los desarrolladores deben identificar y especificar los casos de uso más importantes, para así, crear un diseño apropiado basándose en la arquitectura guía seleccionada, luego se debe implementar mediante componentes y verificar que dichos componentes satisfacen los casos de uso planteados.

Los beneficios que conlleva una iteración controlada son:

- Reduce el costo del riesgo al costo de un solo incremento.
- Identificación de riesgos en fases tempranas de desarrollo del software.
- Trabajo eficiente para la obtención de resultados claros a corto plazo.
- Permite reconocer que las necesidades y requisitos de los usuarios no pueden definirse totalmente al inicio.

La Figura 3.4 muestra el ciclo de vida iterativa e incremental que aplica el Proceso de Desarrollo Unificado (PUD).

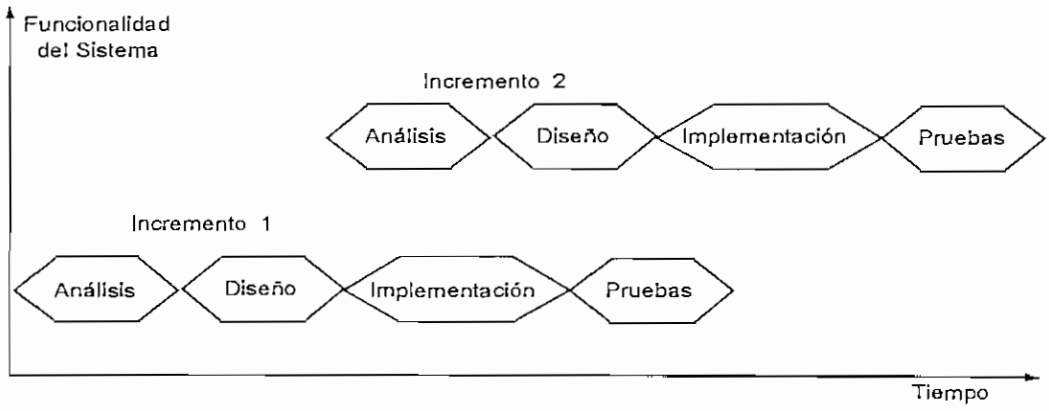



Figura 3.4 Proceso Iterativo e Incremental[20]

### 3.3.1.4 Personas, Proyecto, Producto y Proceso

Las personas son los arquitectos, desarrolladores, ingenieros de prueba, personal de gestión, usuarios y clientes, que tienen un conjunto de responsabilidades y llevan a cabo un conjunto de actividades. Una persona puede pasar de ser un recurso latente a un trabajador, si dispone de las habilidades y recursos necesarios para ello.

Un proyecto es un elemento organizativo a través del cual se gestiona el desarrollo del software. El resultado de un proyecto es una versión de un producto.

El producto es un conjunto de artefactos de ingeniería y de gestión que se crean durante la vida del proyecto.

Un proceso es un conjunto de actividades para crear un producto. Se define en términos de flujo de trabajo mediante diagramas UML y permite identificar trabajadores y artefactos.

### 3.3.1.5 Fases del Proceso Unificado de Desarrollo

Una fase es un intervalo de tiempo entre dos hitos[21] dentro del PUD. Cada fase termina con un hito, y puede descomponerse en iteraciones. Los hitos permiten

[20] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, Pag .97.
[21] Hito: punto limite entre fases o iteraciones.

obtener un conjunto de datos a partir del seguimiento de tiempo y esfuerzo consumido en cada fase, para realizar la estimación de tiempo y recursos humanos para futuros proyectos. Las fases del Proceso de Desarrollo Unificado se describen en la siguiente tabla:

| Fase | Descripción | Hitos |
|---|---|---|
| Inicio | Permite desarrollar el análisis del proyecto hasta justificar su puesta en marcha, para lo cual es necesario: delimitar el alcance y objetivos del proyecto, definir la funcionalidad y capacidades del proyecto, determinar una posible arquitectura a emplear, reducir riesgos, estimación inicial de costos y definir una agenda de trabajo. | Establecer el ámbito del producto, la identificación de los principales riesgos y la viabilidad del proyecto. |
| Elaboración | En esta fase se analiza el dominio del problema, se define la arquitectura básica, se planifica el proyecto acorde a los recursos disponibles, y se eliminan los elementos de mayor riesgo del proyecto. | Obtener una línea base de la arquitectura del sistema, capturar la mayoría de los requisitos y reducir los riesgos principales. |
| Construcción | Se asigna personal y se fijan criterios de evaluación, de tal modo que se obtiene la versión beta del software, una lista de casos de uso implementados y la documentación inicial para el usuario. Durante esta fase, se desarrolla y prueba la aplicación a través de iteraciones, tomando en cuenta que cada una de estas involucra análisis, diseño e implementación, requiriendo documentar tanto la aplicación elaborada como su manejo. | Desarrollo del sistema con calidad de producción y prepararse para la entrega al equipo de transición. Si el proyecto no logra alcanzar este hito, entonces la transición deberá posponerse una iteración. |
| Transición | Comprende el período de entrega del software completo a los usuarios, incluyendo tareas de instalación, configuración, entrenamiento, soporte y mantenimiento. | Decidir si los objetivos se cumplieron y si debe comenzarse otro ciclo de desarrollo. Resulta de la revisión y aceptación por parte del cliente de los artefactos entregados. |

Tabla 3.1 Fases del PUD

### 3.3.1.6 Flujos de Trabajo del Proceso Unificado

También denominados disciplinas, permiten organizar las actividades de gestión y desarrollo de un proyecto. Existen dos tipos de disciplinas: desarrollo y gestión.

Las disciplinas de desarrollo incluyen: requisitos, análisis, diseño, implementación y pruebas, mientras que las de gestión contemplan la gestión del proyecto y gestión del entorno, las cuales se resumen a continuación:

| DISCIPLINA | OBJETIVOS |
|---|---|
| Análisis de Requisitos | Establecer un acuerdo con los clientes en lo que el sistema debe hacer y proporcionar a los desarrolladores del sistema los requisitos y límites del mismo. Servir de base para planificar los contenidos técnicos de las iteraciones posteriores y para estimar el costo y tiempo necesario para desarrollar el sistema. |
| Análisis y Diseño | Transformar los requisitos planteados en un diseño (sistema a construir). Desarrollar una arquitectura robusta del sistema y adaptar el diseño para que corresponda con el ambiente de implementación, tomando en cuenta el rendimiento. |
| Implementación | Definir la organización del código en términos de subsistemas y capas. Convertir los elementos del diseño en elementos de implementación (fichero fuentes, binarios, ejecutables, y otros). Realizar pruebas de unidad a los componentes desarrollados. Integrar los resultados producidos por programadores individuales en un solo sistema ejecutable. |
| Pruebas | Encontrar y documentar defectos en la calidad del software. Validar las suposiciones hechas en el diseño y especificaciones de requisitos mediante demostraciones concretas. Validar que el producto de software funciona como se diseñó y que los requisitos fueron implementados apropiadamente. |
| Gestión del Proyecto | La gestión de proyectos de software es el arte de balancear objetivos en competencia, gestionar los riesgos, y sobreponerse a las restricciones para crear con éxito un producto que satisfaga las necesidades tanto de los clientes como de los usuarios finales. |
| Gestión del Entorno | Describe las actividades necesarias para desarrollar las directrices que regirán el desarrollo del proyecto, proporcionando a la organización el entorno de desarrollo de software apropiado, que contendrá las herramientas de desarrollo y del proceso, plantillas, documentos, convenciones a seguir, y cualquier otro elemento necesario para llevar adelante con éxito el desarrollo del proyecto. |

**Tabla 3.2 Disciplinas de PUD**

### 3.3.1.7 Artefactos del Proceso Unificado

Un artefacto se define como cualquier tipo de información producida por los desarrolladores de un sistema que se construye de forma incremental. Un

artefacto puede ser un documento, modelo o elemento de un modelo. Los modelos empleados para este proceso son los siguientes:

- Modelo de Casos de Uso
- Modelo de Análisis
- Modelo de Diseño
- Modelo de Despliegue
- Modelo de Implementación
- Modelo de Pruebas

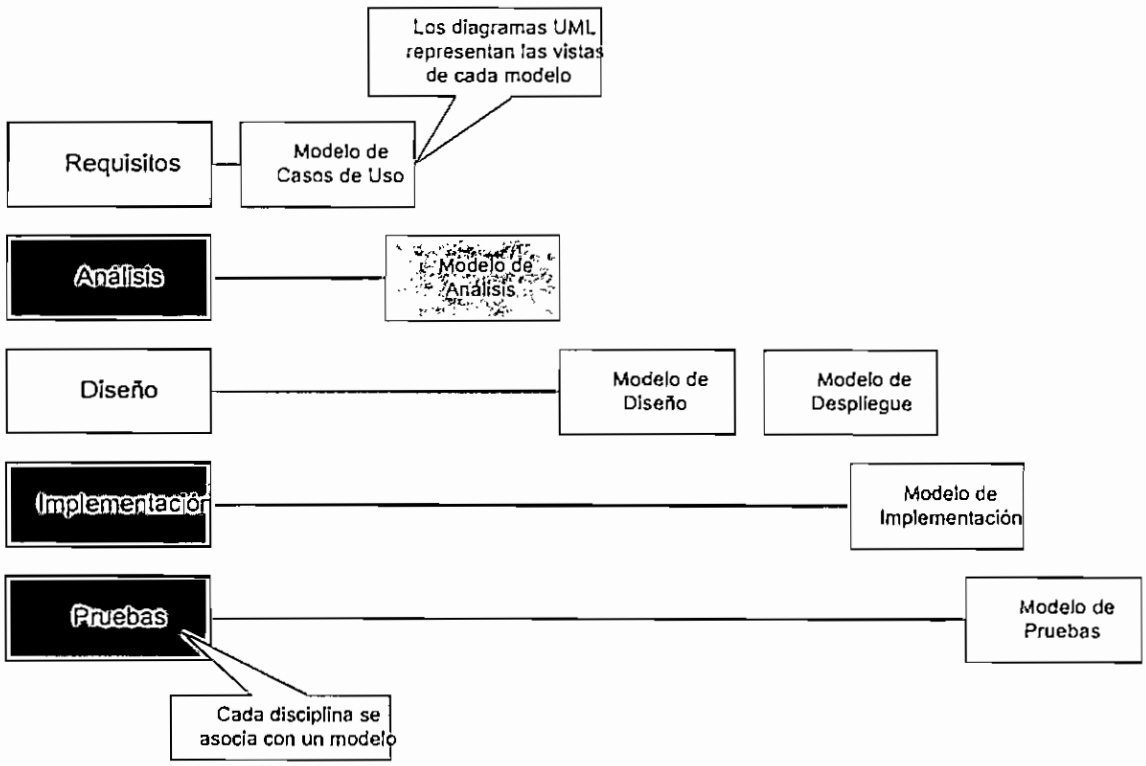



Figura 3.5 Modelos del PUD[22]

### 3.3.1.8 Modelos de Casos de Uso

Este implica el diseño del Modelo del Negocio y del Modelo del Dominio, para lo cual se toman en cuenta los siguientes conceptos:

[22] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, Pag. 32.

- **Actor**: es algo o alguien que va a interactuar con el sistema.
- **Caso de Uso**: conjunto de acciones a ejecutar por el sistema, cuyo resultado es de interés para un actor.
- **Colaboración**: especifica las interacciones entre objetos, para que estos desempeñen sus funciones adecuadamente.
- **Relaciones**: establece el direccionamiento de las interacciones. Existen tres tipos de relaciones: asociación (invocación desde un actor o caso de uso a otra operación), instanciación (dependencia entre casos de uso), y generalización (relación que puede ser de uso o de herencia).

#### *3.3.1.8.1 Modelo del Negocio*

Detalla como se realiza un proceso a través de un conjunto de trabajadores, considerando entidades y unidades de trabajo a utilizar.

Se deben identificar los diversos tipos de negocio y sus actores, desarrollando un modelo de objetos con los trabajadores, entidades de negocio, y unidades de trabajo, además de definir un actor por cada trabajador y sus funciones para los distintos casos.

#### *3.3.1.8.2 Modelo del Dominio*

Define el área de trabajo del sistema, el dominio dentro del área, los requerimientos funcionales y no funcionales, y el listado preliminar de clases acorde a su relación con los requerimientos.

Adicionalmente en este modelo, se define un diagrama de clases para describir el contenido del sistema. Un diagrama de clases muestra la estructura estática del modelo, incluyendo clases y tipos existentes, estructura interna, y relaciones con otras clases.

### 3.3.1.9 Modelo de Análisis

Representa la estructura global del sistema, y permite depurar los casos de uso, detallándolos para estructurarlos en clases y paquetes de análisis, como se muestra en la Figura 3.6.

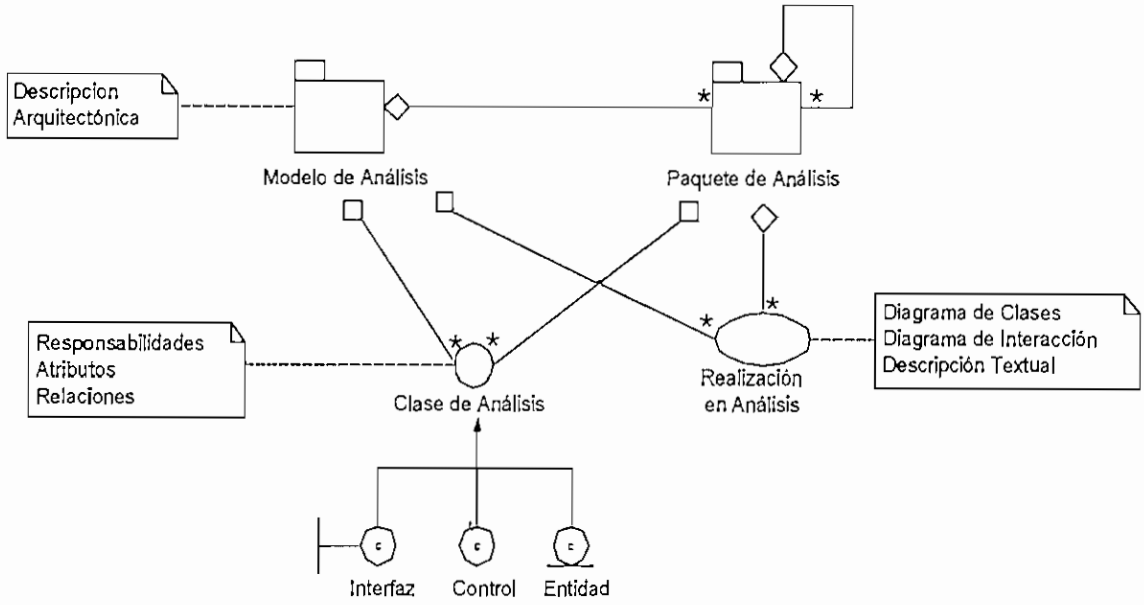



**Figura 3.6 Modelo, Clase y Paquete de Análisis**[23]

- **Clases de Análisis**: se basan en los requisitos funcionales, definiéndose tres tipos de clases: Clase Interfaz (interfaz del sistema y peticiones del actor), Clase Control (lógica del negocio, cálculos y flujo de control de un caso de uso), y Clase Entidad (maneja información y operaciones asociadas).
- **Paquetes de Análisis**: permiten organizar, las clases de análisis, los casos de uso y otros paquetes, acorde a un criterio de afinidad.

### 3.3.1.10 Modelo de Diseño

Define las actividades de implementación del sistema, y tiene los siguientes elementos: subsistema de diseño e interfaz, clases de diseño y la realización del diseño.

En la Figura 3.7 se resume los componentes del modelo de diseño y su interrelación.

[23] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, Pag. 172.

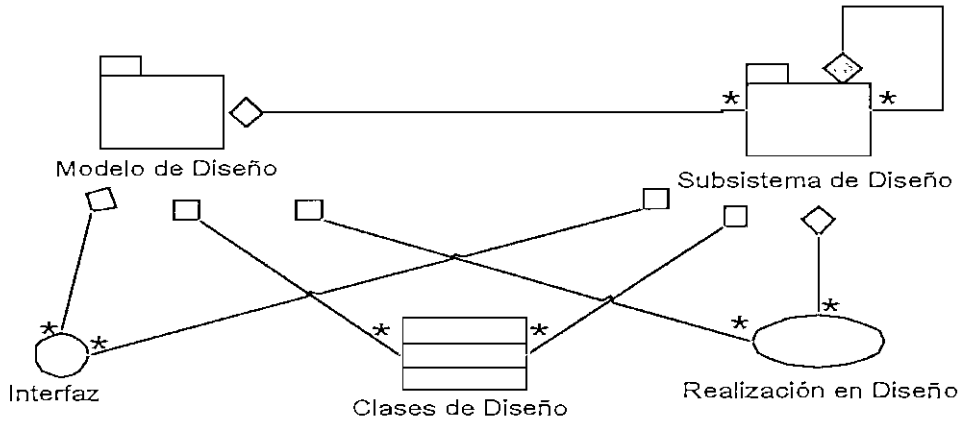



**Figura 3.7 Modelo de Diseño**[24]

*3.3.1.10.1 Clases de Diseño*

Es una abstracción de una clase de implementación que, maneja atributos, operaciones, tipos, y relaciones entre clases de diseño. Su manejo depende del lenguaje de programación a utilizar para la implementación.

*3.3.1.10.2 Realización del Diseño*

Para realizar el diseño de un caso de uso, se debe realizar:

- **Diagramas de Clases**: una clase de diseño puede ser parte de varios casos de uso.
- **Diagramas de secuencia**: cuando un actor envía mensajes a un objeto de diseño, se produce una secuencia de acciones de un caso de uso.
- **Descripción textual del flujo de eventos**: describe un diseño de secuencia.
- **Requisitos de implementación**: gestiona requisitos del diseño no considerados inicialmente.

*3.3.1.10.3 Subsistema de Diseño e Interfaz*

El subsistema de diseño organiza: clases de diseño, casos de uso, interfaces y otros subsistemas.

[24] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, Pag. 208.

Para que las clases de diseño soporten las operaciones del interfaz se deben utilizar métodos, en cambio para que los subsistemas de diseño soporten dichas operaciones, requieren utilizar las clases de diseño.

### 3.3.1.11 Modelo de Despliegue

Describe la distribución física del sistema, definiendo las funciones a ejecutar por un nodo computacional y los mecanismos existentes entre ellos. La funcionalidad de un nodo se determina por sus componentes.

### 3.3.1.12 Modelo de Implementación

Describe la forma como los elementos del diseño se implementan en componentes. Sus objetivos son: planificar integraciones del sistema, distribuir el sistema en nodos, implementar clases y subsistemas, y probar componentes individualmente. La figura muestra los elementos del modelo de implementación.

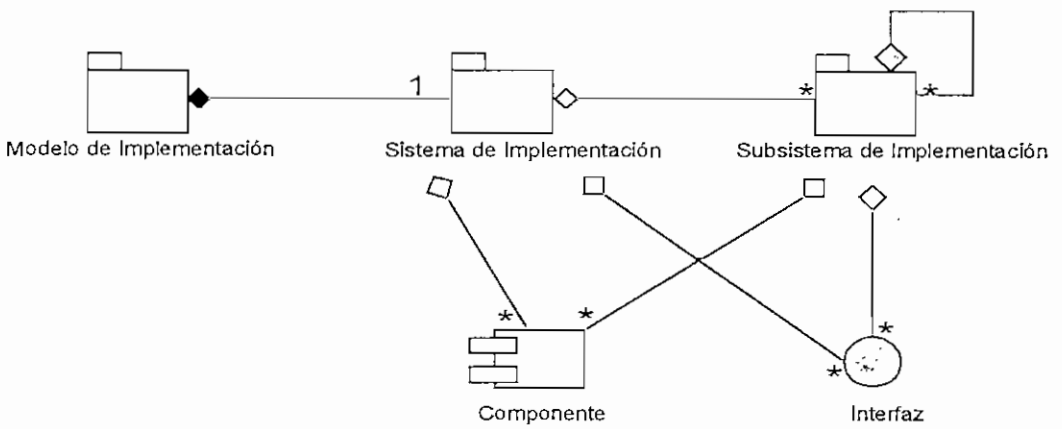



**Figura 3.8 Modelo de Implementación**[25]

Los componentes constituyen los elementos del modelo del diseño empaquetados, e implementan varios elementos y proporcionan una interfaz. Un subsistema de implementación, es el mecanismo de empaquetamiento que organiza los elementos del modelo de implementación. Finalmente una interfaz es una operación implementada por componentes y subsistemas de implementación.

[25] JACOBSON I., BOOCH G., RUMBAUGH J.; El Proceso Unificado de Desarrollo de Software, Pag. 257.

#### 3.3.1.13 Modelo de Pruebas

Permite validar los casos de uso basándose en las pruebas realizadas, y planificar las pruebas de sistema y de integración necesarias para cada iteración.

En esta etapa se prueba el modelo de implementación, empezando por el nivel bajo del sistema, pasando por los casos de uso y finalmente realizando una prueba en el mismo sistema. Un modelo de prueba puede ser comprobado mediante un modelo de requerimientos.

Para realizar una prueba se deben seguir los siguientes pasos: planificar y describir detalladamente lo que se desea probar, y especificar los recursos necesarios para ello. Adicionalmente se debe especificar y describir el propósito de realización de las pruebas, detallando cada paso realizado en las mismas.

Finalmente se almacenan los resultados de las pruebas realizadas en una tabla de decisión, en la que se incluyen factores de peso a subtests según su importancia. Se debe medir y comparar la prueba total, para determinar si ésta fue exitosa o fallida.

### 3.3.2 ESTUDIO DE FACTIBLIDAD

Previo a elaborar el sistema, es necesario determinar la factibilidad de realización y utilización del mismo. Los recursos a considerar son:

a) Humanos: analista/programador, y responsable del mantenimiento y actualización del proyecto.
b) Tecnológicos: recursos de hardware y software.

Para evaluar estos recursos, se lo hace mediante el costo de elaboración del sistema (Tabla 3.3 Costos), por ser uno de los parámetros de mayor importancia para la adquisición del mismo a nivel de mercado de compra.

Para el caso de los programadores, se considera su trabajo por tres meses, y un costo - hora de $3, dando un total de $1440 por cada persona. Adicionalmente,

para el costo de los computadores, se considera su tiempo de uso, ya que los analistas disponen de los mismos.

| Recursos | Cantidad | Costo Parcial | Costo Total |
|---|---|---|---|
| Analista/ Programador | 2 | 1440 | 2880 |
| Licencias de Software | 2 | - | - |
| Computadores | 2 | 100 | 200 |
| | | Total | 3080 |

**Tabla 3.3 Factibilidad del Sistema**

Mediante la utilización de este software, las entidades médicas, serán capaces de mantener un control centralizado de la información, tanto de pacientes como doctores, además de convertirse en una organización cero papel en lo que a atención médica se refiere. Adicionalmente, permite disminuir el error humano en mediciones clínicas provocado por descuidos involuntarios y reducir el tiempo del proceso de atención.

Con estos antecedentes, se justifica ampliamente la factibilidad del software a elaborar.

### 3.3.3 ANÁLISIS DEL SISTEMA

El propósito de este ítem es dar a conocer los requerimientos del personal médico y administrativo de la clínica, para en base a ellos llevar a cabo el proceso unificado de desarrollo de software y así elaborar la aplicación.

La "Clínica Durán", es una institución cuyo manejo de información tanto de pacientes como del personal médico se manipula de forma manual, pese a contar con los equipos de cómputo adecuados.

Con estas referencias, se busca automatizar el proceso de atención al paciente, mediante el manejo de la información a través del sistema a elaborarse. El sistema llevará a cabo un procedimiento ordenado en lo que a administración de usuarios - pacientes - doctores - citas, obtención de signos vitales, manejo de historias clínicas, y reportes se refiere.

En este análisis se toman en cuenta únicamente las dos áreas de mayor concurrencia de pacientes dentro de la Clínica "Durán", como son Consulta Externa y Emergencia, para lo cual se detalla su proceso de funcionamiento:

En Consulta Externa:

- El paciente llama o se presenta a reservar una cita médica, especificando día, hora y especialidad médica que requiere.
- En la fecha acordada, el paciente se presenta en la clínica y se acerca a cancelar el valor de su consulta, generando así un formulario que contiene la Historia Clínica del paciente, el cual es enviado al encargado de la toma de Signos Vitales.
- El paciente es llamado a la toma de signos vitales, utilizando los sensores; estos datos se transfieren en tiempo real a la base de datos.
- El Doctor luego de atender al paciente, agregará su diagnóstico a un formulario general, que contiene todos los ítems anteriores.

En el caso de Emergencia se contemplarán dos opciones:

- La llegada del paciente sin contar con los servicios de la clínica, para lo cual la medición de signos vitales se llevará a cabo en emergencias, donde se generará el formulario del paciente con su historia clínica si la tuviese.
- Y la llegada del paciente en la ambulancia de la clínica, en la cual se realizará la medición de signos vitales, en caso de que el paciente cuente con su historial clínico, éste y la información de signos vitales se cargarán en el formulario de Emergencias.

Finamente, el doctor luego de atender al paciente, agregará su diagnóstico al formulario en ambos casos.

#### 3.3.3.1 Requerimientos Específicos

##### *3.3.3.1.1 Funcionalidad*

- **Gestionar Coordinadores**: registro, actualización y eliminación de la información de usuarios y sus perfiles.

- **Gestionar Pacientes**: registro, actualización y eliminación de la información de los pacientes, esta información puede ser manipulada por el administrador y los coordinadores.
- **Gestionar Signos Vitales**: registro, y actualización de los datos de signos vitales obtenidos a través de los sensores.
- **Gestionar Citas**: registro, actualización y eliminación de reservación de citas para la atención médica de pacientes en Consulta Externa.
- **Gestionar Diagnóstico Médico**: registro, actualización y eliminación de historias clínicas en Consulta Externa y Emergencias.
- **Generar Reportes**: despliega la información registrada en el sistema acorde a las necesidades del administrador.

*3.3.3.1.2 Usabilidad*

- **Entrenamiento a Usuarios**: el sistema debe ser amigable y fácil de usar, por lo que se requiere entrenar a los coordinadores sobre el funcionamiento del sistema.
- **Estándares de Interfaz de la Aplicación Cliente – Servidor**: mantener áreas definidas para la manipulación de la información con botones, menús, y mensajes.

*3.3.3.1.3 Confiabilidad*

- **Disponibilidad**: el sistema debe estar disponible las 24 horas del día, los 365 días del año.
- **Reparación de Fallas**: se provee un tiempo no mayor a 3 horas para reparar el sistema en el caso de falla.

*3.3.3.1.4 Desempeño*

- **Tiempo de Respuesta**: las transacciones simples no deben demorar más de 1 segundo y las de obtención de datos de los equipos no más de 15 segundos.

La principal razón de estos parámetros de tiempo, se debe a que en el campo médico, un segundo puede ayudar a salvar la vida de un paciente.

- **Capacidad**: debido a que el sistema no va a tener gran afluencia de usuarios no se requiere llevar un control de acceso.

*3.3.3.1.5 Soporte*

Se elaborará el sistema en base a estándares de programación y bases de datos, lo que facilitará su mantenimiento.

### 3.3.3.2 Modelo de Casos de Uso

*3.3.3.2.1 Definición de Actores*

| ACTORES | DESCRIPCIÓN |
|---|---|
| Administrador | - No tiene restricciones de acceso al sistema.<br>- Acceso total a la información del sistema.<br>- Administra los usuarios del sistema. |
| Coordinador | - Acceso a los formularios de Reserva de Citas, Pago de Citas, Medición de Signos Vitales e Historia Clínica.<br>- Estos perfiles son creados solo por el administrador. |

**Tabla 3.4 Definición de Actores**

*3.3.3.2.2 Diagrama de Casos de Uso*

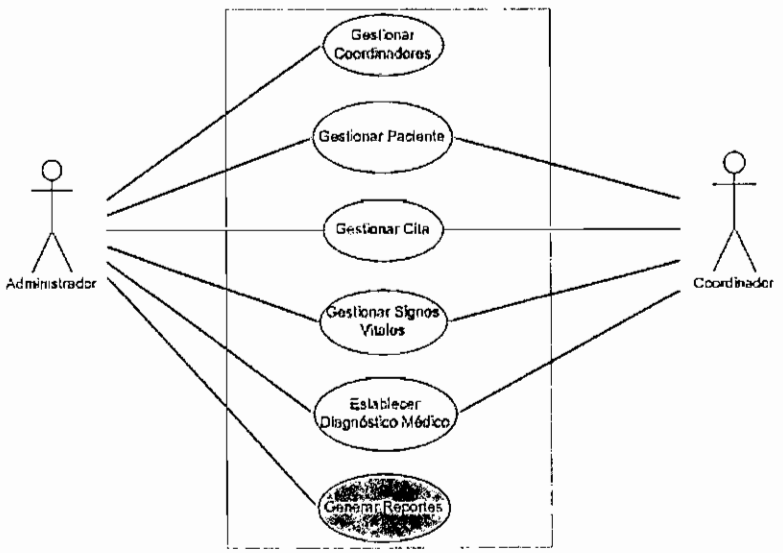



**Figura 3.9 Diagrama de Casos de Uso**

### *3.3.3.2.3 Especificación del Diagrama de Casos de Uso*

| CASO DE USO | DESCRIPCIÓN |
|---|---|
| Gestionar Coordinadores | Mediante el sistema el Administrador puede registrar, actualizar y eliminar coordinadores. |
| Gestionar Pacientes | El sistema activa esta opción para el Administrador y Coordinadores (Doctores y Receptor de Citas), y registra la información ingresada de los pacientes. |
| Gestionar Citas | El sistema verifica la existencia del paciente, la disponibilidad médica del doctor con el que se desea reservar la cita y permite registrar, actualizar y eliminar citas para atención médica en Consulta Externa. |
| Gestionar Signos Vitales | El sistema permite al Administrador y Coordinador (Enfermeras) registrar la información obtenida por los sensores. |
| Gestionar Diagnóstico Médico | El sistema recoge la información del paciente y signos vitales en un solo formulario, por solicitud del coordinador (Doctor), para establecer la historia clínica y diagnostico del paciente. |
| Generar Reportes | El sistema permite al Administrador obtener información de los pacientes en el proceso de atención, solicitada por los coordinadores. |

**Tabla 3.5 Especificación del Diagrama de Casos de Uso**

### *3.3.3.2.4 Especificación de Casos de Uso*

| ANÁLISIS CASO DE USO: Gestionar Coordinadores | |
|---|---|
| ID | Gestionar Coordinadores |
| Descripción | Registrar la información de los coordinadores en el sistema. |
| Precondición | Ninguna. |
| Actividades:<br>1. El Administrador accede al formulario de registro de Coordinadores.<br>2. El sistema verifica si existe el coordinador.<br>3. El Administrador digita la información.<br>4. El sistema valida la información ingresada.<br>5. El sistema almacena el coordinador y su perfil. | |
| Alternativas:<br>1. En 2 si no existe el coordinador se lo agrega.<br>2. En 4 si la información es incorrecta, el sistema pide reingresarla adecuadamente. | |
| Poscondición | El sistema guarda la información del coordinador. |

**Tabla 3.6 Análisis del Caso de Uso Gestionar Coordinadores**

| ANÁLISIS CASO DE USO: Gestionar Pacientes | |
|---|---|
| ID | Gestionar Pacientes |
| Descripción | Su objetivo es registrar los datos de los pacientes en el sistema. |
| Precondición | Que exista una solicitud de registro de paciente. |
| Actividades:<br>1. El Administrador/Coordinador abre el formulario de registro de pacientes.<br>2. El sistema verifica la existencia del paciente.<br>3. El Administrador/Coordinador digita la información.<br>4. El sistema valida la información ingresada.<br>5. El sistema guarda la información. | |
| Alternativas:<br>1. En 2 si no existe el paciente se lo agrega.<br>2. En 4 si la información es incorrecta, el sistema solicita reingresarla adecuadamente. | |
| Poscondición | Registro y actualización de la información en el sistema. |

**Tabla 3.7 Análisis del Caso de Uso Gestionar Pacientes**

| ANÁLISIS CASO DE USO: Gestionar Citas | |
|---|---|
| ID | Gestionar Citas |
| Descripción | Permite registrar la cita médica de un paciente para Consulta Externa. |
| Precondición | Que exista una solicitud de registro de cita. |
| Actividades:<br>1. El Administrador/Coordinador accede al formulario de reserva de cita médica para Consulta Externa.<br>2. El sistema verifica la existencia del paciente.<br>3. El Administrador/Coordinador selecciona la información de la cita médica.<br>4. El sistema verifica la disponibilidad del horario deseado.<br>5. El sistema valida la información ingresada.<br>6. El sistema almacena la cita médica.<br>7. El Administrador/Coordinador accede al formulario de pago de la cita.<br>8. El sistema verifica la existencia de la cita.<br>9. El sistema valida la información ingresada.<br>10. El sistema almacena el pago de la cita médica | |
| Alternativas:<br>1. En 2 si no existe el paciente se lo agrega.<br>2. En 4 si la fecha no está disponible, el sistema pide seleccionar otra.<br>3. En 8 si no existe la cita, el sistema pide realizarla.<br>4. En 5 y 9 si la información ingresada es incorrecta, el sistema pide reingresarla adecuadamente. | |
| Poscondición | El sistema guarda la cita médica y el pago de la misma. |

**Tabla 3.8 Análisis del Caso de Uso Gestionar Citas**

| ANÁLISIS CASO DE USO: Gestionar Signos Vitales | |
|---|---|
| ID | Gestionar Signos Vitales |
| Descripción | Obtener los datos de la medición de signos vitales de los pacientes a partir de los sensores. |
| Precondición | Definir los sensores de medición disponibles y obtener una lista de los pacientes que deben acceder a la medición. |
| Actividades:<br>1. El Administrador/Coordinador accede al formulario de Medición de Signos Vitales.<br>2. El sistema obtiene los datos de la medición de signos vitales a través de los sensores disponibles.<br>3. El Administrador/Coordinador digita la información de los signos vitales faltantes.<br>4. El sistema valida la información ingresada.<br>5. El sistema almacena los datos finales de medición. | |
| Alternativas:<br>1. En 2 si los sensores fallan se reintenta la medición.<br>2. En 5 si la información ingresada es incorrecta, el sistema pide reingresarla adecuadamente. | |
| Poscondición | El sistema guarda la información de la medición. |

**Tabla 3.9 Análisis del Caso de Uso Gestionar Signos Vitales**

| ANÁLISIS CASO DE USO: Establecer Diagnóstico Médico | |
|---|---|
| ID | Establecer Diagnóstico Médico |
| Descripción | Permite recoger la información del paciente en un formulario para que el coordinador (Doctor) de un diagnóstico y toda esta información se almacene en la historia clínica. |
| Precondición | - En Consulta Externa: que se haya reservado una cita y se haya tomado los signos vitales el paciente.<br>- En Emergencia: que se haya registrado al paciente y que se le hayan tomado los signos vitales. |
| Actividades:<br>1. El Administrador/Coordinador accede al formulario de Diagnóstico.<br>2. El Administrador/Coordinador verifica si la información es correcta.<br>3. El Administrador/Coordinador ingresa la información de chequeo del paciente.<br>4. El sistema valida la información ingresada.<br>5. El sistema almacena la información en la historia clínica del paciente. | |
| Alternativas:<br>1. En 2 si la información es incorrecta el Administrador/Coordinador la corrige y almacena.<br>2. En 3 en casos de Emergencia se puede llenar únicamente el estado del paciente y el doctor responsable del mismo, y el sistema genera información por defecto para el mismo. | |
| Poscondición | El sistema guarda la información del diagnóstico. |

**Tabla 3.10 Análisis del Caso de Uso Establecer Diagnóstico Médico**

| ANÁLISIS CASO DE USO: Generar Reportes | |
|---|---|
| ID | Generar Reportes |
| Descripción | Permite visualizar información solicitada por el Administrador en respuesta a una petición de un Coordinador. |
| Precondición | Registro de Datos. |
| Actividades:<br>1. El Administrador selecciona el tipo de reporte.<br>2. El sistema genera el reporte.<br>3. El sistema muestra los resultados. | |
| Alternativas:<br>1. En 3 si no existe información se debe seleccionar otro reporte. | |
| Poscondición | Se visualiza la información deseada. |

**Tabla 3.11 Análisis del Caso de Uso Generar Reportes**

### 3.3.3.3 Modelo de Análisis

#### *3.3.3.3.1 Diagramas de Clases de Análisis*

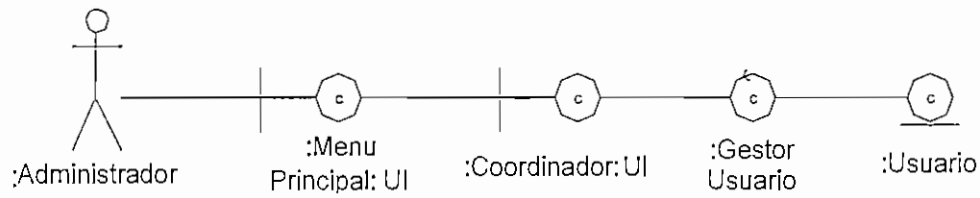



**Figura 3.10 Diagrama de Realización del Caso de Uso Gestionar Coordinadores**

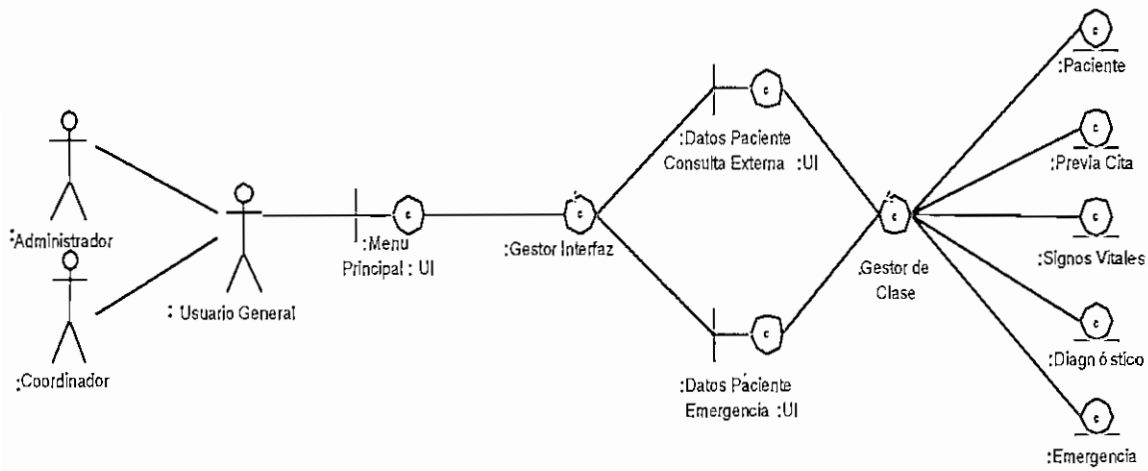



**Figura 3.11 Diagrama de Realización del Caso de Uso Gestionar Pacientes**

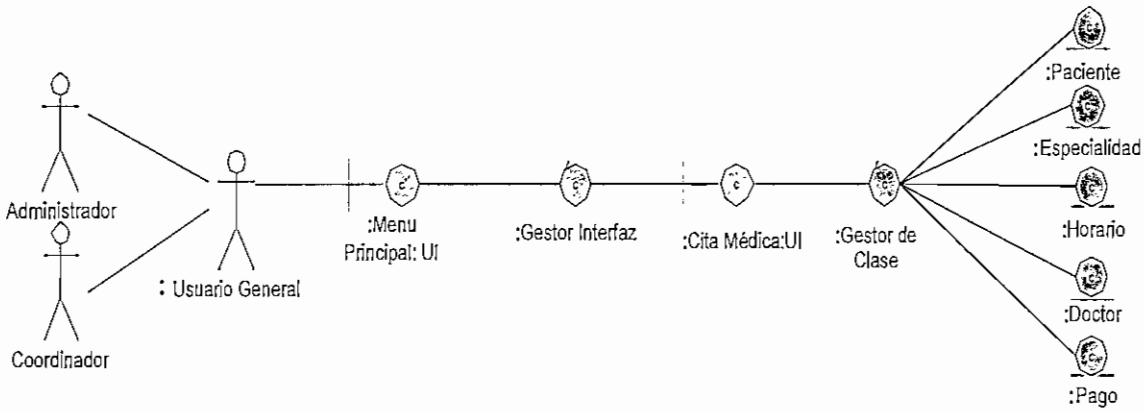



Figura 3.12 Diagrama de Realización del Caso de Uso Gestionar Citas

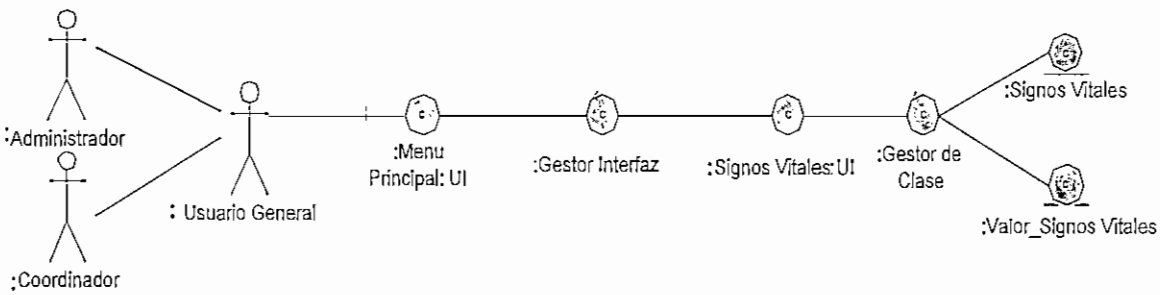



Figura 3.13 Diagrama de Realización del Caso de Uso Gestionar Signos Vitales

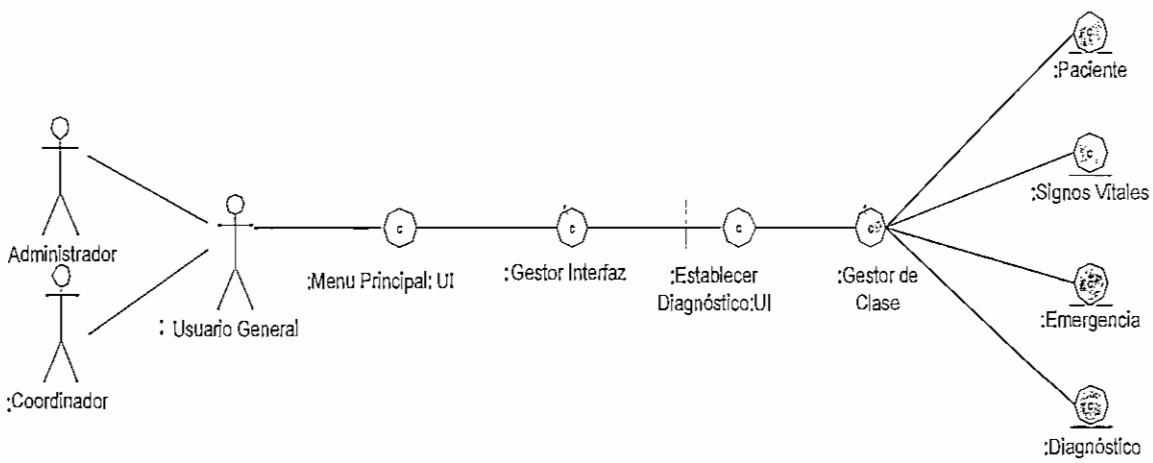



Figura 3.14 Diagrama de Realización del Caso de Uso Establecer Diagnóstico

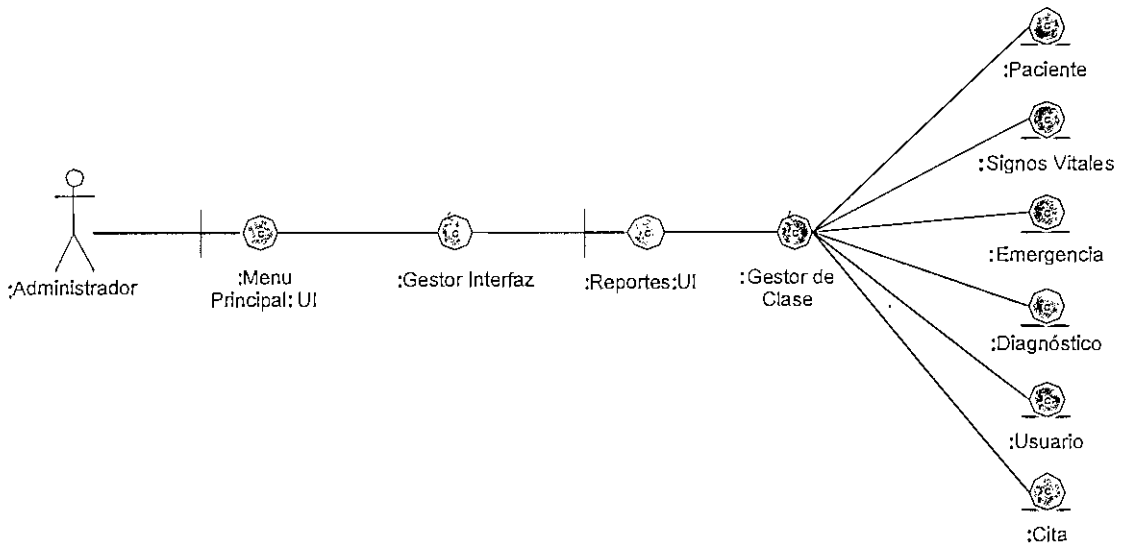



Figura 3.15 Diagrama de Realización del Caso de Uso Generar Reportes

### *3.3.3.3.2 Paquetes de Análisis*


Figura 3.16 Paquete de Administración

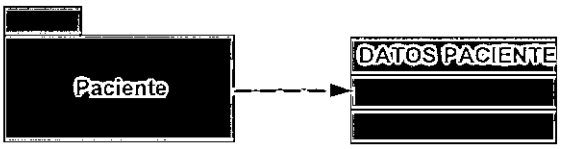



Figura 3.17 Paquete de Paciente


Figura 3.18 Paquete Administrar Cita

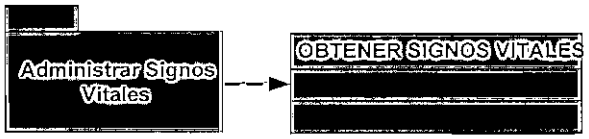



Figura 3.19 Paquete Administrar Signos Vitales

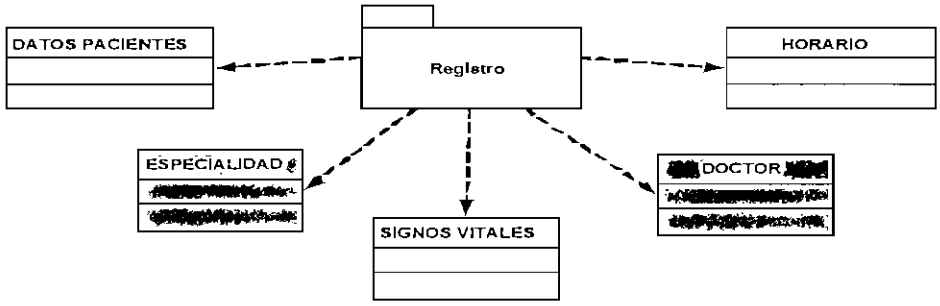



Figura 3.20 Paquete de Registro

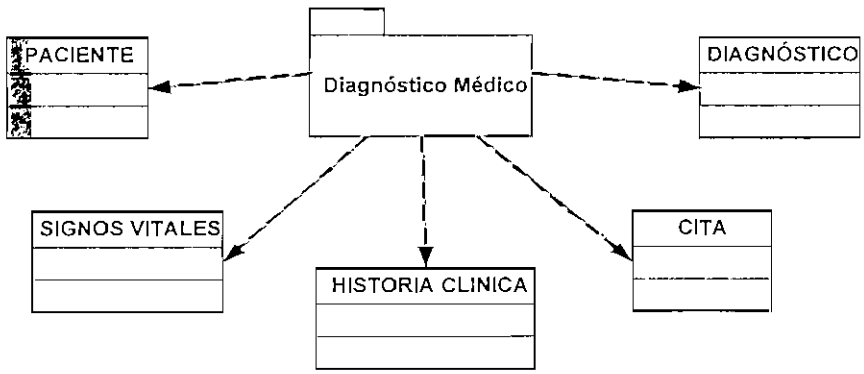



Figura 3.21 Paquete de Diagnóstico Médico

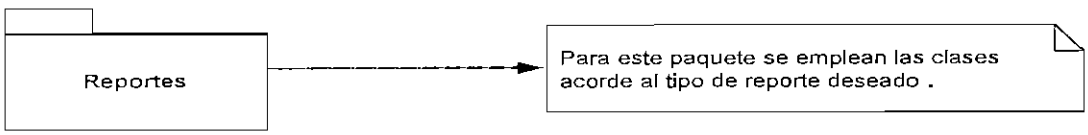



Figura 3.22 Paquete de Reportes

### 3.3.3.4 Diseño de las interfaces de Usuario

*3.3.3.4.1 Diagrama de Navegación*

El diagrama de navegación está en función del perfil de usuario que ingrese al sistema, ya sea como Coordinador o Administrador.

Estos esquemas se muestran a continuación:

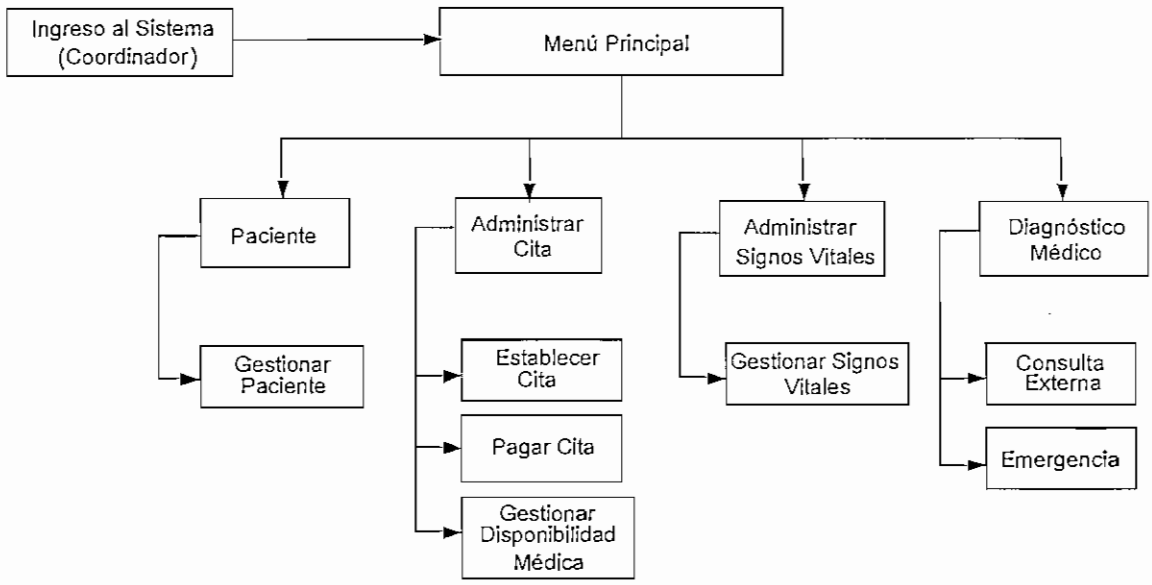



Figura 3.23 Diagrama de Navegación Coordinador

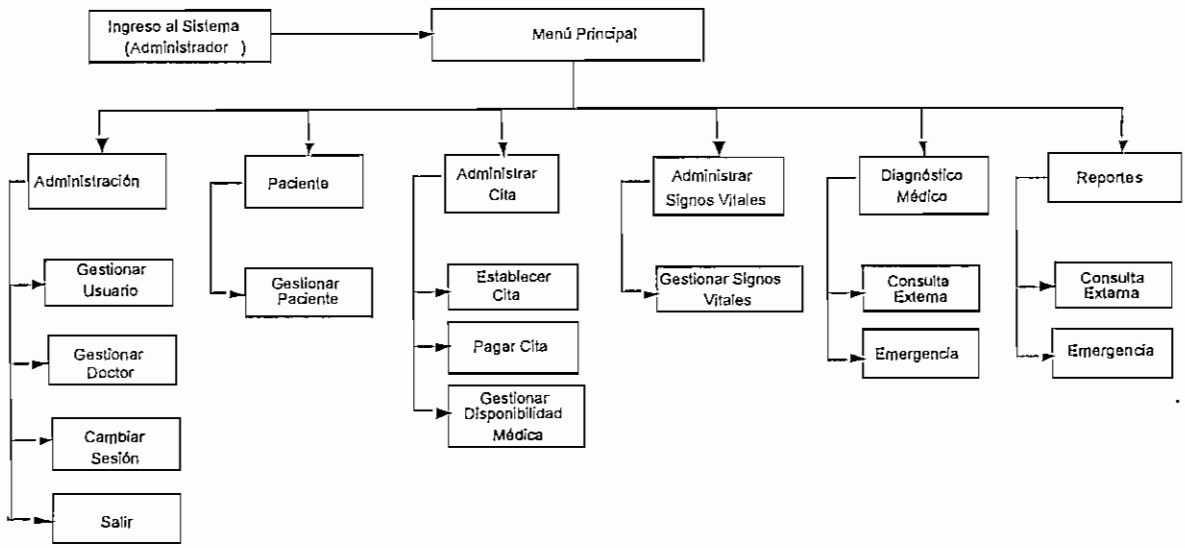



Figura 3.24 Diagrama de Navegación Administrador

### *3.3.3.4.2 Descripción de las Interfaces de Usuario*

La pantalla de Administración de usuario/doctor incluye tres áreas:

- **Área de Título**: incluye el nombre del formulario del sistema.

- **Área de Registro de Usuario/Doctor**: en esta área se encuentran las cajas de texto para ingresar los datos del usuario/doctor.
- **Área de Botones**: en esta área se localizan los botones que permiten agregar, eliminar o actualizar los datos del usuario/doctor del sistema.

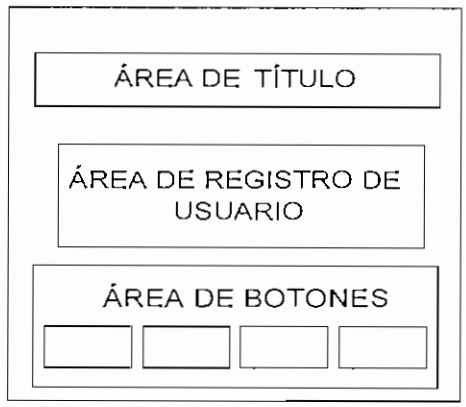



**Figura 3.25 Interfaz de Registro de Usuario/Doctor**

En las Pantallas restantes se diferencian las siguientes áreas principales:

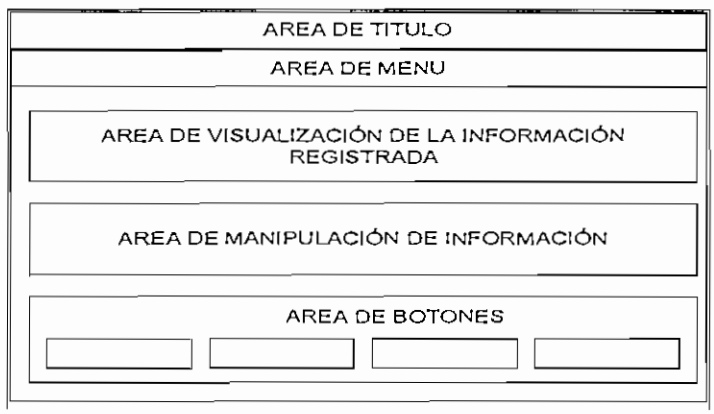



**Figura 3.26 Interfaz General del Sistema**

- Área de Título: incluye el nombre del formulario del sistema.
- Área de Menú: en ésta área se ubica el menú principal del sistema.
- Área de Visualización de información: en ésta área se despliegan los registros existentes en la base de datos de la entidad que se manipula.
- Área de Manipulación de Información: en esta área se colocan las cajas de texto, botones de selección, cajas de selección múltiple, y otras, para permitir registrar información en el sistema.

- Área de Botones: en esta área se ubican los botones del sistema que permiten realizar diversas tareas como: almacenamiento, consulta, actualización o eliminación de registros.

## 3.4 CREACIÓN DE LA BASE DE DATOS

### 3.4.1 Arquitectura del Sistema

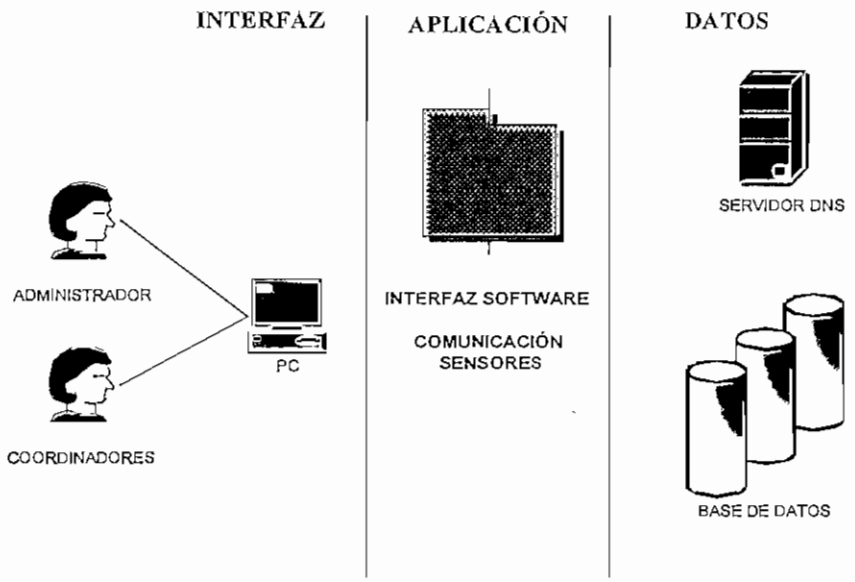



**Figura 3.27 Interfaz, Aplicación y Datos**

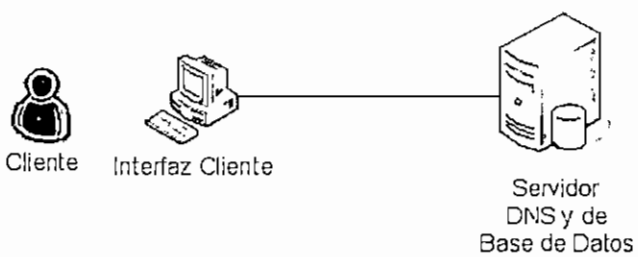



**Figura 3.28 Arquitectura del Sistema**

Servidor de Base de Datos.- se encarga del control de la apertura de las bases de datos, las cuales se abren una sola vez, sin importar el número de estaciones que estén accediendo a los archivos.

Se selecciona *MySQL Server 5.0* como motor de base de datos, por ser una herramienta gratuita, y lo suficientemente completa para este proyecto. En el

servidor de base de datos se levantará la base diseñada en *MySQL*, que incluirá tablas, procedimientos, reglas y tipos de datos definidos.

Servidor DNS.- proporciona el servicio DNS, como mecanismo de asociación a la red, para proveer perfiles de acceso a la misma.

Interfaz de Cliente.- es el Terminal mediante la cual se accede al sistema siempre y cuando se tengan las claves y permisos para realizarlo, luego de lo cual se ingresa al sistema de acuerdo al perfil designado.

### 3.4.2 Modelo de Diseño

#### 3.4.2.1 Modelo del Dominio

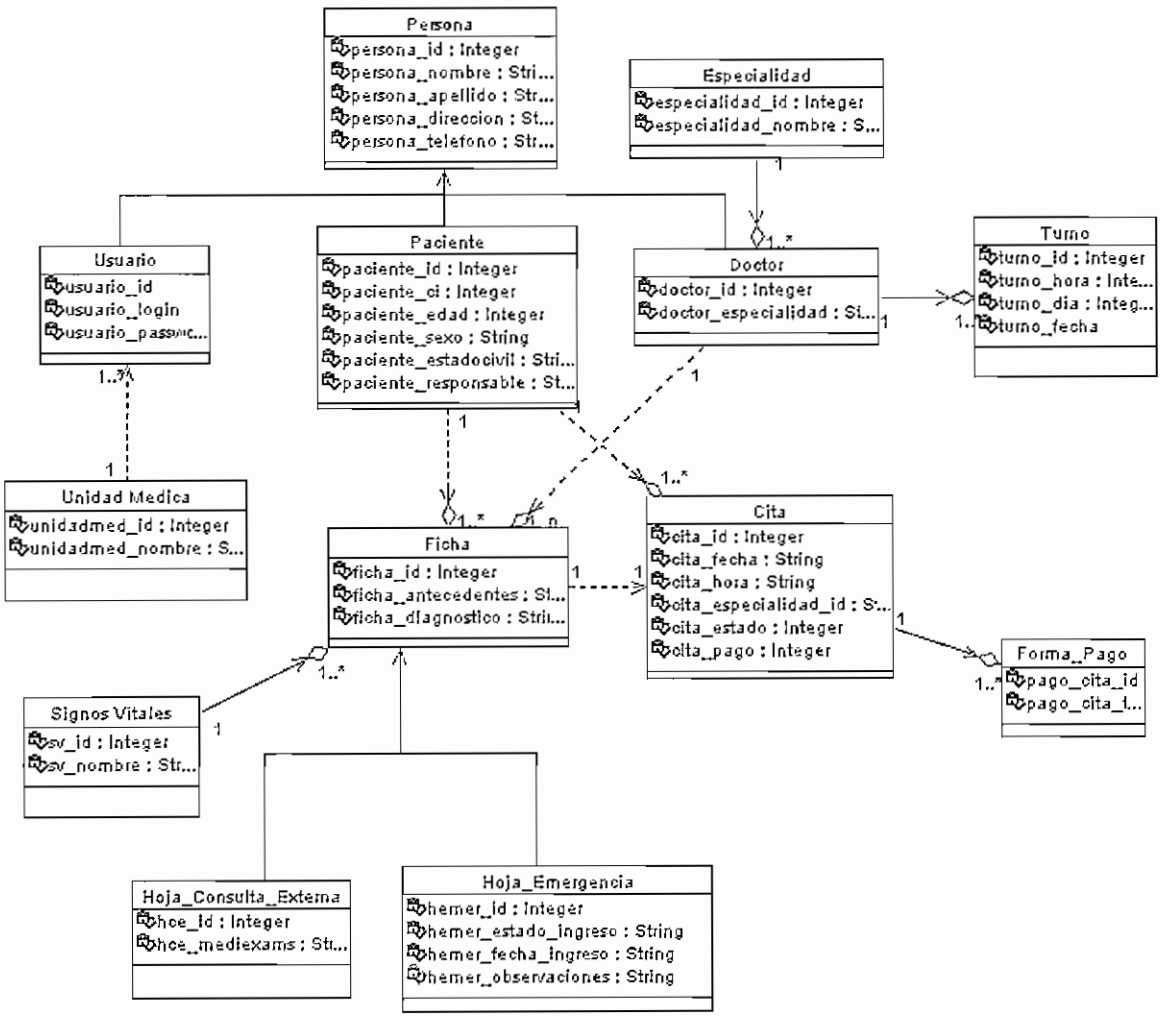



**Figura 3.29 Modelo de Dominio**

### 3.4.2.2 Diagrama de Secuencia

Para este proyecto, se ha decidido elaborar los Diagramas de Secuencia para los casos de mayor complejidad, los cuales se presentan a continuación.

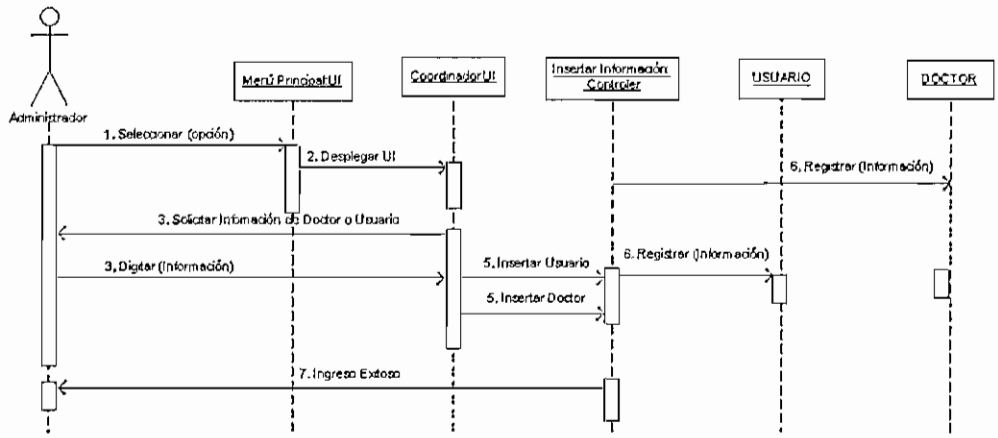



Figura 3.30 Diagrama de Secuencia del Caso de Uso Gestionar Coordinadores

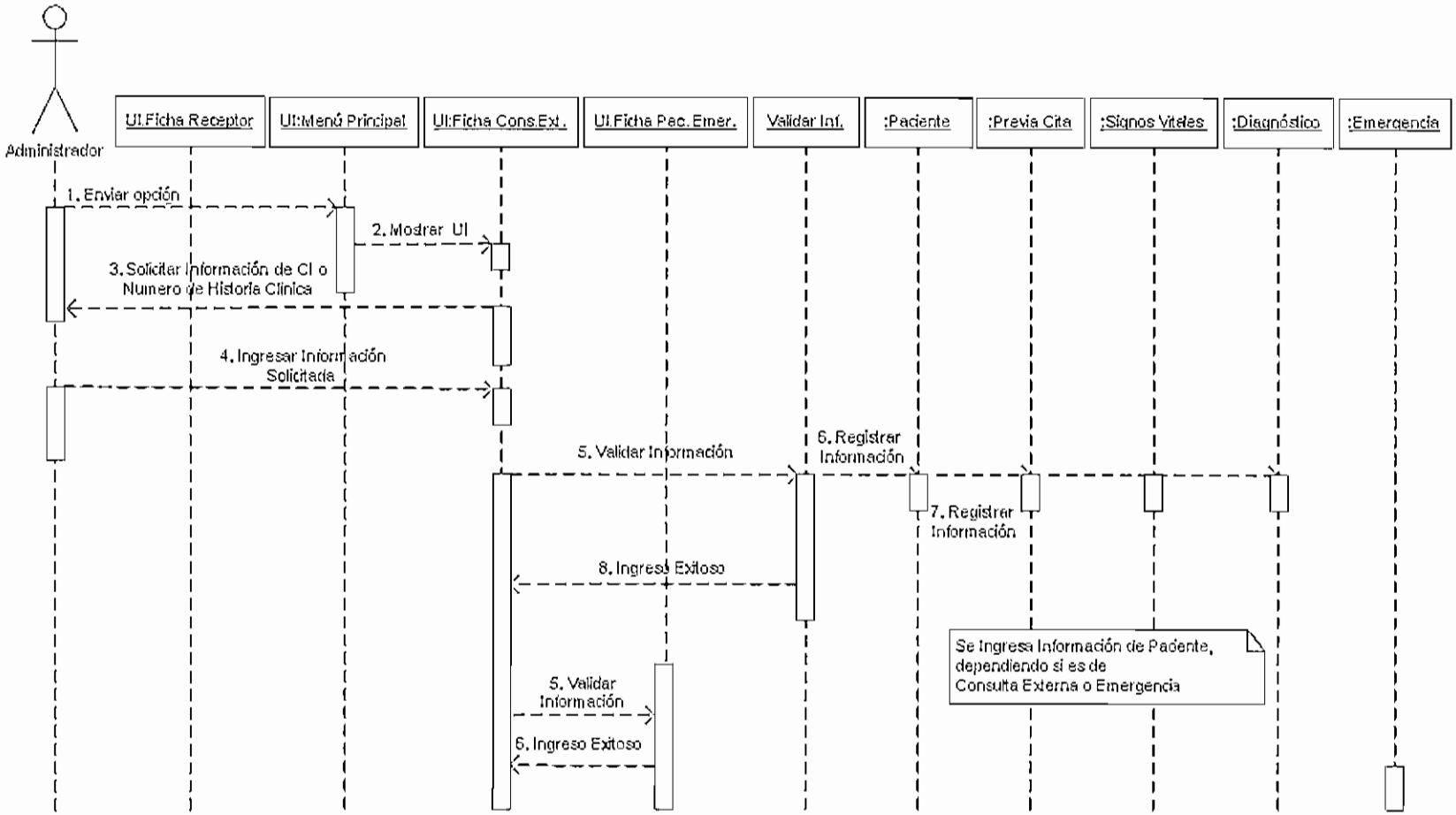



Figura 3.31 Diagrama de Secuencia del Caso de Uso Gestionar Pacientes

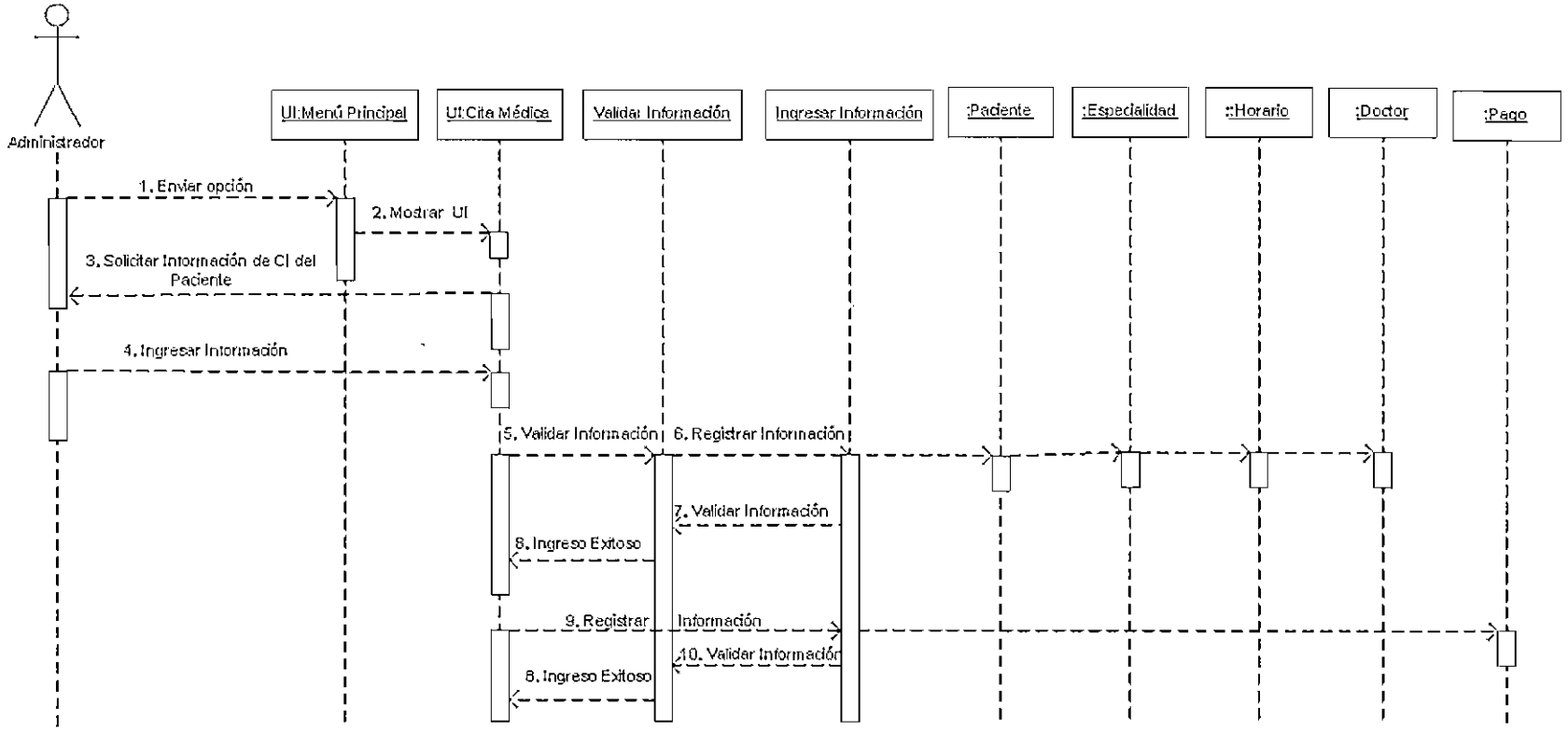



Figura 3.32 Diagrama de Secuencia del Caso de Uso Gestionar Cita

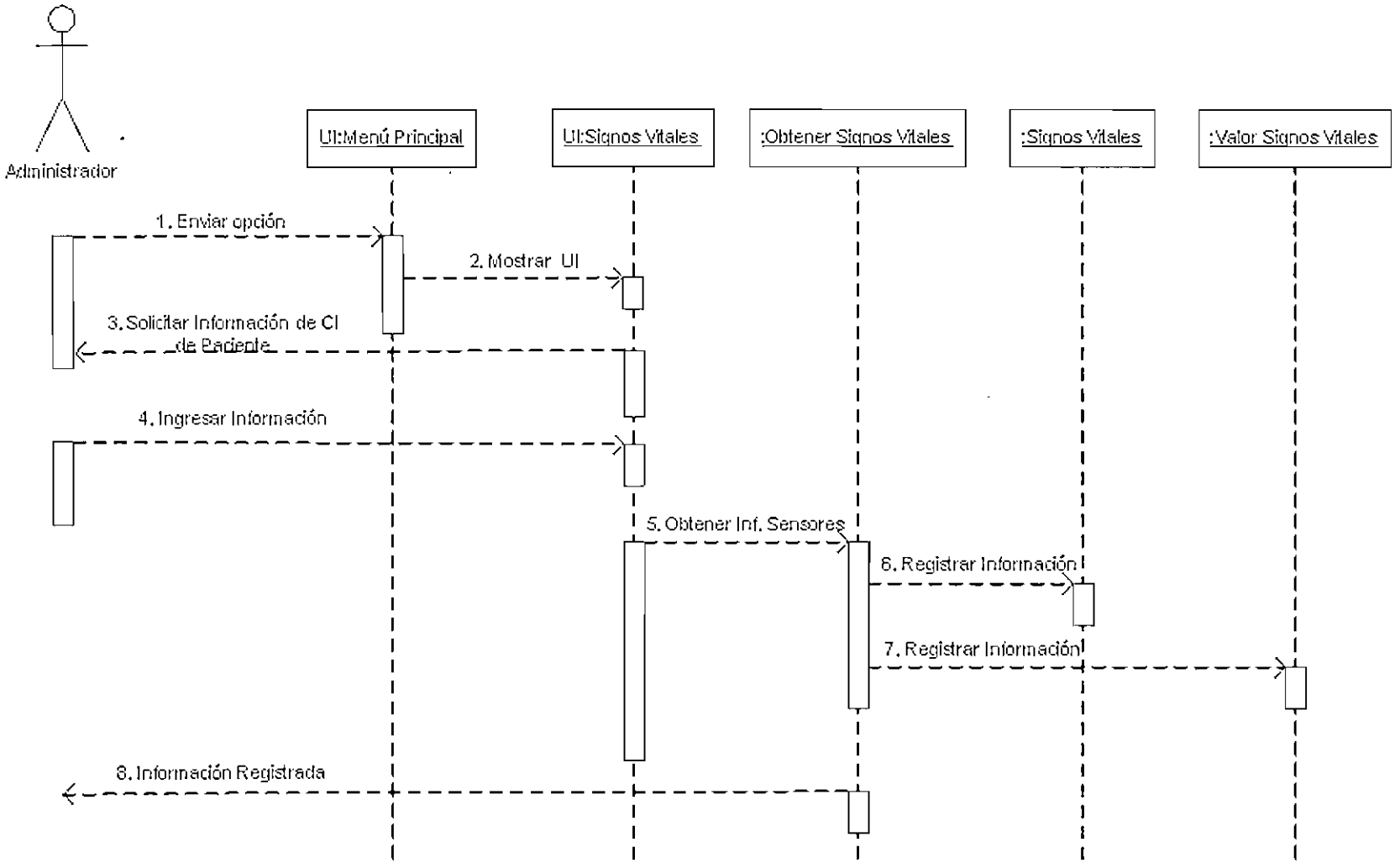



Figura 3.33 Diagrama de Secuencia del Caso de Uso Gestionar Signos Vitales

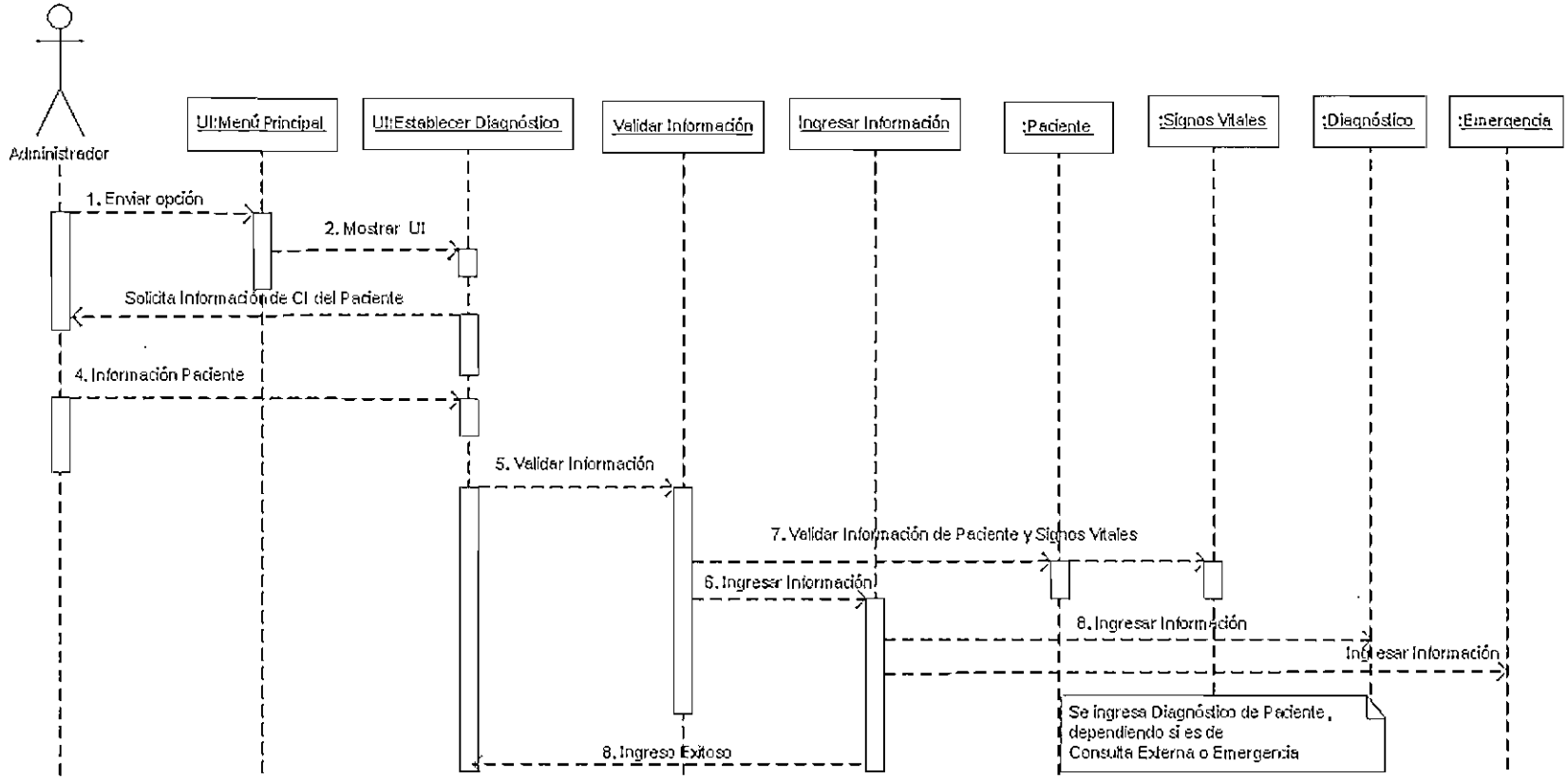



Figura 3.34 Diagrama de Secuencia del Caso de Uso Establecer Diagnóstico

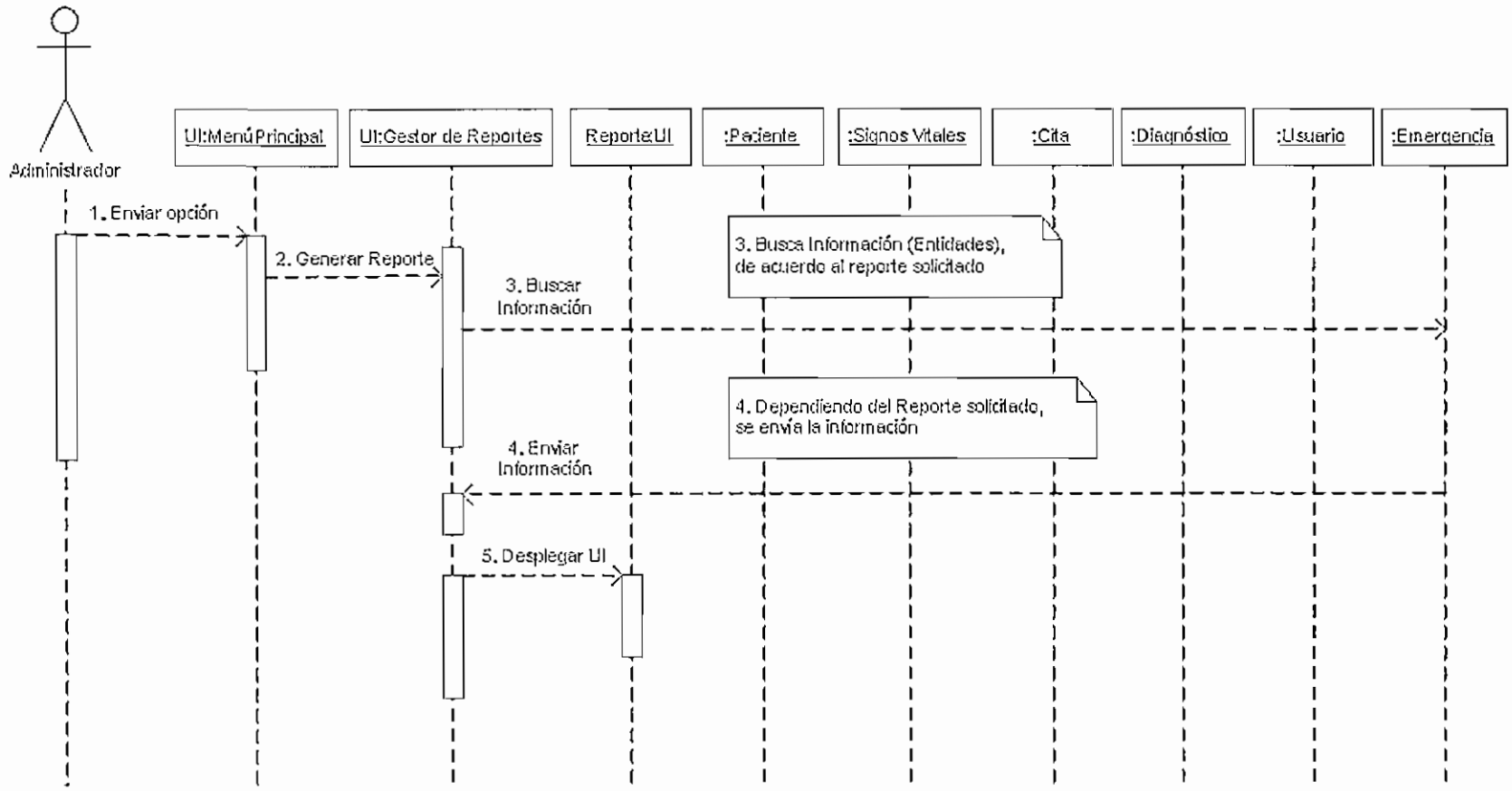



Figura 3.35 Diagrama de Secuencia del Caso de Uso Generar Reportes

### 3.4.2.3 Diagrama de Actividad

Dentro del sistema se tienen varios casos de uso, los mismos que tienen sus respectivos Diagramas de Actividad. A continuación se presentan dos ejemplos: un simple y un complejo, el resto de esquemas se los omite por ser similares a los presentados.

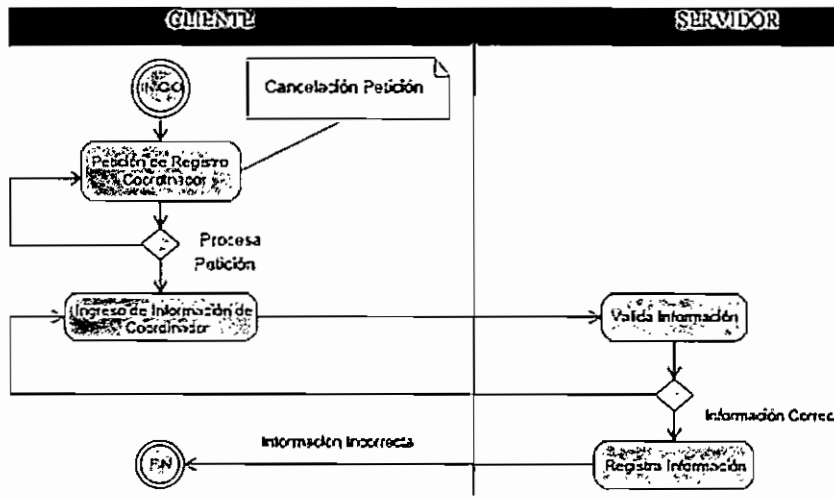



Figura 3.36 Diagrama de Actividad del Caso de Uso Gestionar Coordinadores

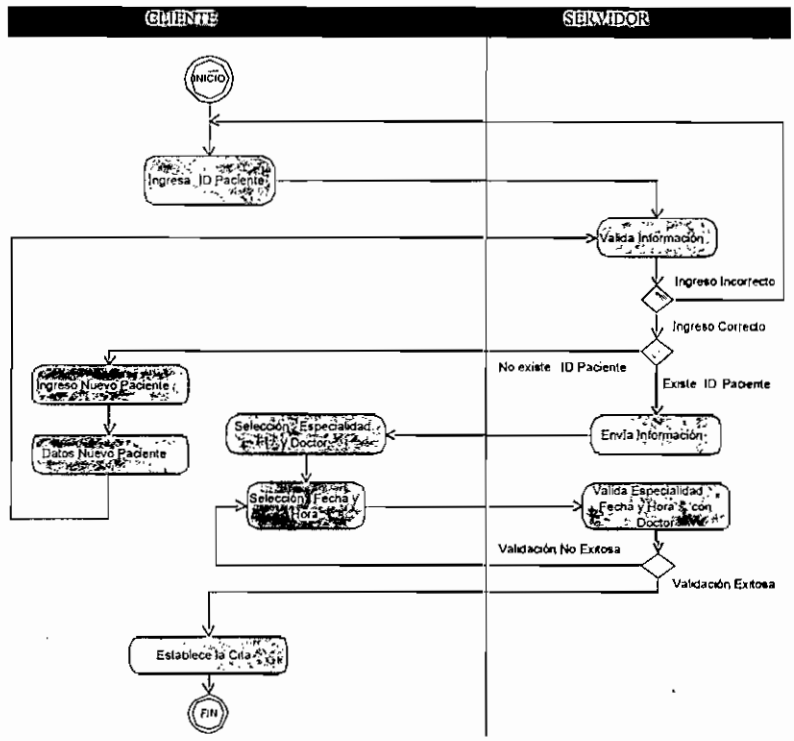



Figura 3.37 Diagrama de Actividad del Caso de Uso Gestionar Cita

### 3.4.2.4 Diagrama de Estados

A continuación se presenta el Diagrama de Estado relevante de este sistema, que corresponde a los estados del establecimiento de una Cita Médica.

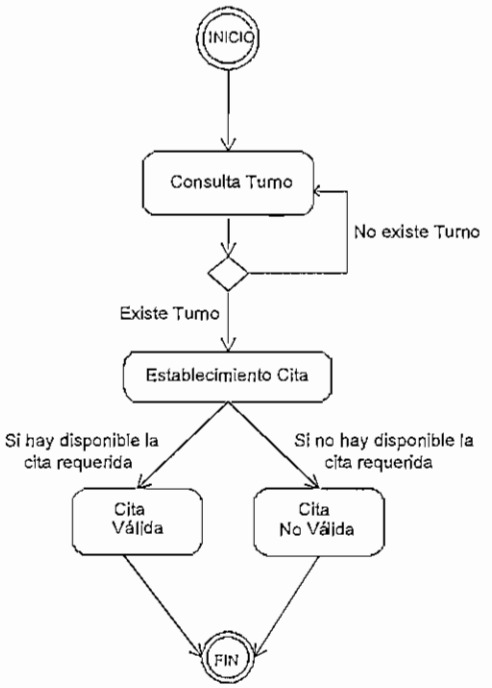



**Figura 3.38 Diagrama de Estado Establecer Cita Médica**

### 3.4.2.5 Diagrama de Componentes

*3.4.2.5.1 Generalidades*

- Componente: equipamiento físico de los elementos de un modelo, que encapsula el código de una aplicación para crear código reutilizable.
- Servicios: son componentes que encierran procesos o algoritmos que desempeñan funciones claras de las aplicaciones, están definidos por un nombre único y su interfaz, a través del cual se puede acceder al servicio. Los servicios permiten que las aplicaciones compartan información y que invoquen funciones de otras aplicaciones independientemente del desarrollo de las aplicaciones, el sistema operativo o la plataforma en que se ejecutan y de los equipos o elementos empleados para acceder a ellas.

- Clase: es una definición de un objeto en la cual se incluyen sus atributos o propiedades, y sus métodos o funcionalidades.

*3.4.2.5.2 Definición de Componentes*

Los componentes que se emplean este sistema son: Servicios, Clases de la Lógica del Negocio, Datos y Presentación. En los servicios existen métodos que permiten manipular la información de la BDD, la presentación es el interfaz expuesto al cliente, y los Datos permiten abrir y cerrar un enlace con la BDD.

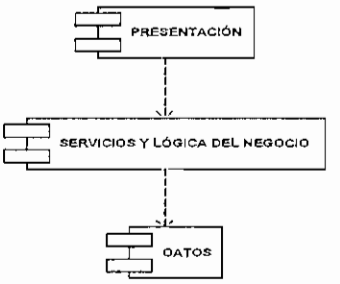



**Figura 3.39 Diagrama de Componentes**

*3.4.2.5.3 Definición de Módulos*

En el sistema se han establecido los siguientes módulos:

- Módulo de Administración
- Módulo de Paciente
- Módulo de Administración Cita
- Módulo de Administración Signos Vitales
- Módulo de Diagnóstico Médico
- Módulo de Reporte

*3.4.2.5.4 Módulo de Administración*

En este modulo se registra a los usuarios que acceden al sistema, definiendo un perfil adecuado para cada uno de ellos y a los Doctores que prestan sus servicios en la clínica y su disponibilidad.

En la tabla se muestra información del servicio empleado en este módulo con sus respectivos métodos.

| Servicio | Métodos |
|---|---|
| Usuario | AgregarUsuario<br>ActualizarUsuario<br>BuscarUsuario<br>EliminarUsuario |
| Doctor | InsertarDoctor<br>BucarDoctor<br>ActualizarDoctor<br>EliminarDoctor |

**Tabla 3.12 Servicios del Módulo de Administración de Usuario/Doctor**

*3.4.2.5.5 Módulo de Paciente*

En este módulo se deben ingresar los datos que son requeridos para el módulo de Paciente. En la tabla se muestra información del servicio empleado en este módulo con sus respectivos métodos.

| Servicios | Métodos |
|---|---|
| DatosPaciente | InsertarPaciente<br>BuscarPaciente<br>ActualizarPaciente<br>EliminarPaciente |

**Tabla 3.13 Servicios del Módulo de Registro**

*3.4.2.5.6 Módulo de Administración Cita*

En este módulo se deben ingresar los datos que son requeridos para establecer y realizar el pago de una cita. En la siguiente tabla se muestra los servicios y métodos correspondientes para este módulo.

| Servicios | Métodos |
|---|---|
| EstablecerCita | BuscarPacienteCita<br>CargarEspecialidadCita<br>SeleccionarFechaCita<br>SeleccionarHoraCita<br>InsertarCita<br>EliminarCita<br>PagoCita |

**Tabla 3.14 Servicios del Módulo Administración Cita**

*3.4.2.5.7 Módulo de Administración Signos Vitales*

En este módulo se deben ingresar los datos que son requeridos para obtener y almacenar los Signos Vitales de un paciente. En la siguiente tabla se muestra los servicios y métodos correspondientes para este módulo.

| Servicios | Métodos |
|---|---|
| SignosVitales | InsertarSignosVitales<br>ObtenerMedicionSignosVitales<br>CalcularIMC<br>ActualizarSignosVitales |

**Tabla 3.15 Servicios del Módulo Administración Signos Vitales**

*3.4.2.5.8 Módulo de Diagnóstico Médico*

En este módulo se deben ingresar los datos que son requeridos para determinar la historia clínica de un paciente. En la siguiente tabla se muestra los servicios y métodos correspondientes para este módulo.

| Servicios | Métodos |
|---|---|
| Paciente | BuscarPaciente |
| Signos Vitales | MostrarSignosVitales |
| Hoja Consulta Externa | VerHistorial |
| Diagnóstico | IngresarAntecedentes<br>IngresarSintomas<br>IngresarMediexams<br>IngresarProximaCita |

**Tabla 3.16 Servicios del Módulo de Diagnóstico Médico**

*3.4.2.5.9 Modulo de Reportes*

En este módulo se filtra información de la BDD para realizar un reporte tanto de pacientes como de usuarios y diagnósticos. La generación de reportes se realizará únicamente en caso de que se tuviese algún problema posterior a la atención de un paciente.

| Servicios | Métodos |
|---|---|
| ReporteEmergencias | PacientesAtendidosFechaSeleccionda |
| ReporteConsultaExterna | PacientesAtendidosFechaSeleccionda |

**Tabla 3.17 Servicios del Módulo de Reportes**

### 3.4.2.7 Modelo Lógico Relacional

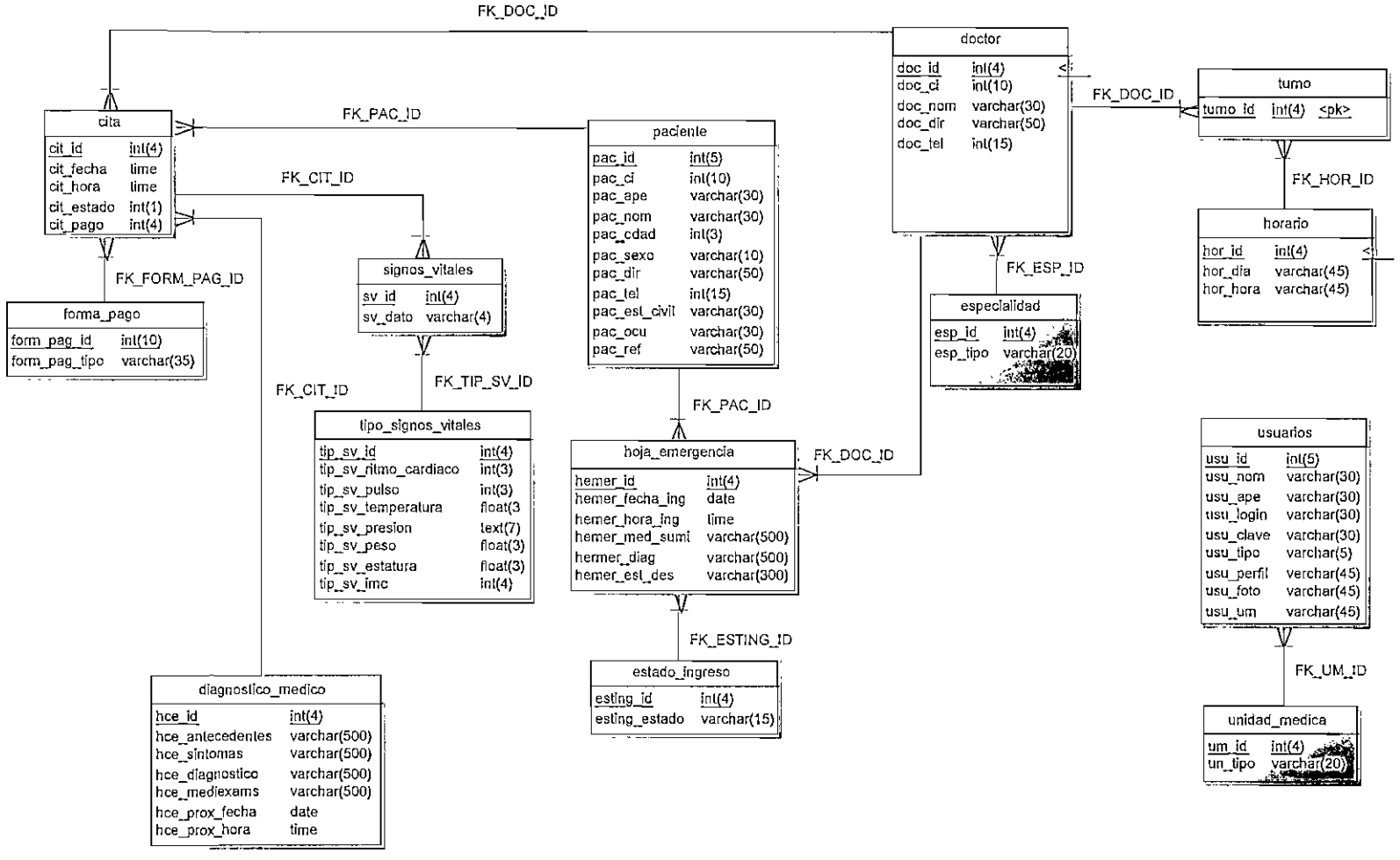



Figura 3.41 Modelo Lógico Relacional

### 3.4.2.8 Modelo Físico Relacional

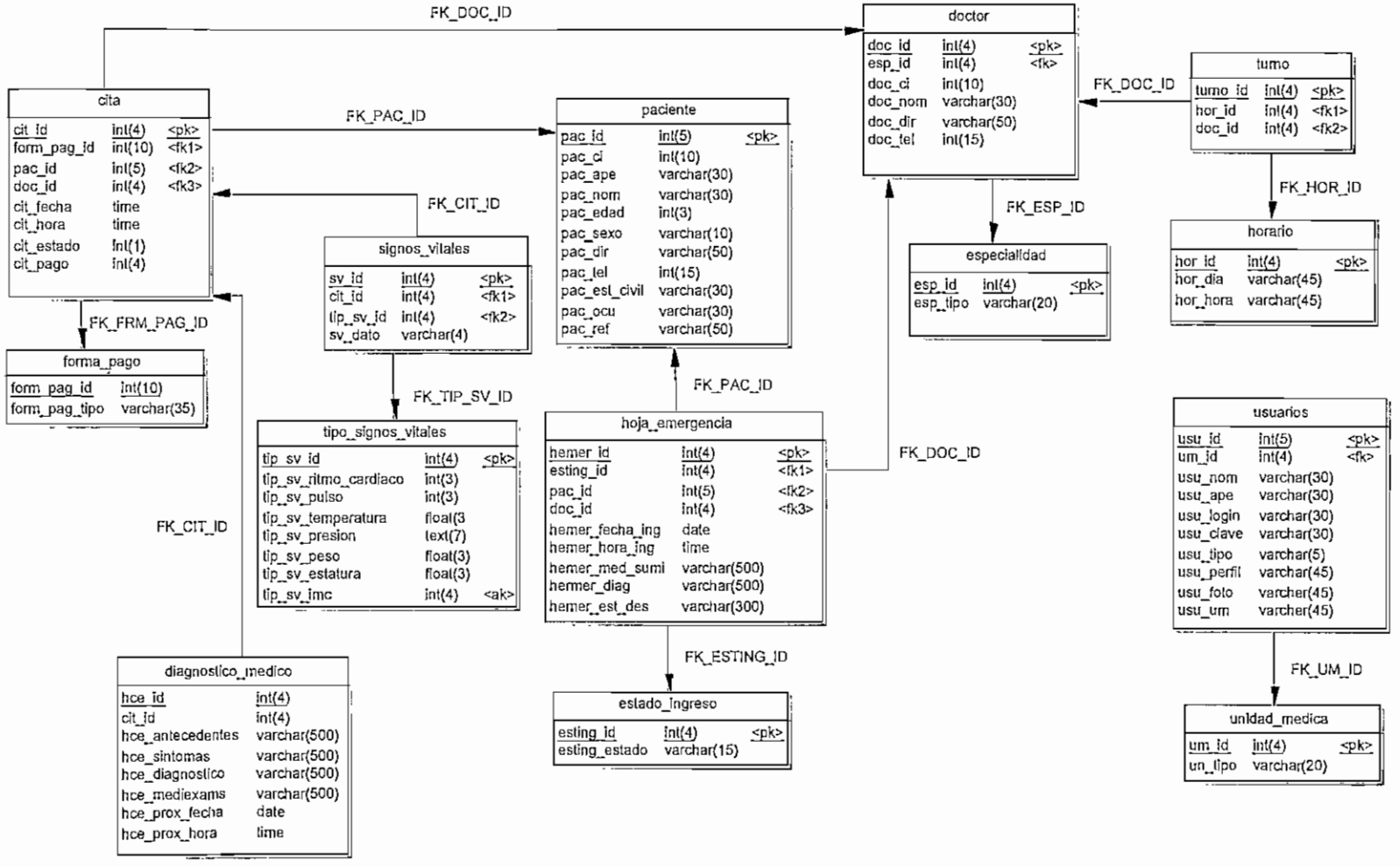



Figura 3.42 Modelo Físico Relacional

# 3.5 INTERCONEXIÓN DE LA BASE DE DATOS CON EL INTERFAZ GRÁFICO

La capacidad para acceder a bases de datos desde Java la ofrece API *JDBC (Java DataBase Conectivity)*. JDBC es un estándar para manejar bases de datos en Java. ODBC es un estándar de Windows para manejar bases de datos, tal que cualquier programa en Windows que desee acceder a bases de datos genéricas debe usar este estándar.

La necesidad de crear un estándar propio para acceder a bases de datos desde Java se explica porque el estándar ODBC está programado en C y un programa que use este estándar, depende de la plataforma. Para solventar este problema las empresas realizan *drivers* que traducen el ODBC a JDBC.

## 3.5.1 Herramientas de Desarrollo

### 3.5.1.1 Detalle de las Herramientas

| Herramienta | Nombre | Descripción |
|---|---|---|
| Base de Datos | MySql 5.0 | - Servidor Robusto<br>- Servicio de Transferencia de Datos (DTS )<br>- Duplicación de cualquier BDD.<br>- Licencia Gratuita. |
| Lenguaje de Programación | NetBeans 5.0 (Java) | - Trabaja con lenguajes y protocolos de estándares abiertos.<br>- Multiplataforma.<br>- Licencia Gratuita.<br>- Previo a su instalación requiere de la Máquina Virtual de Java 1.5.0.7<br>- Paquete *javax.com* para la comunicación serial con el sensor |

**Tabla 3.18 Herramientas de Desarrollo**

## 3.5.2 Estándares de Programación

| Tipo | Estándar |
|---|---|
| Variable Local | vl_tipodatoNombre |
| Variable Global | vg_tipodatoNombre |
| Función Local | Funcion_Nombre |
| Formulario | Frm_Nombre |
| Clase | ClassNombre |
| Servicios | Frm_NombreFormulario_Nombre |

**Tabla 3.19 Estándares de Programación**

### 3.5.3 Pasos para Realizar la Interconexión

El *driver* más adecuado para la realización de este proyecto, es un puente JDBC-ODBC, ya que se desea ejecutar la aplicación en una red hibrida y el *driver* de *Mysql* para Java *Conector/J* utiliza para su interconexión un puerto físico, lo que ocasiona que las estaciones inalámbricas no puedan comunicarse con el servidor de base de datos.

#### 3.5.3.1 Requisitos previos

Lo primero que se tiene que hacer es disponer de la configuración apropiada, para elaborar la interconexión, esto incluye los siguientes pasos:

- Instalar el *driver* para JDBC: el *driver* "puente JDBC-ODBC" viene incluido en las versiones Solaris o Windows de JDK 1.1 en adelante.
- Instalar el Controlador de Base de Datos de *MySql*: si no se tiene instalado el controlador de base de datos, es necesario descargarlo de la página Web oficial de *MySql*, para este proyecto se ha empleado el controlador "MyODBC-3.51.11-1-win".

#### 3.5.3.2 Selección de la Base de Datos

Previo a realizar la selección de la Base de Datos a emplear para la interconexión con el interfaz gráfico, se asume que esta ya esta creada y se llama **tesis**.

#### 3.5.3.3 Establecimiento de la Conexión

Para establecer una conexión con el controlador de base de datos a emplear se deben realizar dos pasos: primero cargar el *driver* y segundo, hacer la conexión.

##### *3.5.3.3.1 Importar Clases para Hacerlas Visibles*

Previo a elaborar cualquier interconexión se debe importar los paquetes o clases que se van a utilizar en la nueva clase.

Todas las clases generalmente utilizan el paquete *java.sql* (API JDBC), que se hace visible cuando la siguiente línea de código precede a la definición de clase.

*import java.sql.*;*

El asterisco (*) indica que todas las clases del paquete *java.sql* serán importadas. Importar una clase la hace visible y significa que no se debe escribir su nombre totalmente cualificado cuando se utilice un método o un campo de esa clase.

### *3.5.3.3.2 Configuración del Puente JDBC-ODBC*

Para elaborar el interfaz gráfico, se empleó NetBeans IDE 5.0 de Java, esta plataforma permite elaborar BDD o trabajar con una ya hecha en cualquier motor de bases de datos. Para el sistema diseñado, se ha decidido utilizar la BDD realizada en *MySql*, e implementar la interconexión mediante el puente JDBC-ODBC.

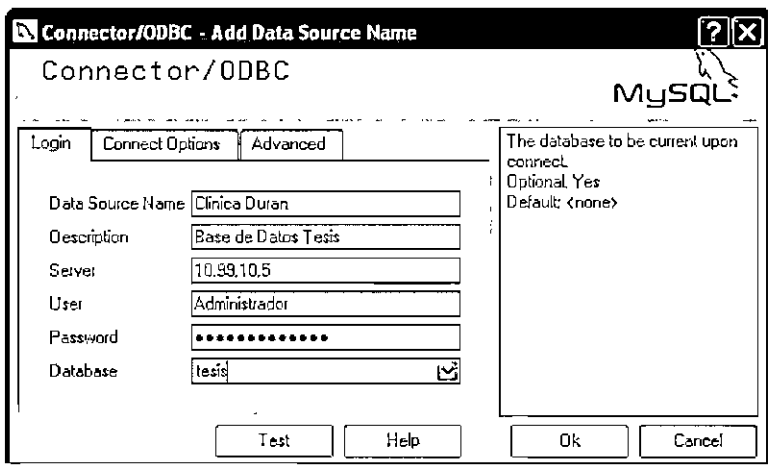



**Figura 3.43 Configuración del puente JDBC- ODBC**

### *3.5.3.3.3 Cargar los Drivers*

Para emplear la conexión establecida en el paso anterior, se debe cargar el driver mediante el siguiente fragmento de código:

```
String cn="sun.jdbc.odbc.JdbcOdbcDriver";
    try{
        Class.forName(cn);
        ...
    }catch(Exception e){}
```

La documentación del *driver* da el nombre de la clase a utilizar. En este caso el nombre de la clase es **jdbc.OdbcDriver**, se carga el *driver* con esa cadena.

No se necesita crear un ejemplar de un *driver* y registrarlo con el ***DriverManager*** porque la llamada a ***Class.forName*** lo hace automáticamente.

Una vez cargado el *driver*, es posible hacer una conexión con un controlador de base de datos.

*3.5.3.3.4 Hacer la Conexión*

El segundo paso para establecer una conexión es contar con el *driver* apropiado conectado al controlador de base de datos. La siguiente línea de código ilustra la idea general.

```
Connection con=null;
con = DriverManager.getConnection(url, "myLogin", "myPassword");
```

Debido a que se esta utilizando el puente JDBC-ODBC, el JDBC URL empezará con *jdbc:odbc:*, el resto de la URL es el nombre de la fuente de datos en el ODBC (clínica).

En lugar de "*myLogin*" se coloca el nombre utilizado para entrar en el controlador de la base de datos; y en lugar de "*myPassword*" se define la clave de acceso para el controlador de la base de datos. Para el presente sistema, el usuario es "Administrador" y la clave es "admin", con lo cual queda establecida la conexión.

El párrafo de código final para el sistema elaborado es:

```
try{
        Class.forName(cn);
        con= DriverManager.getConnection(
           "jdbc:odbc:Clinica Duran","Administrador","admin");
        System.out.println("conectado");
    }catch(Exception e){
        JOptionPane.showMessageDialog(null,e.getMessage(),"ALERTA!...",1);
    }
```

La clase *DriverManager*, maneja todos los detalles del establecimiento de la conexión detrás de la escena. La conexión devuelta por el método *DriverManager.getConnection* es una conexión abierta que se puede utilizar para crear sentencias JDBC que pasen las sentencias SQL del sistema, al controlador de la base de datos.

# CAPÍTULO 4

# IMPLEMENTACIÓN DEL PROTOTIPO DE PRUEBA Y COSTOS DE IMPLEMENTACIÓN

# 4. IMPLEMENTACIÓN DEL PROTOTIPO DE PRUEBA Y COSTOS DE IMPLEMENTACIÓN

El prototipo de prueba de este proyecto, busca mostrar un breve ejemplo de la utilización de la tecnología inalámbrica en la medicina, y a la vez abrir una ventana en este campo, para aprovechar adecuadamente los avances tecnológicos que se ofrecen actualmente.

## 4.1 DESCRIPCIÓN DEL PROTOTIPO DE PRUEBA

El prototipo de prueba a realizar incluye los siguientes elementos:

- Una red de prueba, para el área de Consulta Externa de la Clínica "Durán", constituida por dos partes: la red inalámbrica y la red de Sensores.
- Un sensor de pulso y ritmo cardiaco tipo *Bluetooth*.
- Un receptor *Bluetooth*.
- Y una aplicación para Consulta Externa, Emergencia y Ambulancia de la Clínica "Durán.

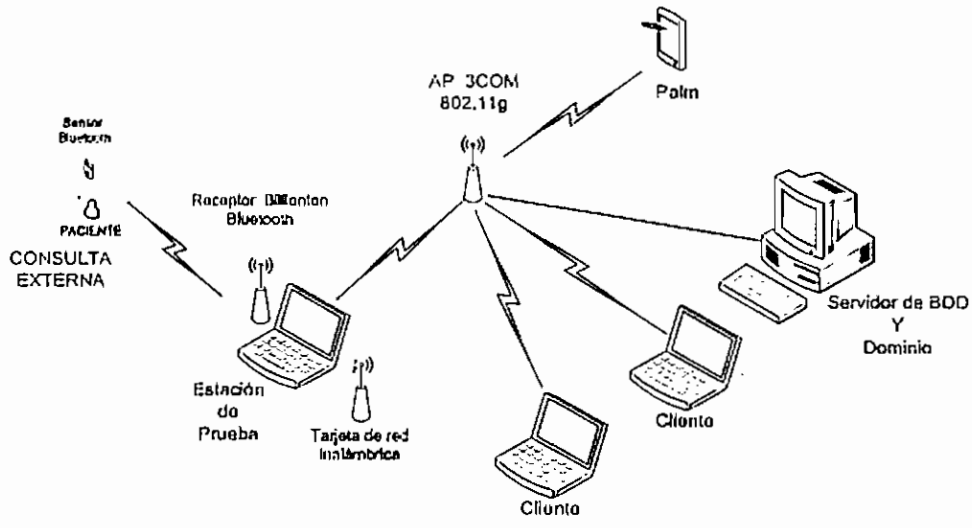



Figura 4.1 Diagrama del Prototipo de Prueba

Adicionalmente se incluyen mecanismos de seguridad tanto para la aplicación como para la red, para garantizar un nivel adecuado de seguridad de la información.

### 4.1.1 RED DE PRUEBA

La red de prueba es de tipo inalámbrica, y trabaja bajo el estándar IEEE 802.11g, sus elementos son: un *Access Point*, cuatro estaciones de trabajo, y una computadora de mano (PALM, PDA).

Una de las estaciones de trabajo ha sido configurada como Equipo Servidor, la cual dispone del sistema operativo *Windows 2003 Server*, de un Dominio llamado ClinicaDuran.com y motor de base de datos *MySQL Server* 5.0. En el dominio, se han creado cuentas con privilegios de Administrador y de Usuario simple, considerando que únicamente las primeras, pueden modificar la información de la Base de Datos y de configuración de recursos compartidos.

El resto de estaciones de trabajo, cuentan con el sistema operativo *Windows XP SP2*; las cuales están debidamente autenticadas en el dominio mencionado, al igual que la PALM. Cabe mencionar que en la estación de trabajo JADYTA, se encuentra una carpeta compartida para el almacenamiento de los datos obtenidos por el sensor, configurada con permisos de lectura, escritura, y control total, por usuario, ya que en este equipo se encuentra conectado el receptor *Bluetooth* al cual llegarán los datos de medición del sensor.

El equipo de interconectividad a emplear es marca *3COM OfficeConnect Wireless 108 Mbps 11g PoE*, indicado previamente[1], el cual se lo ubica en Consulta Externa de la clínica, por ser el sitio elegido para la implementación del prototipo.

Las 3 estaciones de trabajo, que funcionan como clientes de la red inalámbrica, disponen de diversos tipos de tarjetas de red inalámbricas, que soportan IEEE 802.11g con velocidades de hasta 54 Mbps, mientras que el equipo servidor se encuentra conectado directamente al Punto de Acceso, a través del puerto *Ethernet*.

---

[1] Véase Capítulo 2.5.2. Equipos de la Red Inalámbrica.

### 4.1.2 RED DE SENSORES

La red de sensores es de tipo PAN, trabaja bajo el estándar IEEE 802.15.1, e incluye un dispositivo central de interconectividad y como elementos de la misma a los sensores.

El equipo central o de control es un receptor *Bluetooth* marca *BlueSoleil 1.4.9.5*, el cual dispone de la implementación completa de la pila del protocolo *Bluetooth*, y permite garantizar seguridad en la red PAN.

Se utiliza un Pulso-Oxímetro (sensor de pulso y sensor de ritmo cardiaco en uno), marca *NONIN AVANT 4100*, ya que es el único existente en el mercado que dispone del estándar IEEE 802.15.1 *Bluetooth*.

Para el Pulso-Oxímetro se ha seleccionado el formato de transmisión de datos 2[2], el cual dispone de 5 bytes y es el recomendado por el fabricante en caso de elaboración de aplicaciones independientes.

### 4.1.3 APLICACIÓN

Se elabora una aplicación denominada JK INC en *NetBeans 5.0* de Java, siguiendo el Proceso Unificado de Desarrollo de Software descrito en el capítulo 3. La aplicación realizada, podrá ser utilizada en Consulta Externa, Emergencia y Ambulancia de la Clínica "Durán".

La aplicación se interconecta con una Base de Datos, realizada en *MySql 5.0* considerando una tasa muestral de 20 pacientes. Dicha base de datos, dispone de 2 cuentas creadas por las administradoras, para acceder a ella y así evitar ataques que puedan perjudicar la seguridad de la información almacenada.

Como mecanismo de seguridad se empleará autenticación mediante usuario y contraseña con un máximo de tres intentos, considerando como usuarios permitidos: al personal médico de la clínica y al administrador de la aplicación.

---

[2] Véase Capítulo 2.5.3. Equipos y Elementos de la Red de Sensores

## 4.2 CONFIGURACIÓN DE EQUIPOS

Acorde al desarrollo del prototipo, es necesario configurar los equipos en el siguiente orden: AP, tarjetas de red, y receptor *Bluetooth*.

### 4.2.1 CONFIGURACIÓN DEL PUNTO DE ACCESO

El Punto de Acceso seleccionado para el desarrollo de este proyecto, incluye diversas características de configuración, entre las cuales se destacan: Control de Acceso, Perfiles de Seguridad, Sistema, Parámetros *Wireless*, y Administración.

Inicialmente el AP dispone de la configuración de fábrica, la cual por seguridad de la red, debe ser cambiada. Para ello se accede a la configuración del Punto de Acceso a través del navegador, con la dirección IP dada por el fabricante, se elige la opción *System* y se ingresan los parámetros requeridos (nombre del punto de acceso, descripción, país, dirección IP, entre otros), como se muestra en la Figura 4.1.

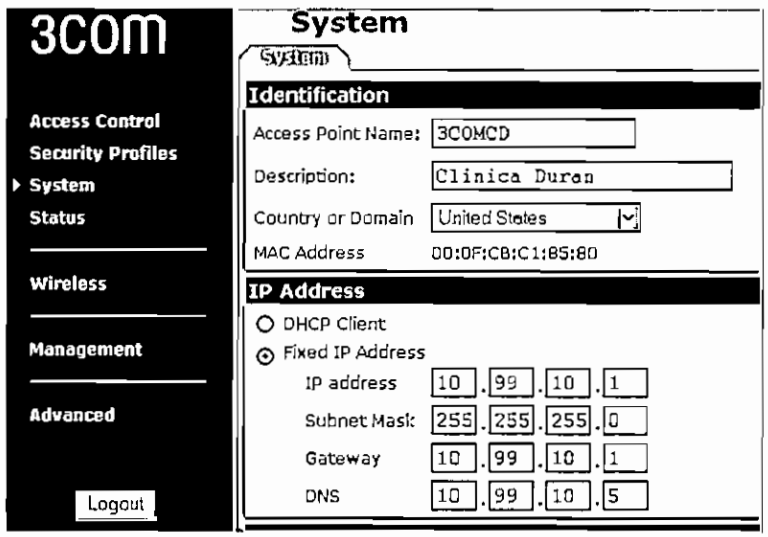



Figura 4.1 Configuración General del AP para el Prototipo

Es importante definir un nombre de usuario y *password* adecuados para acceder a la configuración del AP, los cuales son proporcionados únicamente para los administradores de la red del prototipo por seguridad. Para determinar estos

parámetros, se elige la opción *Management*, y se ingresan los datos necesarios, como se muestra a continuación:

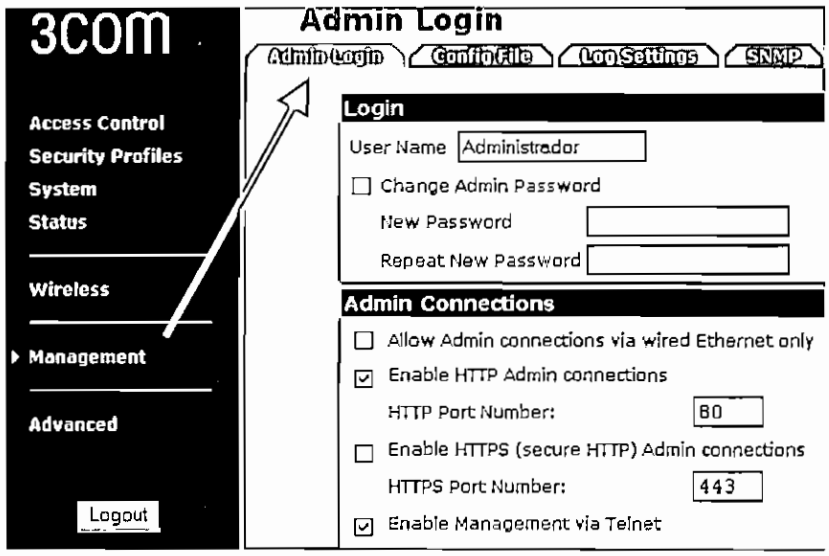



Figura 4.2 Configuración de Administrador

Lo primero a realizar para implementar la red inalámbrica, es la creación de un Perfil de Seguridad, mediante el cual los usuarios de la clínica accederán a la misma. Para visualizar los perfiles del AP, se accede a la opción *Status*, y luego a la pestaña *Profiles*, como se muestra en la figura.

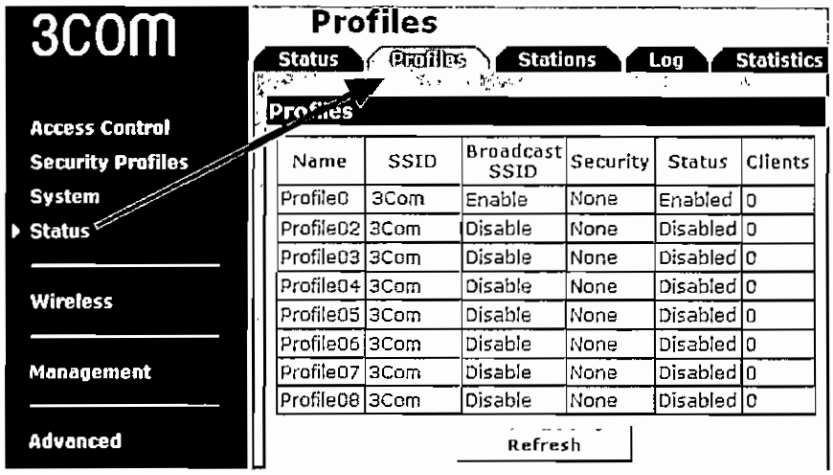



Figura 4.3 Perfiles del Punto de Acceso

Ahora, se procede a crear el perfil, accediendo a la opción *Security Profiles*, en la cual aparece la siguiente pantalla:

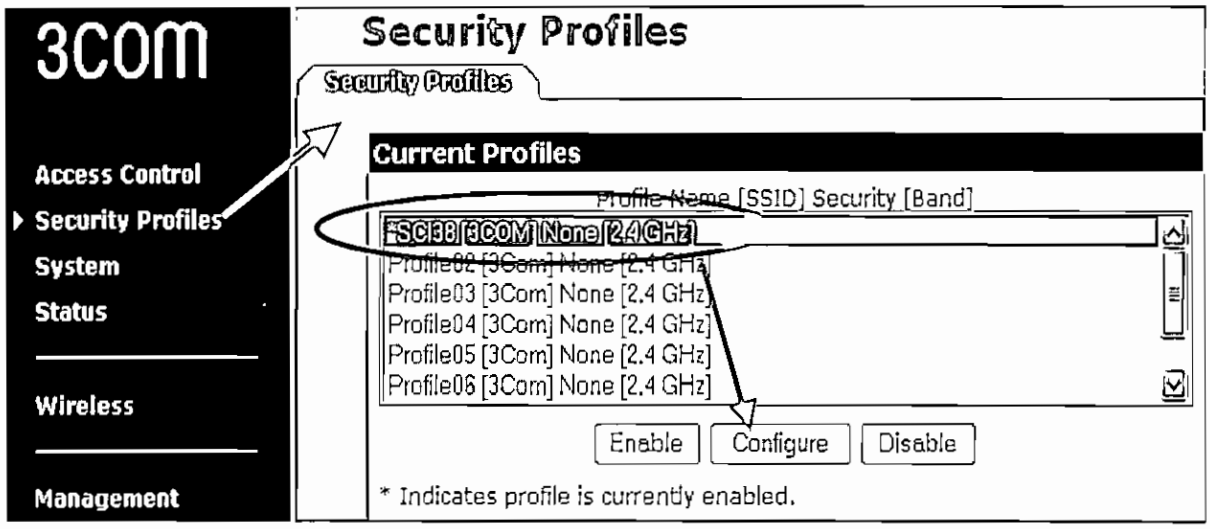



Figura 4.4 Perfiles del AP

Entonces se selecciona un perfil vacío, y se oprime el botón *Configure*, mostrando la Figura 4.5.

El perfil recibe el nombre de "JK INC", e incluye como SSID[3] jkinc5457. Adicionalmente se configuran los parámetros de seguridad, como se explica más adelante.

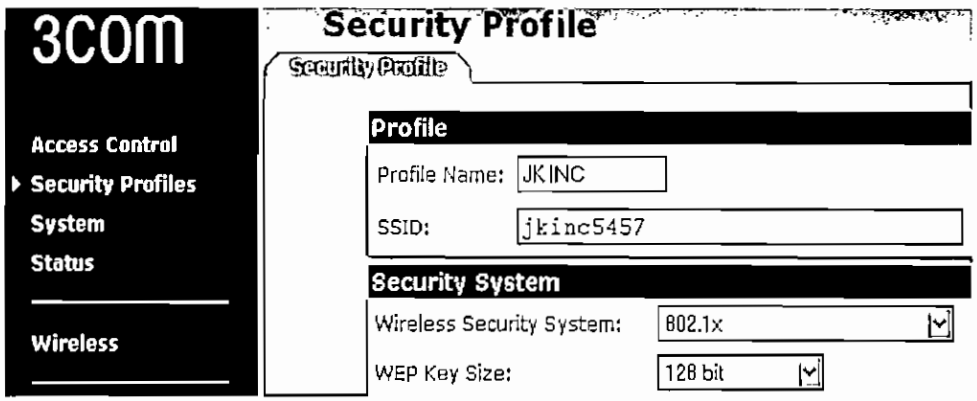



Figura 4.5 Configuración de Perfil "JK INC" para el Prototipo

Finalmente se definen los parámetros propios de trabajo de la red inalámbrica, mediante la opción *Wireless*. Para el prototipo, se debe emplear IEEE 802.11b e IEEE 802.11g, ya que la PALM/PDA trabaja con el primero.

[3] Identificador del Conjunto de Servicios

Se escoge "*Access Point*" como modo de trabajo del equipo, y se define el modo Broadcast SSID, como se muestra en la siguiente Figura 4.6.

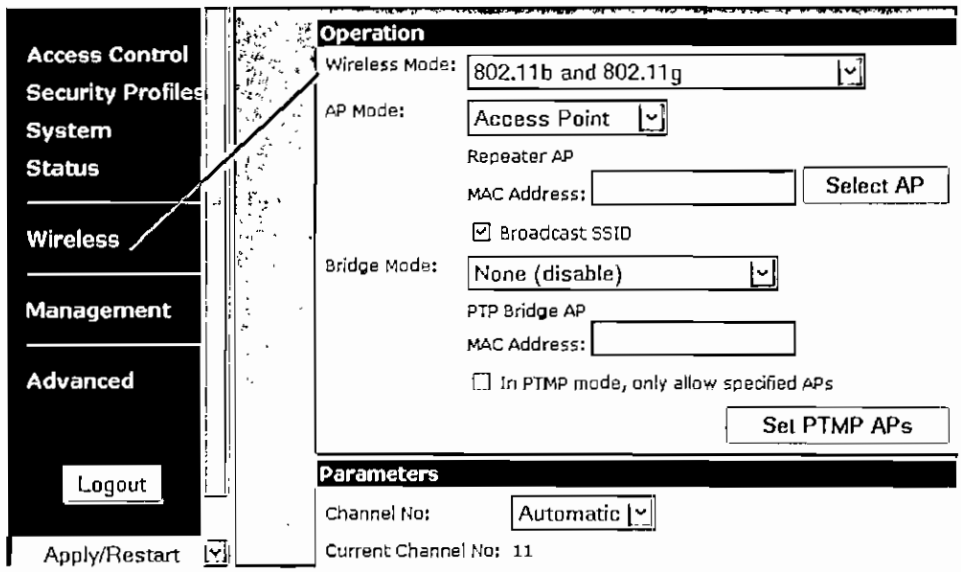



**Figura 4.6 Configuración de Parámetros de la Red Inalámbrica**

Con lo cual el Punto de Acceso queda configurado acorde a las necesidades del prototipo planteado, faltando únicamente los parámetros de seguridad a ser configurados más adelante.

### 4.2.2 CONFIGURACIÓN DE LAS TARJETAS DE RED

Las tarjetas de red de las estaciones de trabajo deben ser configuradas con: una dirección IP, una máscara de red y un *Gateway*. Además, se debe seleccionar el protocolo de encripción que se está manejando para la seguridad, como se efectuará más adelante.

Se tienen disponibles 252 direcciones IP para acceder a la red, esta asignación debe ser configurada en el AP, como se muestra en la Figura 4.7, el rango establecido va desde la dirección IP: 10.99.10.1 hasta 10.99.10.254, excepto la dirección IP 10.99.10.1 utilizada para el equipo *Acces Point* y la dirección 10.99.10.5 utilizada para el equipo Servidor.

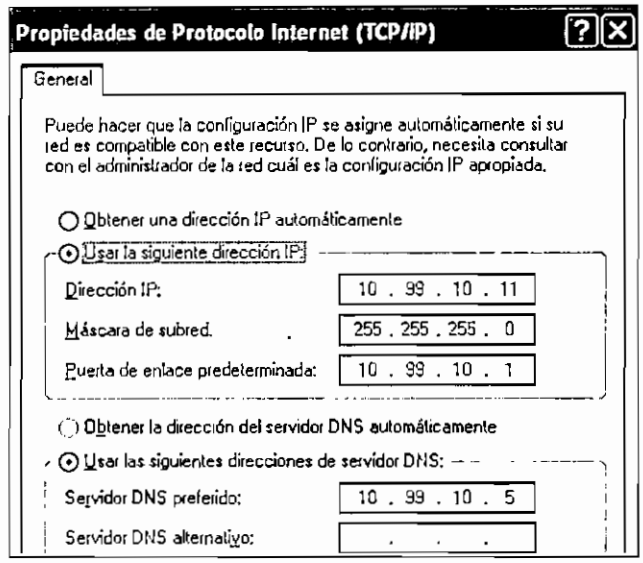



Figura 4.7 Configuración de las tarjetas de red

Adicionalmente, se incluye la configuración de la PALM, en la que, se accede a la aplicación *WiFiLT* para establecer los parámetros TCP/IP, y los correspondientes a la red inalámbrica acorde a lo establecido en el Punto de Acceso.

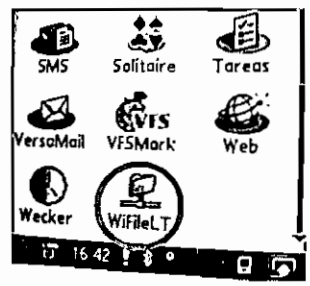



Figura 4.8 Aplicación para la configuración inalámbrica en la PALM

Luego se selecciona la red inalámbrica creada anteriormente en el AP, y se elige la opción Editar – Configurar, como se muestra en la siguiente figura.

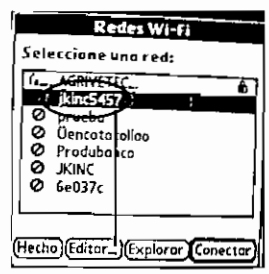



Figura 4.9 Selección de la red inalámbrica a conectarse a través de la PALM

Seguidamente se ingresa el SSID de la red, y el mecanismo de seguridad a emplear para acceder a la misma.


Figura 4.10 Selección de la red a configurar en la PALM

Luego se define el modo de conexión de la PALM, que para el presente caso es mediante el Punto de Acceso (Infraestructura), a través del botón **Detalles** mostrado en la Figura 4.11.


Figura 4.11 Modo de trabajo de la PALM para acceder a la red inalámbrica

Con lo cual se procede a ingresar los parámetros TCP/IP, mediante la opción **Avanzadas**, como se muestra en la Figura 4.12.


Figura 4.12 Configuración de los Parámetros TCP/IP en la PALM

### 4.2.3 CONFIGURACIÓN RECEPTOR *BLUETOOTH*

*Billionton*, es un dispositivo *Bluetooth*, que permite a los ordenadores de escritorio o portátiles *Bluetooth*® conectarse directamente y de forma inalámbrica a otros dispositivos *Bluetooth*. Además permite crear redes e intercambiar datos con otros ordenadores o PDA *Bluetooth*. Este dispositivo es manejado por el Software *BlueSoleil*, que trabaja en plataformas Windows 98SE/ME, y Windows 2000/XP.

Para conectar y compartir servicios mediante la tecnología inalámbrica *Bluetooth*, dos dispositivos deben admitir el mismo perfil *Bluetooth* y asumir funciones de dispositivo opuestas (maestro/esclavo). Para el caso del prototipo a implementar, la topología de red a utilizarse, es tipo estrella, donde *Billionton* es el dispositivo Maestro, y el equipo de medición de pulso y ritmo cardíaco *4100 AVANT NONIN*, es Esclavo.

#### 4.2.3.1 Configuración de Hardware

El software *BlueSoleil* admite los siguientes tipos de adaptadores: USB y tarjeta *CompactFlash* (UART o BCSP). Para este proyecto se utiliza el adaptador *Bluetooth* USB, el cual se establece en el menú Herramientas/Mi dispositivo *Bluetooth*.

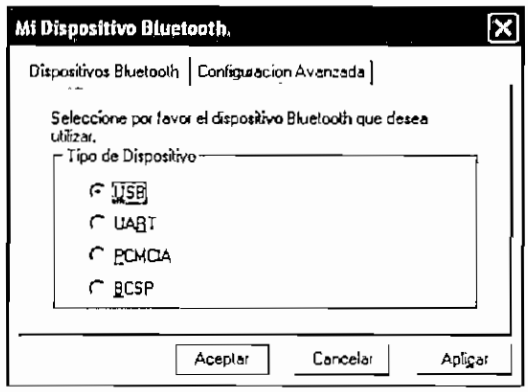



Figura 4.13 Selección Dispositivo *Bluetooth*

#### 4.2.3.2 Configuración de Propiedades

Para configurar las propiedades del dispositivo local, se hace clic en Mi *Bluetooth*/ Propiedades de dispositivo.

La configuración general se realiza según la Figura 4.14

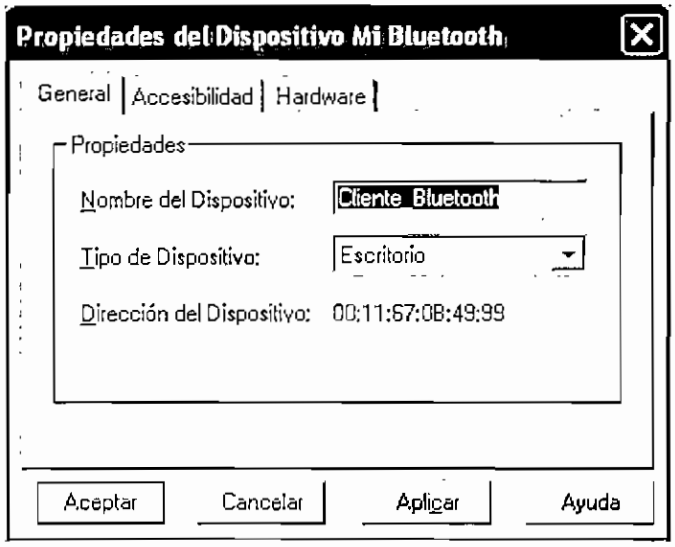



**Figura 4.14 Página de Propiedades Generales**

*4.2.3.2.1 Accesibilidad*

Permite determinar el Modo de conexión, de detección y de asociación (vinculación) de los dispositivos.

- Conectable: Permite a dispositivos *Bluetooth* conectar con su equipo.
- No Conectable: Prohíbe a dispositivos *Bluetooth* conectarse con su equipo.
- Detección general: Permite que otros dispositivos *Bluetooth* detecten a su equipo.
- Detección limitada: Permite que otros dispositivos *Bluetooth* detecten a su equipo con una Solicitud limitada.
- No detectable: Prohíbe que otros dispositivos *Bluetooth* detecten a su equipo.
- Acepta vinculación: Permite que otros dispositivos *Bluetooth* se asocien con su equipo. Si el otro dispositivo inicia un procedimiento de asociación con su equipo, cada dispositivo debe introducir la misma contraseña antes de poder completar el proceso.
- No acepta vinculación: Rechaza todos los intentos de asociación iniciados por otros dispositivos *Bluetooth*.


Figura 4.15 Página de Propiedades de Accesibilidad

### 4.2.3.3 Configuración de la Seguridad de Servicios Locales

Para acceder a la pantalla de configuración de seguridad de servicios locales, se ingresa en Mi *Bluetooth* / Seguridad y luego se escoge la opción de Servicios.

#### *4.2.3.3.1 Servicios Locales*

- **Autenticación**: Esta opción requerirá una contraseña cada vez que un dispositivo remoto intente conectar con este servicio.
- **Cifrado**: En esta opción, los datos transmitidos entre los dispositivos con este servicio se cifrarán.

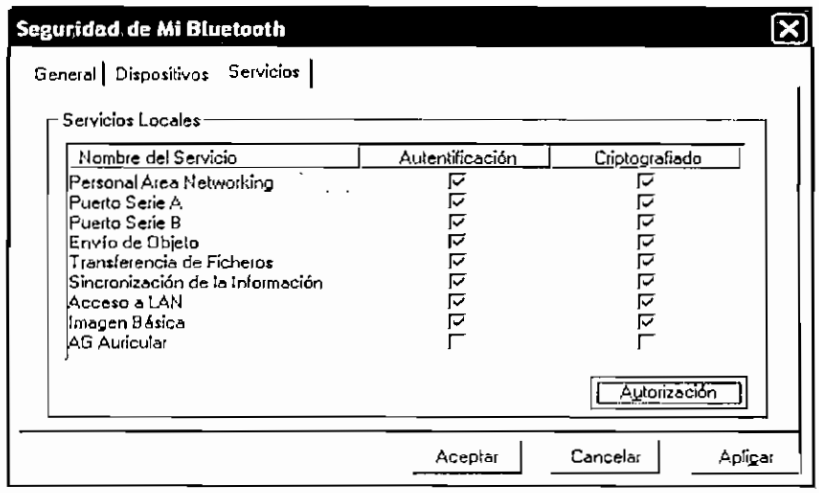



Figura 4.16 Seguridad *Bluetooth*

En la pantalla **Autorización de servicio** aparecen las siguientes opciones de configuración:

- **Dispositivos de confianza:** Seleccione si se desea confiar en los dispositivos de esta pantalla para utilizar el servicio seleccionado de su dispositivo. Cuando se confía en un dispositivo, este puede acceder al servicio libremente. Haga clic en **Añadir/Eliminar** para editar la lista de dispositivos.
- **Confiar en todos los dispositivos**: Se aceptarán las solicitudes de conexión de todos los dispositivos.
- **Preguntar al usuario si no se trata de un dispositivo de confianza para este servicio**: Si un dispositivo que no es de confianza intenta acceder al servicio, aparecerá un cuadro de diálogo que le permitirá acceder o rechazar la conexión.
- **Rechazar el dispositivo si no se trata de un dispositivo de confianza para este dispositivo:** Si un dispositivo que no es de confianza intenta acceder al servicio, la conexión se rechazará automáticamente sin informar al usuario.

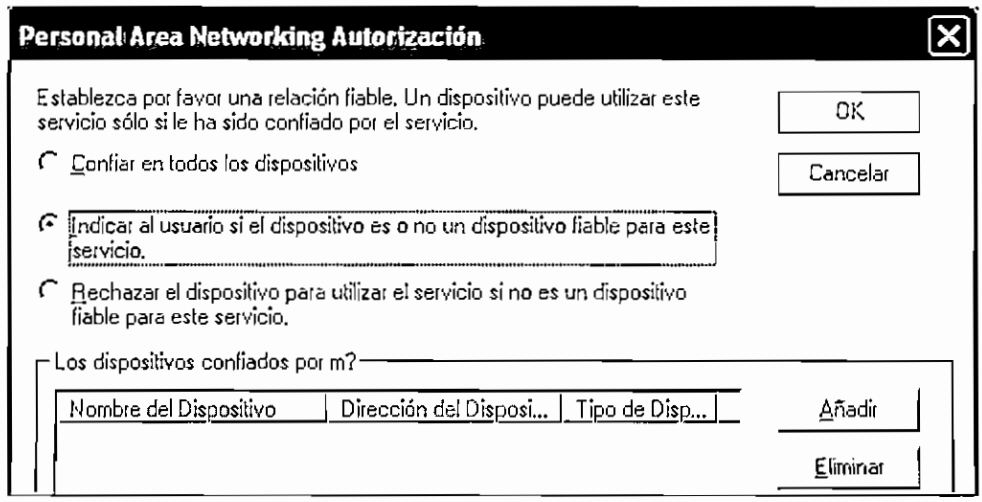



**Figura 4.17 Tipos de Acceso a la Red *Bluetooth***

Se agrega el dispositivo con el cual se realizará la conexión y se interactuará (4100 AVANT NONIN), para que éste sea asignado como un dispositivo de confianza.

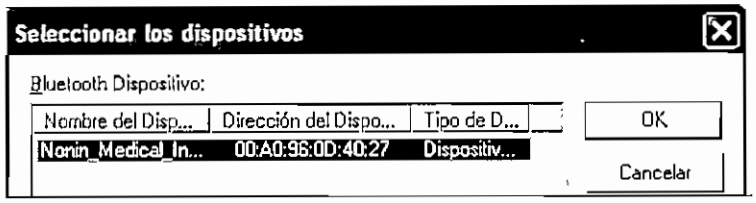



Figura 4.18 Agregación del Pulso-Oxímetro *Bluetooth* como Dispositivo de Confianza

#### *4.2.3.3.2 Dispositivos*

Para realizar la autorización de servicios locales que se desea tener para este dispositivo, se selecciona el equipo NONIN en Dispositivos de Seguridad de Mi *Bluetooth*.

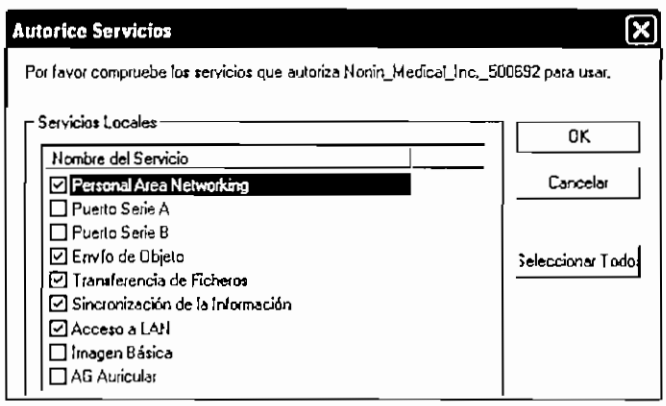



Figura 4.19 Autorización de Servicios para NONIN AVANT 4100

#### *4.2.3.3.3 General*

En la sección General de Seguridad, se establece el nivel de seguridad para las conexiones de entre tres niveles:

- **Bajo** (Modo de seguridad 1, Sin seguridad): No es necesario ningún procedimiento de seguridad para las conexiones.
- **Medio** (Modo de seguridad 2, seguridad de nivel servicio): Se solicita Autenticación *o* Autorización cuando un servicio específico es accedido por otro dispositivo *Bluetooth*. Si dos dispositivos están conectando por primera vez, o bien, si dos dispositivos no tienen una relación de confianza, debe proporcionarse la misma contraseña en ambas partes para completar la

autenticación. Este modo le permite asignar diferentes derechos de acceso para cada servicio admitido por el servidor.

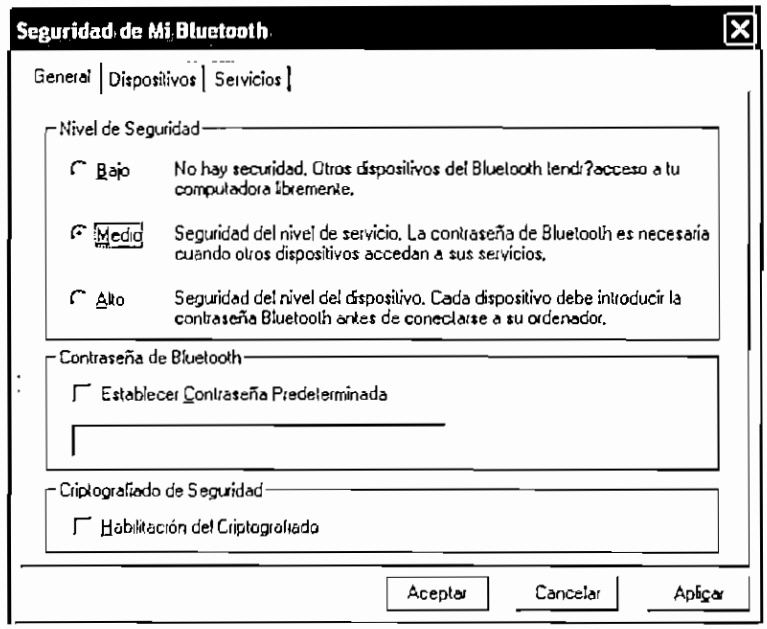



**Figura 4.20 Nivel de Seguridad en las Conexiones**

- **Alto** (Modo de seguridad 3, Seguridad de nivel vínculo): Si cualquiera de los dos dispositivos aplica el modo de seguridad 3, la autenticación se solicitará cada vez que se inicie una conexión entre dos dispositivos *Bluetooth*. Para completar la autenticación es necesario proporcionar en ambas partes la misma contraseña.

***Nota:*** *En el modo de seguridad 2, el usuario puede añadir cada dispositivo autenticado en una lista de dispositivos de confianza para acelerar conexiones futuras.*

En el caso de este proyecto se requiere tener una conexión establecida, luego de realizar una relación de confianza con una sola autenticación inicial, para lo cual se ha elegido el Nivel de Seguridad: Medio.

#### 4.2.3.4 Establecimiento de una Conexión *Bluetooth*

La conexión se inicia, por lo general, desde el cliente.

En la ventana principal:

1. Se hace clic en Mi dispositivo (globo central), para buscar los dispositivos *Bluetooth* dentro del ámbito de funcionamiento.

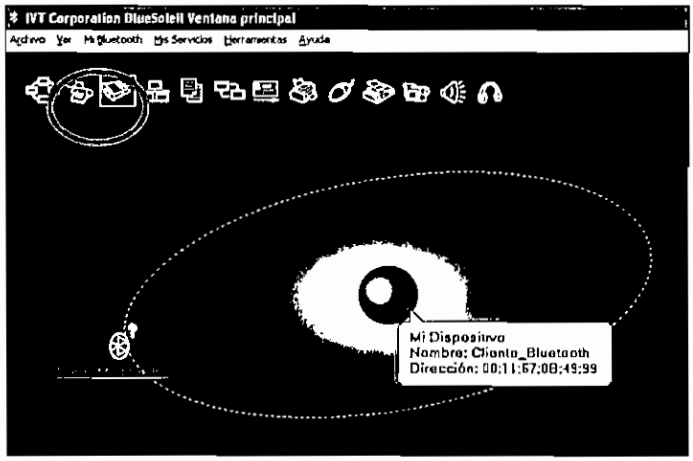



Figura 4.21 Pantalla Inicial de Establecimiento de Conexión

2. Se busca el dispositivo *Bluetooth,* en caso de existir algunos, haciendo doble clic en el icono del dispositivo (4100 AVANT NONIN). El botón del servicio situado en la parte superior de la ventana principal de *BlueSoleil* se resaltará si el dispositivo admite el servicio. Si es necesario emparejar los dispositivos, se debe introducir la misma contraseña *Bluetooth* en ambos equipos. Para este caso se debe introducir la clave incluida en el equipo.

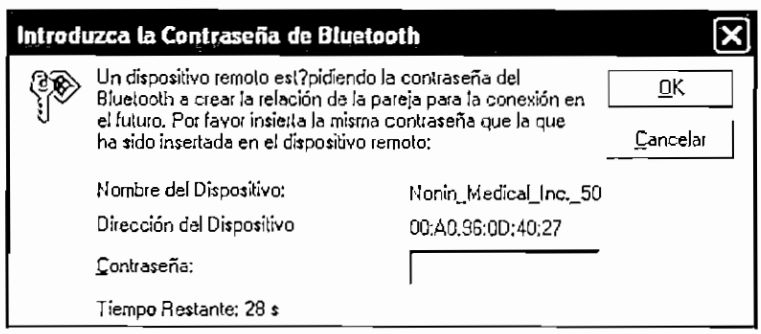



Figura 4.22 Autenticación del Dispositivo Esclavo

3. Conexión: Se da un clic derecho en el dispositivo encontrado y se escoge la opción de Conectar/Servicio de Puerto Serie *Bluetooth*, con lo cual se ha establecido la conexión entre los dispositivos (*Billionton* y NONIN).

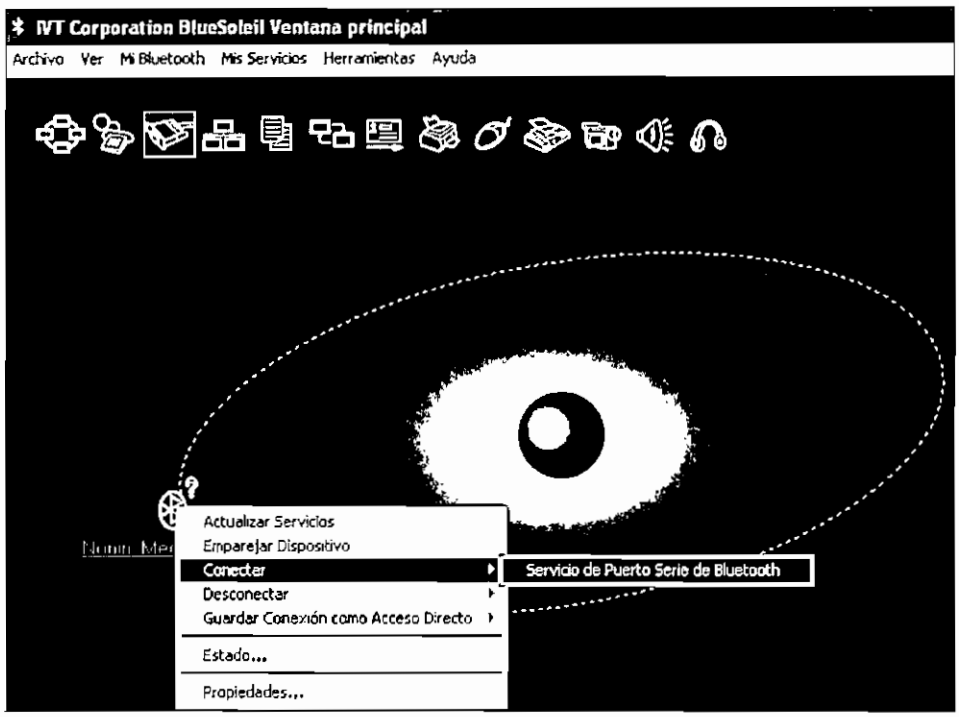



Figura 4.23 Conexión del Sensor con el Dispositivo de Interconectividad

Una vez establecida la conexión, estos datos se guardan en la memoria del software *BlueSoleil*, para acceder de manera más rápida la próxima vez que localice al dispositivo

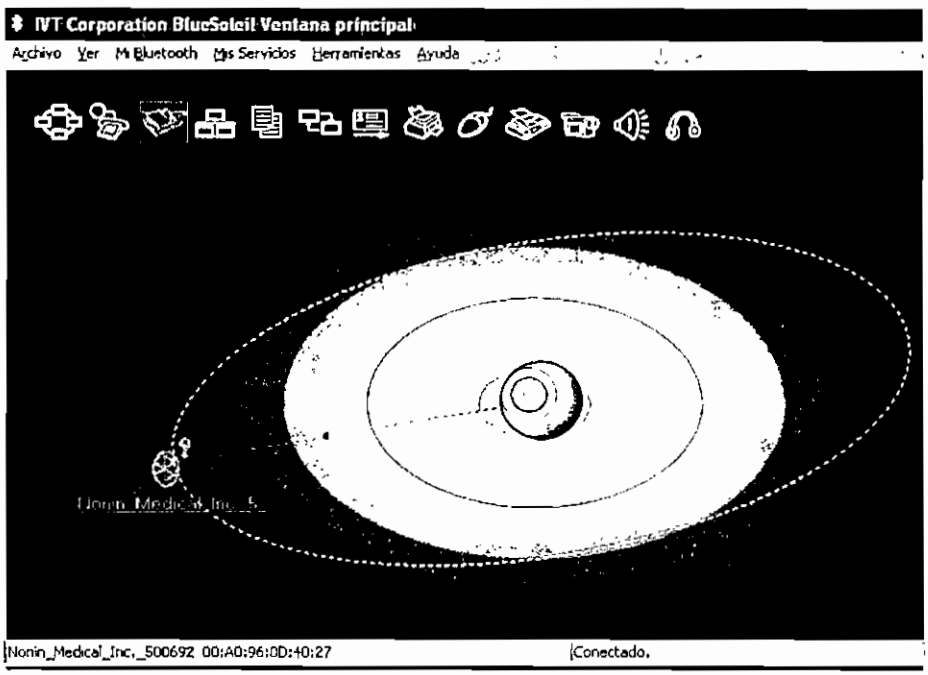



Figura 4.24 Sensor y Dispositivo Maestro Interconectados

Para observar el estado de la conexión, se hace clic derecho en el dispositivo NONIN, y se escoge la opción Propiedades.

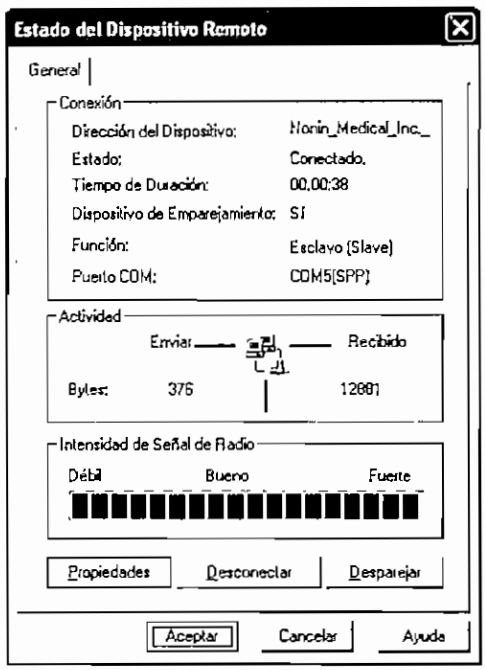



Figura 4.25 Propiedades de la Conexión Sensor - Dispositivo Maestro

Con lo cual se puede verificar que existe una conexión entre los dispositivos y sus características. Así queda establecida la conexión de los dispositivos *Bluetooth* a utilizarse en el prototipo.

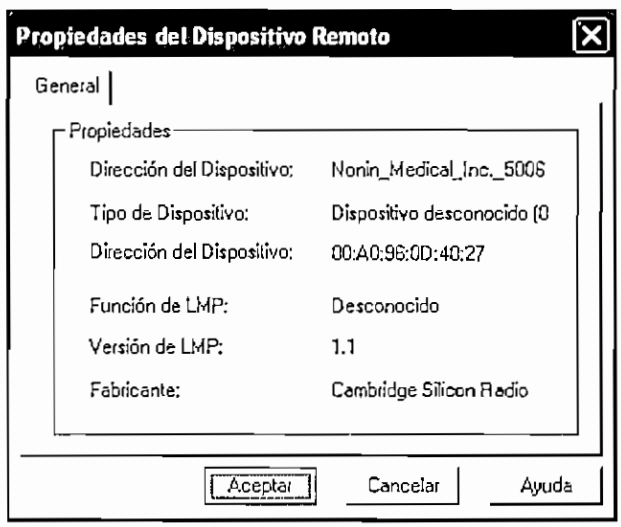



Figura 4.26 Propiedades del Dispositivo Remoto (Sensor NONIN)

## 4.3 CONFIGURACIÓN DE SEGURIDADES

Para la implementación de la seguridad del prototipo, se considera a la red inalámbrica y a la aplicación desarrollada que ha sido llamada "JK INC".

La aplicación, incluye un mecanismo de seguridad básico llamado autenticación, el cual permite al sistema identificar si un usuario es permitido para acceder al mismo, y en base a ello determinar cual es su perfil de trabajo.

Las configuraciones de los mecanismos de seguridad para la red de prueba, incluyen: filtrado MAC, WEP y Autenticación por medio de un servidor *RADIUS*, las mismas que serán configuradas en el equipo de interconectividad y en el servidor respectivamente.

### 4.3.1 SEGURIDAD DE LA APLICACIÓN

En la siguiente pantalla se muestra la ventana principal de acceso al sistema elaborado, la cual incluye un *login* y *password* facilitado por el administrador de la red.


Figura 4.27 Pantalla de Acceso a JK INC

Los usuarios admitidos para acceder a JK INC, están almacenado en la Base de Datos (BDD) del sistema, y en caso de requerir un nuevo usuario, éste debe ser agregado manualmente por el Administrador.

### 4.3.2 SEGURIDAD DE LA RED DE PRUEBA

La seguridad de la red de prueba, se garantiza con la seguridad de la red inalámbrica, ya que el equipo empleado para la red de sensores incluye la pila del

protocolo *Bluetooth* completa, asegurando el funcionamiento de la misma y sus datos. Cabe notar que el dispositivo *Bluetooth Billionton*, provee mecanismos de seguridad, que ya fueron configurados anteriormente.

Para la red inalámbrica, se emplean los mecanismos de seguridad que presta el AP y adicionalmente se emplea un Servidor *RADIUS*.

#### 4.3.2.1 Seguridades Propias del AP

El Punto de Acceso dispone de mecanismos básicos y avanzados para mantener la red inalámbrica segura, seleccionando para el prototipo: Filtrado MAC y WEP.

##### *4.3.2.1.1 Filtrado MAC*

Para realizar el filtrado MAC, se accede mediante el *Web Browser* al AP, y se elige la opción *AccessControl*, para presentar las direcciones MAC confiables, tal como se muestra en la siguiente figura:

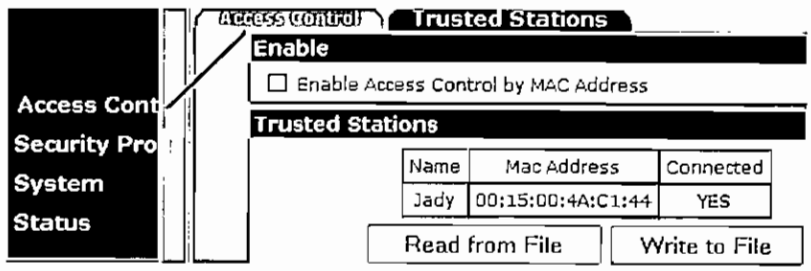



Figura 4.28 Direcciones MAC de Estaciones Confiables

Ahora se procede a agregar una dirección MAC que pertenecerá al grupo de estaciones confiables, en la pestaña *Trusted Stations.*

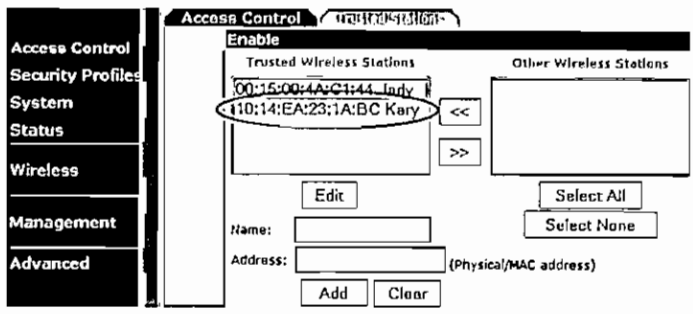



Figura 4.29 Agregación de una Dirección MAC Confiable

Una vez agregada la dirección MAC manual o automáticamente (si la estación esta conectada a la red inalámbrica), se debe habilitar el filtrado de direcciones MAC, como se muestra en la Figura 4.30.

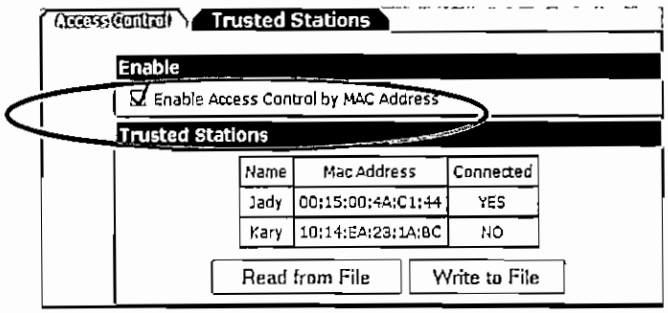



**Figura 4.30 Habilitación del filtrado MAC**

Cabe notar que al determinar el AP automáticamente la dirección MAC de una estación, la coloca en el grupo de "otras estaciones", y se la debe cambiar al grupo de "estaciones confiables" manualmente.

*4.3.2.1.2 WEP*

Para el mecanismo WEP se ha elegido emplear una clave de 128 bits, tipo ASCII, cuya longitud es de 13 caracteres, tal como se aprecia en la siguiente figura.

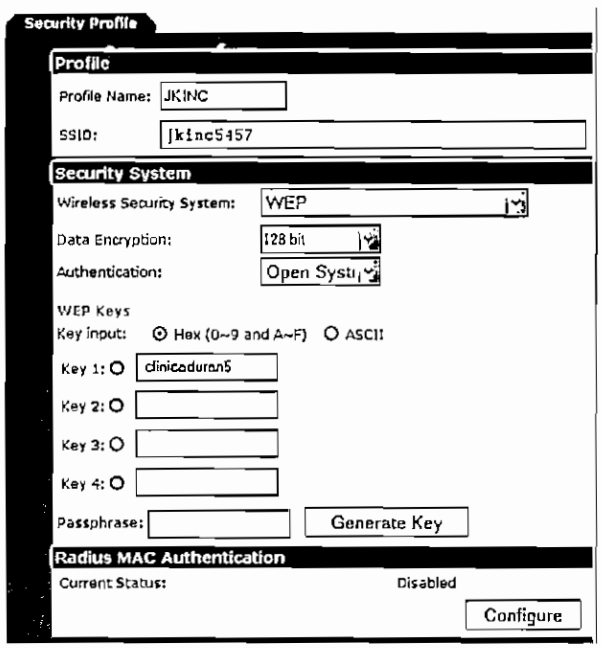



**Figura 4.31 Configuración WEP en el Punto de Acceso**

#### *4.3.2.1.3 IEEE 802.1x con RADIUS*

La seguridad de los datos a manipular en la red, es de vital importancia, ya que la pérdida o inconsistencia de alguno de ellos, podría ocasionar situaciones críticas en la salud de los pacientes; es por ello que se emplea IEEE 802.1x con *RADIUS* para mantener la disponibilidad e integridad de la información.

Para implementar este mecanismo de seguridad, se accede a la configuración del AP, a la opción *Security Profiles*, y se selecciona el perfil creado para el prototipo.

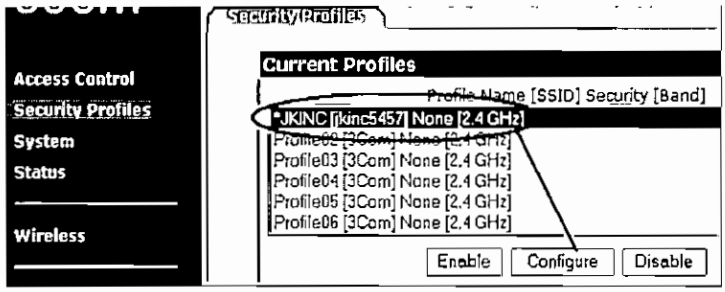



**Figura 4.32 Selección del Perfil**

Luego se ingresan los datos del mecanismo de seguridad para que los clientes puedan autenticarse, tal como se muestra en la siguiente figura.

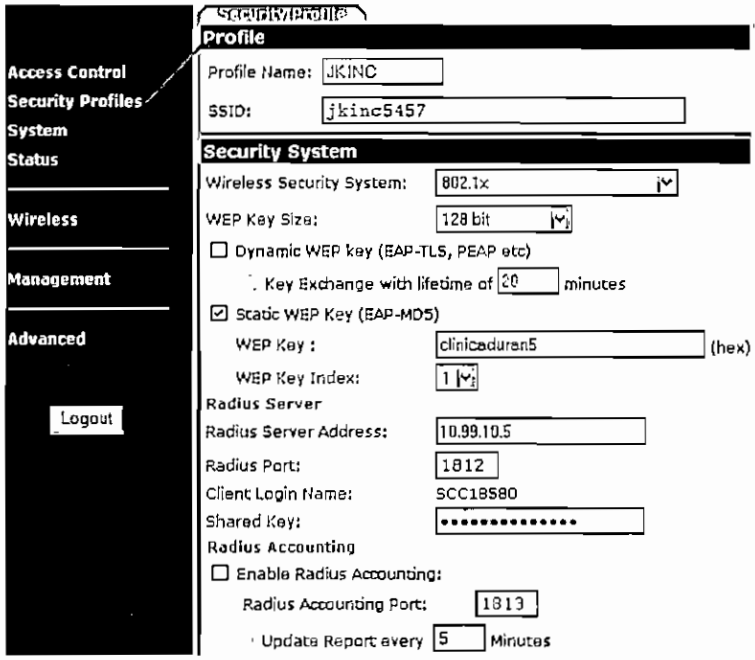



Figura 4.33 Configuración de IEEE 802.1x con RADIUS

Para comprobar que la configuración de seguridad se ha aplicado correctamente, se accede a la opción *Status,/Profiles*. Es necesario adicionalmente, levantar el Servidor y cliente RADIUS para que el proceso de seguridad quede implementado por completo.

#### 4.3.2.2 Seguridad Adicional para el AP

Como se menciono en el ítem anterior, al implementar IEEE 802.1x con RADIUS, se requiere disponer de un Servidor *RADIUS* para poder ejecutar la autenticación. El Servidor *RADIUS* realiza la autenticación de estaciones que requieran conectarse a la red inalámbrica, asegurando ser accedida únicamente por el personal autorizado y su transmisión de datos.

En el Anexo 4A se muestra la configuración del Cliente/Servidor *RADIUS*.

## 4.4 INSTALACIÓN DE LA APLICACIÓN E INTERCONEXIÓN CON LA BASE DE DATOS

Para la instalación de la aplicación, se procede a establecer la conexión ODBC en cada cliente para que tenga acceso al servidor de Base de Datos, ya que se instalará el ejecutable de la aplicación pero se deberá tener el puente de conexión *MySQL ODBC* configurado. La configuración del Servidor de Base de Datos se establece en el Anexo 4B.

### 4.4.1 Instalación de la Aplicación

Establecido el servidor y realizada la conexión ODBC en cada cliente, se podrá acceder a JK INC mediante un ejecutable instalado en cada máquina.

Previo a la utilización del sistema JK INC, es necesario realizar ciertos procedimientos, que se describen en el Manual de Usuario, ubicado en el Anexo 4C.

A continuación, se muestra un ejemplo de acceso desde la aplicación desarrollada en *Java NetBeans* a la Base de Datos, como Administrador, para luego realizar la búsqueda de un paciente por cédula de identidad.

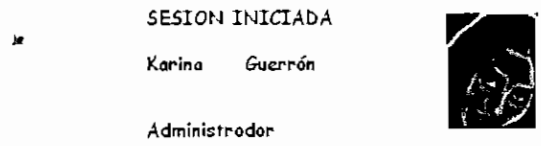



Figura 4.34 Sesión Iniciada

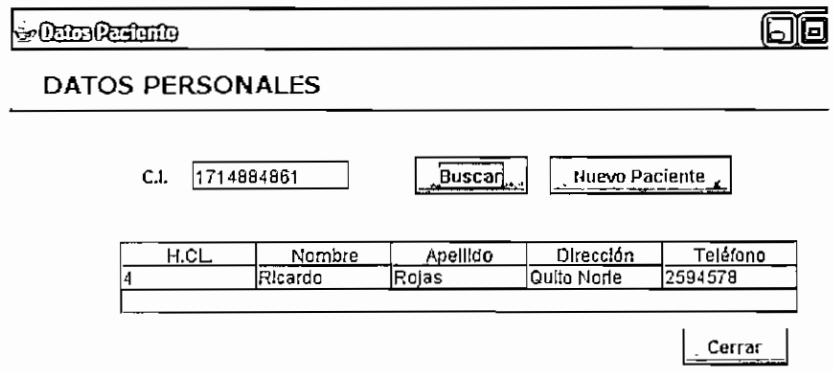



Figura 4.35 Consulta de un Paciente

Cuyo código fuente para la realización de la consulta a la Base de Datos es el siguiente:

```
Coneccion c= new Coneccion();
c.conectar("sun.jdbc.odbc.JdbcOdbcDriver","jdbc:odbc:Clinica Duran");
ResultSet re;
re=c.consultar("Select ... from)
...
```

## 4.5 PRUEBAS DE FUNCIONAMIENTO DEL PROTOTIPO DE PRUEBA

El escenario en el cual se realizó las pruebas fue en las instalaciones de la Clínica "Durán" en conjunto con el personal médico, para realizar los correctivos necesarios y garantizar un funcionamiento adecuado.

Las pruebas del prototipo consta de tres partes fundamentales: pruebas del sistema JK INC, pruebas de la Redes IEEE 802.11 y *Bluetooth*, y pruebas de seguridad del sistema y de la red.

Para la realización de las pruebas de funcionamiento del prototipo, se consideró un equipo servidor, una estación móvil de prueba, dos estaciones de trabajo fijas,

una Palm, un Punto de Acceso, un receptor *Bluetooth*, y un Pulso – Oxímetro tipo *Bluetooth*, como se muestran en las siguientes figuras.

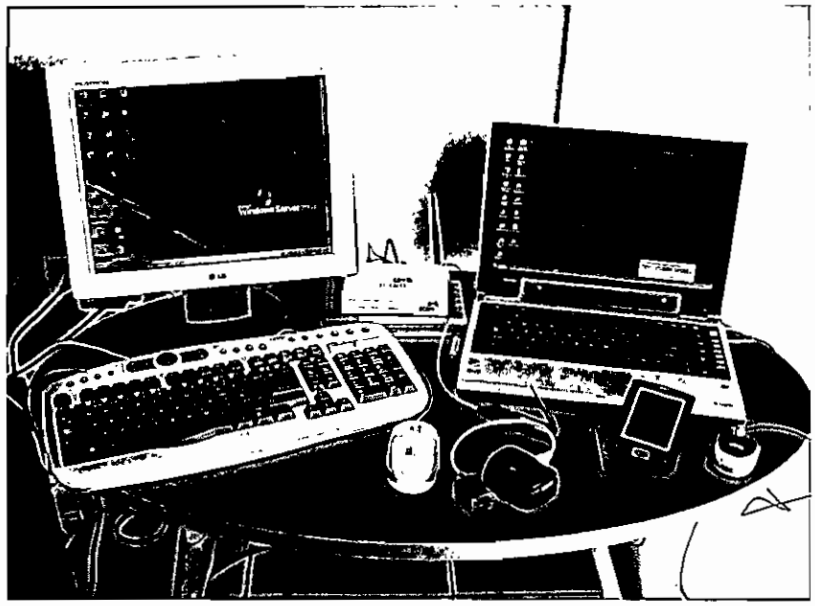


Figura 4.36 Elementos del prototipo

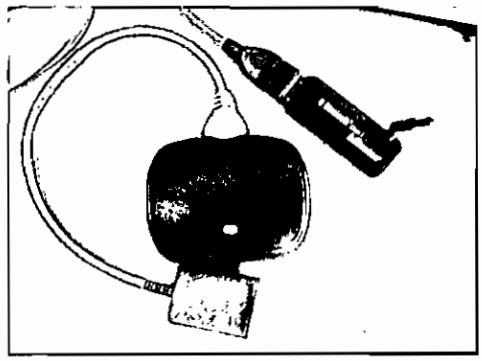


Figura 4.37 Sensor y Receptor *Bluetooth*

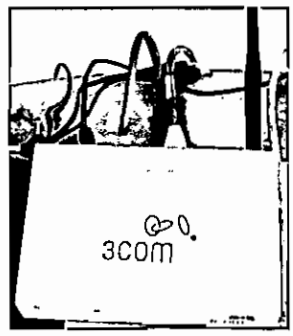



Figura 4.38 Punto de Acceso 3COM

Cabe mencionar, que las estaciones de trabajo fijas, se encuentran ubicadas en Emergencia y en Consulta Externa.

### 4.5.1 PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA JK INC

Previo a la realización de este ítem, se procedió a instalar el sistema JK INC en el equipo móvil de prueba, y verificar su conectividad inalámbricamente con la Base de Datos ubicada en el servidor, como se muestra en las figuras.

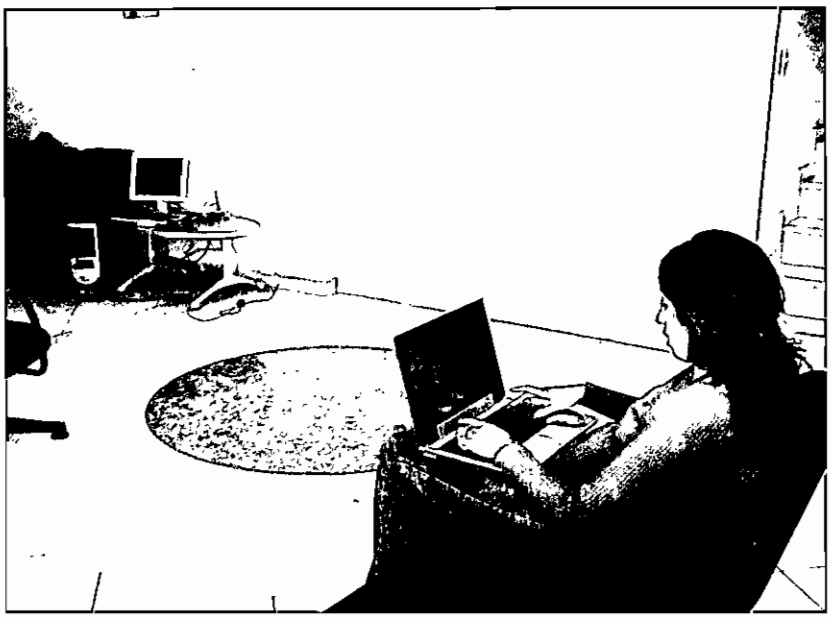


**Figura 4.39 Conectividad inalámbrica del equipo móvil con el servidor**

Para finalizar el Proceso Unificado de Desarrollo de Software planteado en el capítulo anterior, se realiza el Modelo de Pruebas detallado a continuación.

#### 4.5.1.1 Casos y Procedimientos de Pruebas

Estas pruebas están basadas en la interacción de una o más clases de acuerdo a un Caso de Uso; refiriéndose a esto a un objetivo concreto y de acuerdo a un evento que inicia un actor sobre el sistema.

Estos casos de prueba, son llevados a cabo con el siguiente planteamiento:

Según el caso de uso: Gestionar Coordinadores, Gestionar Pacientes, Gestionar Signos Vitales, Gestionar Citas, Gestionar Diagnóstico Médico, Generar Reportes.

| PRUEBAS POR CASOS DE USO | |
|---|---|
| CASO DE USO: Gestionar Coordinadores | |
| DESCRIPCIÓN | Permite administrar la información de los coordinadores en el sistema. |
| ESCENARIO DE PRUEBAS | El usuario con perfil de Administrador puede registrar, actualizar y eliminar Coordinadores. |
| ENTRADA:<br>1. Nombre: Juan Jose<br>2. Apellido: Duran<br>3. *Login*: jduran<br>4. *Password*: jduran<br>5. Perfil: Administrador<br>6. Unidad Médica: Administrativa | |
| PRE CONDICIONES:<br>1. Debe existir un usuario registrado con el perfil de Administrador. | |
| PROCEDIMIENTO:<br>o Ingresar al sistema con perfil de Administrador.<br>o Seleccionar del menú principal la opción de Archivo.<br>o Seleccionar el submenú la opción Administración.<br>o Escoger la opción de Usuario/Doctor.<br>o Escoger nuevo Usuario/Doctor.<br>o Ingresar Datos de Usuario/Doctor.<br>o Se debe dar Clic en guardar. | |
| RESULTADO:<br>Se realizó la verificación de los datos, validándose cada una de las entradas, se devuelven mensajes de error en caso de ser incorrecto el número de cédula ingresado o el login, o de ya existir en la BDD. | |
| OBSERVACIÓN:<br>Se puede verificar la existencia de elementos en la Base de Datos, para eso después del tercer procedimiento visualizar todas las entradas que a este caso de uso se refieren. | |

**Tabla 4.1 Prueba del Módulo de Administración**

| CASO DE USO: Gestionar Pacientes | |
|---|---|
| DESCRIPCIÓN | Su objetivo es registrar los datos de los pacientes en el sistema. |
| PRE CONDICIÓN:<br>1. Que exista una solicitud de registro de paciente. | |
| PROCEDIMIENTO:<br>1. Escoger la opción Paciente del Menú Principal, luego Datos Paciente.<br>2. Ingresar el número de cédula o nombre, para verificar si existe el registro del paciente.<br>3. En caso de no existir el Paciente, se debe dar un clic en el botón Agregar Paciente.<br>4. Ingresar los datos para el nuevo registro de paciente y dar clic en Aceptar. | |
| RESULTADO:<br>Realizada la entrada de valores, se validan en el sistema y se procede a almacenarlos, correctamente. | |
| OBSERVACIÓN:<br>En caso de no tener ningún valor de entrada, pero de hacer clic en el botón de Aceptar, se despliega un mensaje con los datos que el usuario debe ingresar para este caso de uso. | |

**Tabla 4.2 Prueba del Módulo de Pacientes**

| CASO DE USO: Gestionar Citas | |
|---|---|
| DESCRIPCIÓN | Permite registrar la cita médica de un paciente para Consulta Externa. |
| PRE CONDICIÓN:<br>1. Que exista registrado un paciente.<br>2. Que exista una solicitud de registro de cita. | |
| PROCEDIMIENTO:<br>1. Escoger la opción Administrar Cita del Menú Principal, luego Establecer Cita<br>2. Ingresar el número de cédula o nombre, para verificar si existe el registro del paciente.<br>3. Seleccionar la especialidad, y Doctor de los combos.<br>4. Luego dar clic en el botón Calendario, para visualizar los horarios disponibles de atención que se puede dar al paciente solicitante de cita.<br>5. Escoger la fecha en el calendario y la hora de la lista de horarios disponibles<br>6. Luego dar clic sobre el botón guardar y se agrega la cita realizada.<br>7. Con lo cual se podrá acceder al formulario de pago, para escoger el valor a cancelar y la forma. | |
| RESULTADO:<br>Realizada la entrada de valores, se validan en el sistema y se procede a mostrar los resultados en primera instancia, luego al escoger una de las citas y establecerla, se procede a asignar la cita válida escogida al paciente. Finalmente, se procede a escoger el valor a cancelar, con lo cual el paciente está habilitado para ir a la toma de signos vitales. | |
| OBSERVACIÓN:<br>En caso de no tener ningún valor de entrada, pero de hacer clic en el botón de Establecer Cita, se despliega un mensaje con los datos que el usuario debe ingresar para este caso de uso. | |

Tabla 4.3 Prueba del Módulo Gestionar Citas

| CASO DE USO: Gestionar Signos Vitales | |
|---|---|
| DESCRIPCIÓN | Obtener los datos de la medición de signos vitales de los pacientes a partir de los sensores. |
| PRE CONDICIÓN:<br>1. Obtener una lista de los pacientes que pueden acceder a la toma de signos vitales y definir los sensores para dicha medición.<br>2. Que exista tanto el establecimiento de la cita y el pago de la misma, por parte del paciente. | |
| PROCEDIMIENTO:<br>1. Escoger la opción de Signos Vitales del Menú Principal, luego Medir SV.<br>2. Se selecciona el paciente a medir los signos vitales.<br>3. Se ingresan los datos peso, estatura, temperatura, y presión.<br>4. Se hace clic sobre el botón Medir Pulso y Ritmo Cardiaco, y se accede al formulario de obtención de estos datos a través de los sensores, al hacer clic en cerrar, se almacena la *última* medición en los cuadros de texto del formulario previo.<br>5. Se hace clic sobre el botón Aceptar y se almacena toda la información. | |
| RESULTADO:<br>Realizada la obtención y entrada de valores, se validan en el sistema y se procede a mostrar los resultados. | |
| OBSERVACIÓN:<br>En caso de no obtener ningún valor de entrada, y de hacer clic en el botón de Aceptar, se despliega un mensaje con los datos que el usuario debe ingresar para completar este módulo. | |

Tabla 4.4 Prueba del Módulo Signos Vitales

| CASO DE USO: Establecer Diagnóstico Médico | |
|---|---|
| DESCRIPCIÓN | Permite recoger la información del paciente en un formulario para que el coordinador (Doctor) de un diagnóstico y toda esta información se almacene en la historia clínica. |
| PRE CONDICIÓN<br>Aquí existen dos casos:<br>1. En Consulta Externa: que se haya reservado una cita, realizado el pago y se haya tomado los signos vitales el paciente.<br>2. En Emergencia: que se haya registrado al paciente y que se le hayan tomado los signos vitales. | |
| PROCEDIMIENTO:<br>1. Escoger la opción de Diagnóstico Médico/Emergencia del Menú Principal.<br>2. Ingresar el número de cédula, nombre o HCL (Historial Clínico), para verificar si existe el registro del paciente.<br>3. En Emergencia se permite agregar al paciente directamente desde el formulario.<br>4. El sistema carga la información del paciente, y la ultima medición de signos vitales.<br>5. Se hace clic sobre el botón ver historial, para acceder al último de ellos.<br>6. El Doctor hace clic sobre el botón Nuevo Registro, e ingresa la información de la atención al paciente.<br>7. Se permite agregar una nueva cita haciendo clic sobre el botón Próxima Cita.<br>8. Se presiona el botón Guardar y se almacenan los datos ingresados. | |
| RESULTADO:<br>Se ingresar las entradas de valores, se validan en el sistema y se almacenan. | |
| OBSERVACIÓN:<br>En caso de no obtener ningún valor de entrada, y de hacer clic en el botón de Aceptar, se despliega un mensaje con los datos que el usuario debe ingresar para completar este módulo. | |

**Tabla 4.5 Prueba del Módulo Diagnóstico Médico**

| CASO DE USO: Generar Reportes | |
|---|---|
| DESCRIPCIÓN | Permite visualizar información solicitada por el Administrador en respuesta a una petición de un coordinador. |
| Precondición | |
| PRE CONDICIÓN:<br>1. Que exista el registro de datos solicitados. | |
| PROCEDIMIENTO:<br>1. El Administrador selecciona el tipo de reporte.<br>2. El sistema genera el reporte.<br>3. El sistema muestra los resultados. | |
| RESULTADO:<br>Se despliegan los valores solicitados, según el tipo de reporte que se requiera. | |
| OBSERVACIÓN:<br>En caso de no obtener ningún valor al reporte seleccionado, se despliega un mensaje de no existencia de datos o incoherencia de reporte solicitado. | |

**Tabla 4.6 Módulo de Generar Reportes**

### 4.5.2 PRUEBAS DE FUNCIONAMIENTO DE LA RED HIBRIDA

Para realizar las pruebas de funcionamiento de la red híbrida planteada, se utilizó la herramienta de análisis de tráfico de red (*snnifer*): *Ethereal Network Protocol Analyzer* v 0.10.14 para la red cableada, *Intel Pro Set Wireless* v 9.0.1.0 para la red inalámbrica, e *IVT Corporation BlueSoleil* para la red *Bluetooth*.

La configuración del Punto de Acceso y la estación de trabajo, estuvo dada por los siguientes parámetros:

- Dirección IP AP: 10.99.10.1
- Máscara AP: 255.255.255.0
- SSID: jkinc5457
- Perfil de pruebas: jkinc
- Dirección IP Estación: 10.99.10.11
- Máscara Estación:255.255.255.0
- Puerta de enlace Estación: 10.99.10.1
- DNS: 10.99.10.5

Mediante el *snnifer ethereal*, se capturaron los siguientes paquetes durante la ejecución del software JK INC en la estación de prueba.

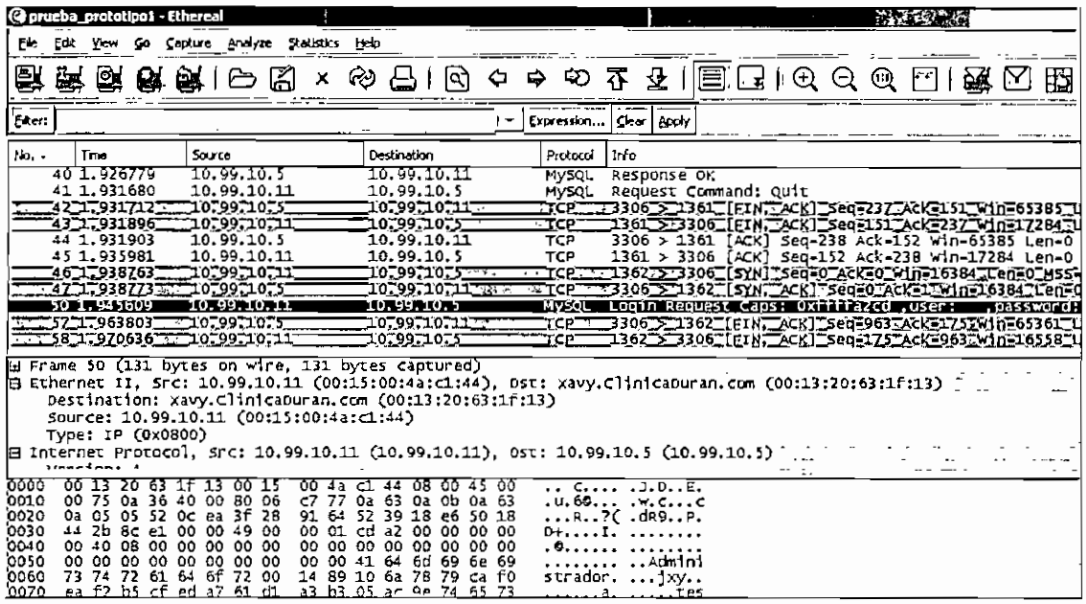



Figura 4.40 Paquete de autenticación de usuario en JK INC

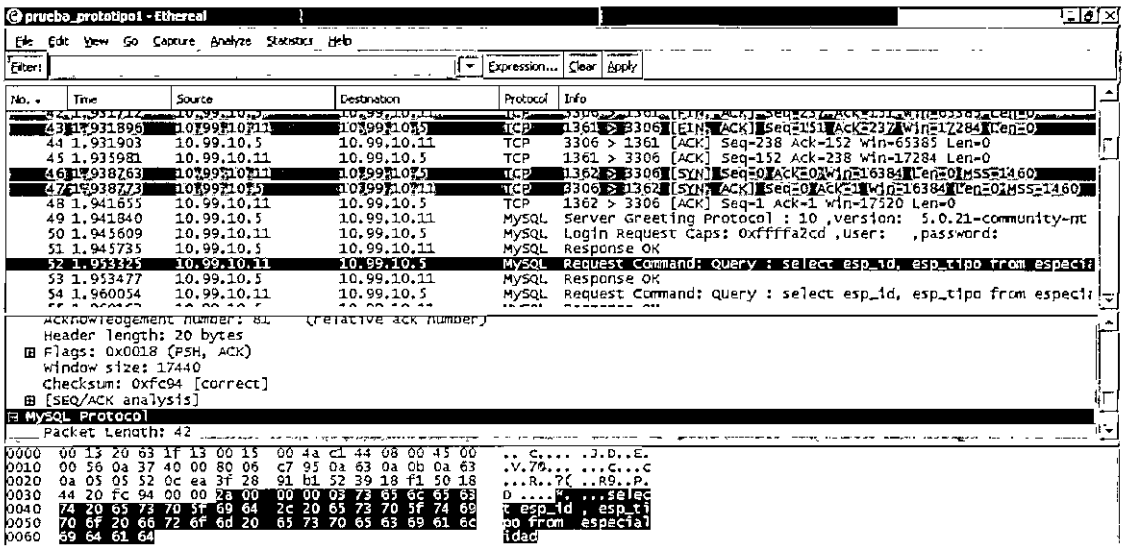



**Figura 4.41 Paquete de consulta de información a la BDD desde JK INC**

Inicialmente, a través del software *Intel Pro Set Wireless*, se procedió a obtener los parámetros de la conexión de red inalámbrica establecida, mediante la estación de prueba, en una habitación ubicada en el segundo piso, adquiriéndose el siguiente resultado.

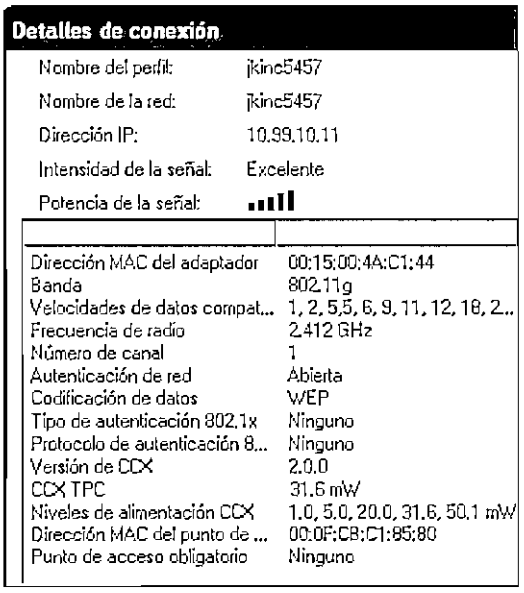



**Figura 4.42 Parámetros de conexión de la red inalámbrica**

Se pudo determinar además, que no existía perdida de paquetes en la transmisión de datos a lo largo de todo el primer piso, y que se mantenía una velocidad promedio de 48 Mbps, tal como se muestra en las siguientes figuras.

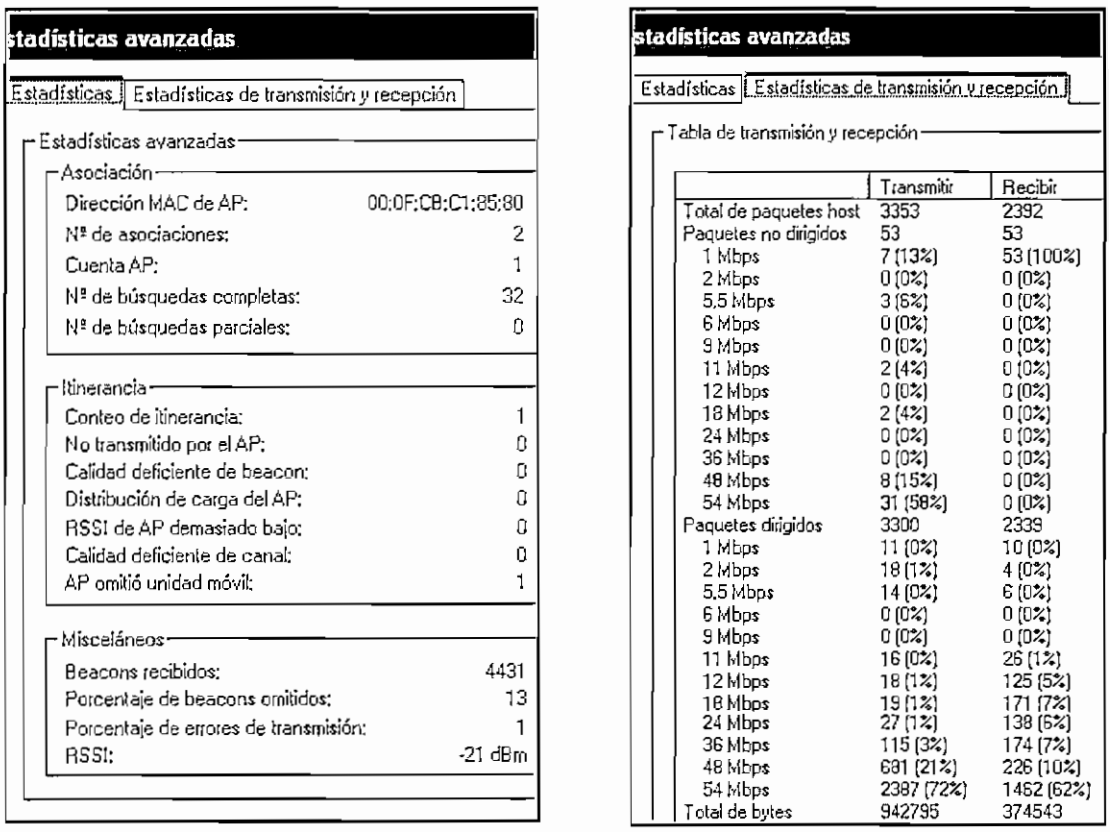



**Figura 4.43 Paquetes transmitidos y estadísticas de transmisión/recepción en la red inalámbrica en 5 segundos**

La conexión a la red inalámbrica mediante el equipo de mano PALM, se realizó empleando la aplicación *WiFiLT*, en la que se configuró, el nombre de la estación a conectarse (JADYTA), y la carpeta a la que se desea acceder.

Cabe aclarar, que la estación a la que se conecta la PALM, es en la cual se encuentra la carpeta de datos de medición de los sensores, como se mencionó anteriormente.


**Figura 4.44 Configuración de la PALM para acceder a la red inalámbrica**

En la opción **Browse** de la Figura 4.45 se procede a seleccionar el dominio o grupo de trabajo al que se desea conectarse, como se muestra en la siguiente figura.

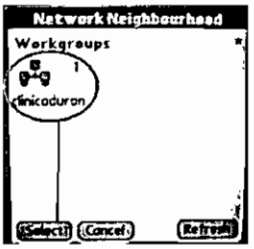



**Figura 4.45 Dominio a conectarse a través de la PALM**

Finalmente se elije el equipo en el cual se ubica la carpeta compartida (**JKINC datos**) a la que se desea acceder mediante la red inalámbrica.


**Figura 4.46 Equipo en el que se encuentran los datos compartidos**

Con lo cual se pueden observar los archivos que incluye dicha carpeta, y acceder a su contenido.

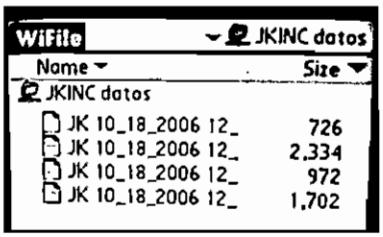



**Figura 4.47 Archivos de la carpeta compartida accedidos desde la PALM**

En lo que la red *Bluetooth* se refiere, mediante la línea de comandos de *Netbeans*, se procedió a capturar los paquetes enviados, durante 18 segundos, obteniéndose un *througput* de hasta 2,2 Kbps. Para determinar este valor, se contabilizó el número de paquetes válidos transmitidos en el intervalo de tiempo

planteado, pasados a bits. En la siguiente figura se muestra un ejemplo de captura de datos.

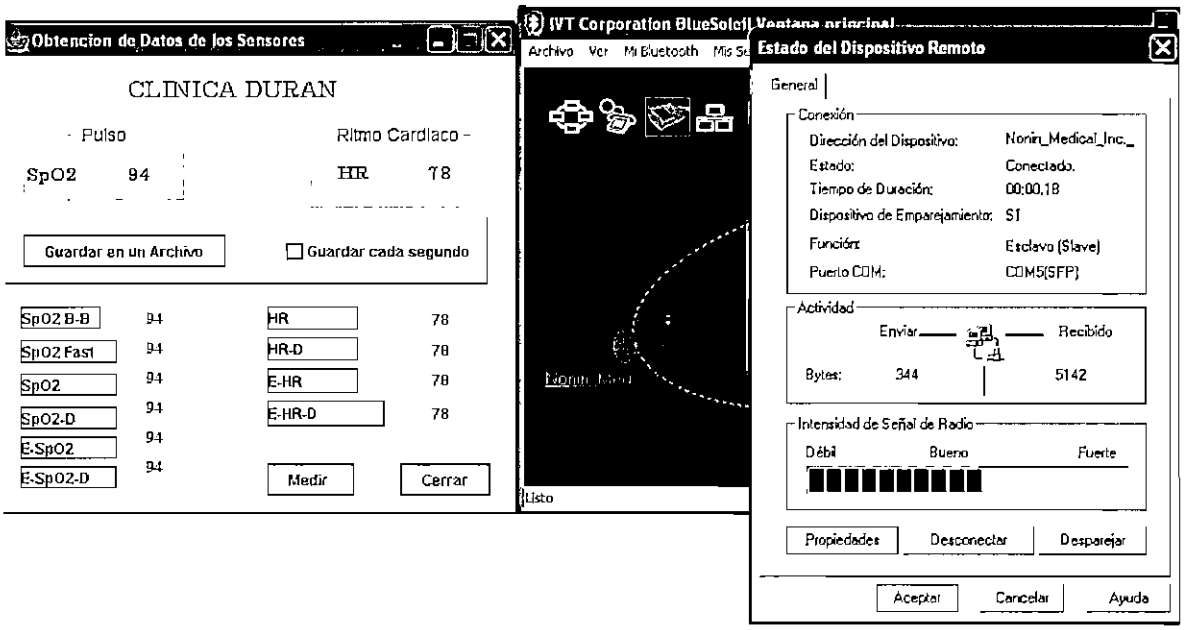



**Figura 4.48 Paquetes transmitidos en la red *Bluetooth* durante 10 segundos**

Finalmente, se compararon los datos obtenidos, con los valores teóricos, como se muestra en la Tabla 4.7, para demostrar el adecuado funcionamiento de la red híbrida planteada.

| Ítem | Red Inalámbrica | | Red *Bluetooth* | |
|---|---|---|---|---|
| | Valor Teórico | Valor de Pruebas | Valor Teórico | Valor de Pruebas |
| Velocidad de Transmisión | 5.5 hasta 54 Mbps | 24, 36 y 54 Mbps | 3.37 Kbps | 2.2 Kbps |

**Tabla 4.7 Velocidades de Transmisión del Prototipo**

En las siguientes figuras, se muestran ejemplos de: instrucción al personal médico del funcionamiento de la aplicación, y del funcionamiento de la red hibrida, mediante la medición del pulso y ritmo cardíaco, en las habitaciones de los pacientes de la clínica, considerando que el servidor se encontraba ubicado en la planta baja de la edificación, y el computador de prueba, al cual se encontraba conectado el receptor *Bluetooth*, ubicado en la estación de enfermería en el segundo piso.

Figura 4.49 Instrucción del funcionamiento de la Aplicación

Figura 4.50 Personal médico probando el Software JK INC

Figura 4.51 Medición de Signos Vitales a paciente previo a ser operado

**Figura 4.52 Medición de Signos Vitales a paciente post – operación y su bebe**

En el software JK INC, se establecen alarmas para ciertos valores de pulso y ritmo cardiaco en función de edad y condiciones del paciente, acorde a los parámetros establecidos en el campo médico, como se muestra en el Anexo 4C.

### 4.5.3 PRUEBAS DE SEGURIDAD

Los mecanismos de seguridad planteados para el prototipo son: Filtrado MAC, WEP, y Servidor RADIUS, como se indicó anteriormente.

En primera instancia se procedió a probar el Filtrado MAC, agregando direcciones MAC de las estaciones de confianza, en el Punto de Acceso. Seguidamente se accedió a la red inalámbrica, con un computador no incluido en la lista de equipos de confianza, razón por la cual no se pudo acceder a la red. En la estación de trabajo de prueba y en la PALM, se configuró el mecanismo de seguridad WEP con la clave **clinicaduran5**, establecida en el AP.

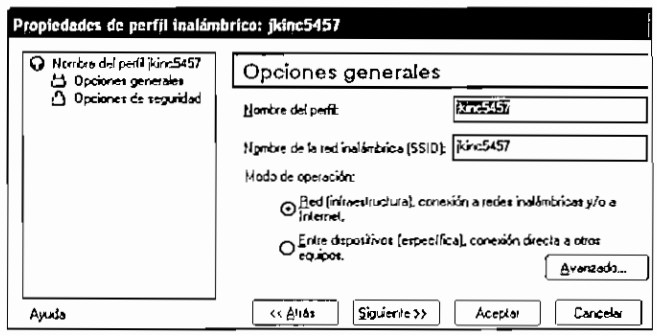



**Figura 4.53 Configuración de la tarjeta de red inalámbrica de la estación de prueba**

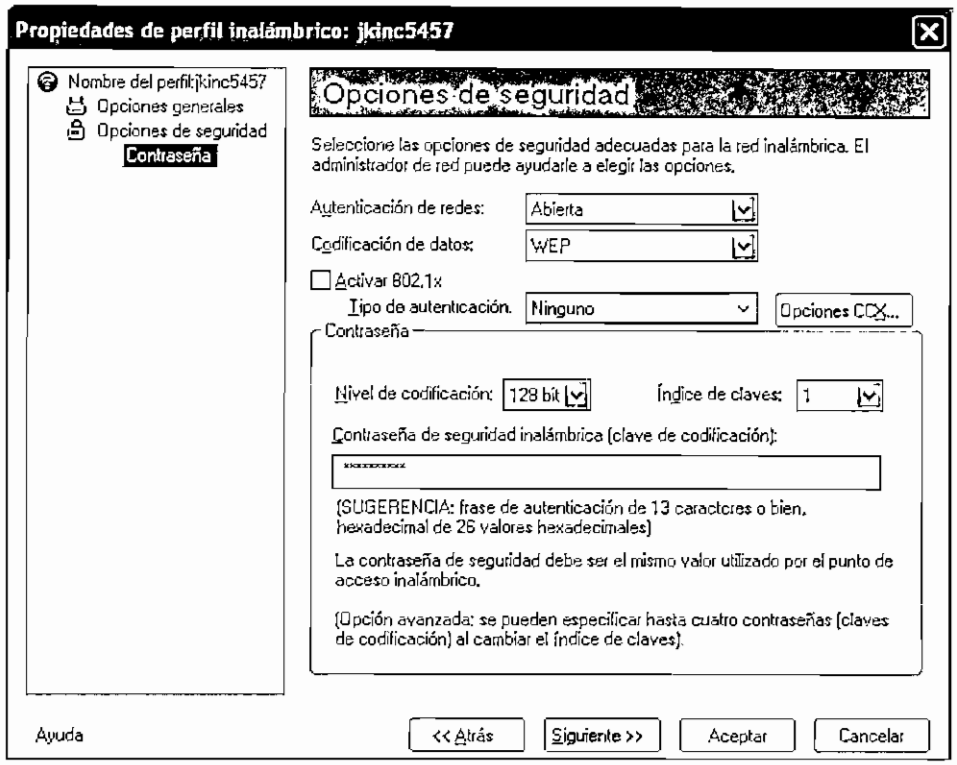



Figura 4.54 Configuración de la seguridad de red inalámbrica de la estación de prueba


Figura 4.55 Configuración del Mecanismo de Seguridad de la PALM

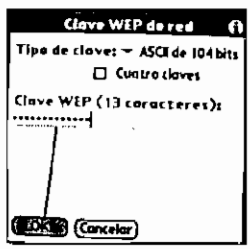



Figura 4.56 Configuración de la Clave WEP en la PALM

Luego, se accedió a la red inalámbrica, mediante la estación de prueba, ingresando la clave WEP definida; posteriormente se ingresó una clave errónea, sin llegar a tener acceso a la red.

Hasta ese instante, implementados los dos mecanismos de seguridad descritos, se obtuvieron resultados satisfactorios en cuanto a velocidad de transmisión de los datos, y su actualización, obteniéndose un retardo máximo de 50 mseg.

Finalmente para probar el mecanismo de seguridad mediante IEEE 802.1x con Servidor *RADIUS*, se procedió a configurar el Punto de Acceso y la estación de trabajo de prueba, acorde a lo establecido en el Anexo 4A.

Seguidamente se intento acceder a la red mediante una clave compartida errónea, y sin ser un usuario permitido, por lo cual no se pudo acceder a la red inalámbrica, ocurriendo lo contrario al ser un usuario autorizado e ingresar la clave correcta.

Es necesario acotar que la PALM de la que se dispone para el prototipo, no dispone de este último mecanismo de seguridad, por lo cual no se pudo realizar las pruebas de funcionamiento con el mismo.

## 4.6 CORRECCIONES AL PROTOTIPO DE PRUEBA

El prototipo planteado, funcionó acorde a las necesidades de la institución, en lo que a velocidad de transmisión, actualización de los datos, y cobertura se refiere, sin embargo, se requirió elaborar dos correcciones, una en lo que a seguridad se refiere, y la otra en el software JK INC.

Realizada una prueba completa del prototipo, con el último mecanismo de seguridad descrito anteriormente, se obtuvieron retardos significativos de hasta 3 segundos en la transmisión de los datos, razón por la cual se decidió, utilizar únicamente los dos primeros mecanismos de seguridad; para así garantizar la disponibilidad de los datos de los pacientes y su actualización a tiempo.

En el software, por petición del gerente de la clínica, Dr. Juan José Durán, se agrega el Índice de Masa Corporal (IMC), y la clasificación que conlleva su valor calculado, en el formulario de Signos Vitales e Historia Clínica, y el dato "Referido por" en el último formulario.

## 4.7 COSTOS DEL PROTOTIPO DE PRUEBA

El presupuesto, incluye los elementos descritos en el inicio de este capítulo, sin embargo para elaborarlo, es necesario incluir la mano de obra de la instalación y configuración de los equipos empleados. El presupuesto no incluye el IVA.

| Ítem | Descripción | Cant. | V Unit. | V Total |
|---|---|---|---|---|
| A | **RED INALAMBRICA 802.11g** | | | |
| A.1 | AP 3COM OFFICECONNECT WIRELESS 108 MBPS 11G POE. | 1 | $ 156,95 | $ 156,95 |
| A.2 | ADAPTADOR DE RED | 4 | $ 40 | $ 160,00 |
| B | **RED DE SENSORES BLUETOOTH** | | | |
| B.1 | RECEPTOR BLUETOOTH BILLIONT | 1 | $ 21,00 | $ 21,00 |
| B.2 | SENSOR DE RITMO CARDÍACO BLUETOOTH | 1 | $ 550,00 | $ 550,00 |
| C | **SISTEMA JK INC** | | | |
| C.1 | DISENO Y ELABORACION DEL SISTEMA | | $ 3.080,00 | $ 3.080,00 |
| 3 | **TRABAJOS DE INSTALACION Y PUESTA EN MARCHA** | | | |
| 3.1 | INSTALACION Y CONFIGURACION DE LA RED | 1 | $ 500,00 | $ 500,00 |
| 3.2 | INSTALACION Y CONFIGURACION DEL SISTEMA | 1 | $ 100,00 | $ 100,00 |
| 3.3 | PLANOS AS BUILT | 1 | $ 80,00 | $ 80,00 |
| **TOTAL PROTOTIPO PRUEBA** | | | | **$ 4.647,95** |

Tabla 4.8 Presupuesto Referencial del Prototipo de Prueba

# CAPÍTULO 5

# CONCLUSIONES Y RECOMENDACIONES

# 5. CONCLUSIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

- Mediante este proyecto se ha realizado el diseño e implementación tanto de la red como de una aplicación de *software*, unificando y complementando tecnologías, que dan posibles y útiles soluciones a los diferentes escenarios que requieren el aporte de la ingeniería para facilitar las tareas cotidianas.
- Se ha establecido una topología de red adecuada, que permitió mantener la jerarquía y orden en el diseño de la misma, proporcionando al servidor la información apropiada para administrar adecuadamente el acceso de sus usuarios y la seguridad de su información.
- El prototipo implementado convierte el proceso de atención médica en un esquema cero papel, garantizando la uniformidad y seguridad de la información.
- Existen diversas herramientas para modelamiento del sistema, de los cuales se utilizó *Racional Rose*, ya que provee soporte para aplicaciones orientadas a objetos, y utiliza lenguaje UML.
- La red de datos no interfiere con los equipos de medición médica, ya que esto ocasionaría pérdida o alteración de la información, por ello se realizó la evaluación del sitio de implementación mediante pruebas de campo, solucionando éste inconveniente.
- En el presente proyecto, para la implementación de tecnologías de comunicación entre dispositivos, se ha empleado el equipo *Billonton* tipo *Bluetooth*, que implementa el estándar en forma parcial, lo que introduce una brecha de seguridad, que es compensada mediante los diferentes mecanismos de seguridad brindados por su *software* de trabajo.
- El alcance del receptor *Bluetooth* es lo suficientemente adecuado para garantizar la confiabilidad de los datos medidos por el sensor, en las áreas planteadas para su uso.
- El sensor B*luetooth*, mantiene un rango de valores de medición de pulso y ritmo cardíaco, con un porcentaje de error de ± 3 %, en comparación con los equipos de mano correspondientes.

- La comunicación en la red híbrida, puede generar un cierto retardo, por lo cual este valor es optimizado o compensado con los otros elementos del sistema.
- No es adecuado implementar mecanismos de seguridad tales como IEEE 802.1x con RADIUS o WPA, ya que incluyen alta ocupación y procesamiento de la red, y esto ocasiona introducir retardos significativos, que pueden hacer la diferencia entre la vida o la muerte de un paciente.
- El prototipo elaborado, satisface las necesidades de atención a pacientes en Consulta Externa, Emergencia y Ambulancia.
- El sistema de medición de signos vitales a través de una red de sensores inalámbricos, es una contribución tecnológica altamente valorada en el campo médico, al eliminar las consecuencias en cuanto a salud del paciente, por descuidos del personal médico.
- Los valores de alarmas en cuanto a pulso y ritmo cardíaco, han sido establecidos en base a patrones de edad, proporcionados por personal médico capacitado.
- El sistema JKINC mediante el paquete javax.com, obtiene los datos de medición del sensor a través del puerto serial, los desencapsula acorde al formato de trama definido por los fabricantes del equipo, y los muestra.
- Mediante PDAs o PALMs, se puede acceder a los datos de un paciente mediante la red inalámbrica, y realizar monitoreo.
- Java es una herramienta muy efectiva para procesamiento multihilo y multiproceso, efectivizando la comunicación del puerto serial en el sistema JKINC.
- Los equipos de interconexión, deben estar trabajando con una versión igual o mayor en cuanto a tecnología se refiere, para garantizar su correcto funcionamiento y configuración de seguridades.

## 5.2 RECOMENDACIONES

- Encender el sensor en el área de consulta externa, únicamente cuando sea necesario, por razones de consumo de batería del mismo.

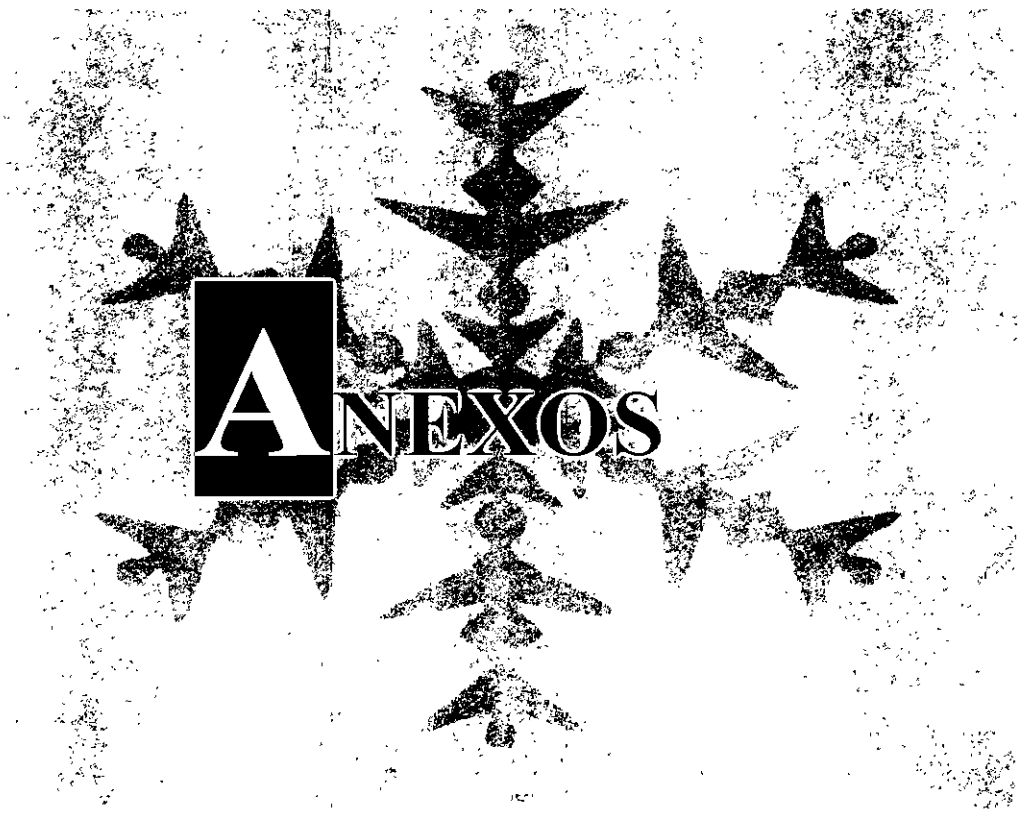
- Hacer caso omiso a las políticas de seguridad planteadas, para evitar perdidas de información irrecuperables y mantener el adecuado funcionamiento de la red.
- Verificar al término de cada semana, el estado del sensor y su margen de error en cuanto a los datos obtenidos, por seguridad de los pacientes y confiabilidad de la clínica.
- Tener conocimientos sobre términos médicos, para entender adecuadamente la funcionalidad del software.
- No cambiar la ubicación definida para los equipos de interconectividad, ya que esto ocasionaría pérdida de cobertura.
- Tomar como referencia este trabajo para futuros proyectos de avance tecnológico en el campo médico, en lo que a automatización de manejo de información se refiere, ya que sienta uno de los primeros precedentes para la aplicación de la telemedicina en nuestro país.

# REFERENCIAS BIBLIOGRÁFICAS

# REFERENCIAS BIBLIOGRÁFICAS


- Machuca Toapanta Sandra Jackeline, Pailiacho Guevara Gabriela Soledad; Sistema Web para determinar el grado de histocompatibilidad entre donantes y receptores de transplantes de órganos y tejidos; Pág. 20 – 40; Marzo 2006.
- JACOBSON I., BOOCH G., RUMBAUGH J., El Proceso Unificado de Desarrollo de Software
- Prasat Ramjee, Luis Muñoz, WLAN and WPAN TOWARDS 4G WIRELESS, Artech House, 2003.
- Matthew Gast, 802.11 Wireless Networks: Designates Guides, O'Reilly, 2002.
- TANENBAUM Andrew S., Redes de Computadoras, Prentice Hall, 4ta edición, 2000.
- SINCHE Soraya, Redes de Área Local Inalámbricas, 2005.
- SINCHE Soraya, Comunicaciones Inalámbricas, 2004.
- HIDALGO Pablo, Redes de Área Local, 2004.
- INSUASTI Jorge, Diseño e implementación de dos soluciones de seguridad para una red inalámbrica, Noviembre del 2004.
- CADENA Alvaro, Diseño y pruebas de campo de una red LAN inalámbrica para la Empresa Eléctrica Quito S.A. (campus El Dorado), empleando el estándar IEEE 802.11g, Octubre del 2005.
- JORDY Mayné, IEEE 802.15.4 y Zigbee.pdf, Octubre del 2004.
- Cisco Systems, Designing Wireless 802.11 Networks.pdf, 2003.
- LEWIS F. L., Wireless Sensor Networks.pdf, 2004.
- IEEE Institute of Electrical and Electronics Engineers., Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, IEEE 802.11g, Junio del 2003.
- IEEE 802.15.4 MAC Overview, Marco Naeve Eaton Corporation, 10 May, 2004.

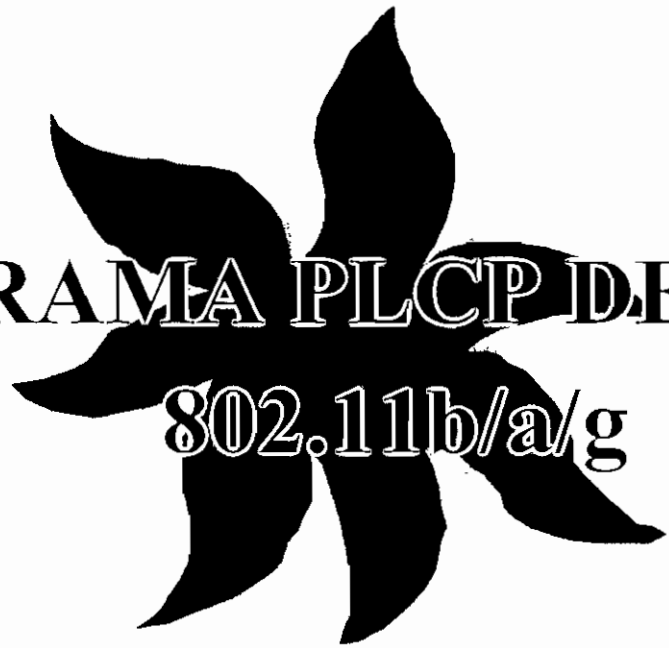
- Sensors Networks for Medical Care, Victor Shnayder, Bor-rong, Chen, Konrad Lorincz, Thaddeus R. F. Fulford-Jones, and Matt Welsh. Harvard University Technical Report TR-08-05, April 2005.
- Time Synchronization for ZigBee Networks, Dennis Cox, Emil Jovanov, Aleksandar Milenkovic, Electrical and Computer Engineering Department, University of Alabama in Huntsville, Huntsville, AL 35899 USA.
- Redes inalámbricas para los nuevos servicios personales de e-salud basados en tecnologías de inteligencia ambiental, Monteagudo Peña, José Luís, Oscar Moreno Gil, Jorge García Pérez y Juan Reig Redondo, Instituto de Salud Carlos III - Área de Investigación en Telemedicina y Sociedad de la Información.
- http://lisisu02.usal.es/~mmoreno/ISWATema4.pdf
- http://www.infor.uva.es/~mlaguna/is2/2-6-Proceso.pdf
- http://www.ieee802.org/15/
- http://www.zigbee.org/
- http://www.nonin.com/
- http://www.eecs.harvard.edu/~mdw/papers/
- http://www.sensorsmag.com/articles/0603/14/
- http://java.sun.com/
- http://www.bluetooth.com/
- http://www.dlinkla.com/home/productos/tecnico.jsp?pro=32
- www.audiotronics.es/product.aspx?productid=25952 - 35k
- http://www1.linksys.com/international/product.asp?coid=38&ipid=275
- http://www1.linksys.com/international/product.asp?coid=38&ipid=272
- http://www.domodesk.com/content.aspx?co=97&t=146&c=43
- http://acis.org.co/memorias/JornadasTelematica/IIJNT/BlueTooth_Zigbee.pdf
- sertel.upc.es/qos/documentos/9_Jaime_Joven_QoS_WSN.pdf
- http://bibliotecnica.upc.es/pfc/mostrar_dades_PFC.asp?id=40380
- www.maxstream.net/products/xbee/ datasheet_XBee_OEM_RF-Modules-Espanol.pdf



# ANEXOS


ANEXO 1A

# TRAMA PLCP DE IEEE 802.11b/a/g



## Formato de la trama PLCP de IEEE 802.11

La capa PLCP de 802.11 consta de tres campos: Preámbulo, cabecera y datos (MPDU). El Preámbulo se trasmite siempre a 1 Mbps y esta constituido por dos subcampos:

- Sincronización: Permite al receptor realizar operaciones de sincronización, esta formado por 128 bits.
- Delimitador de inicio de trama: indica el inicio de una trama.

La cabecera está compuesta por los campos:

- Señalización: consta de 8 bits y permite definir el esquema de modulación a emplear para el intercambio de datos. La velocidad conseguida, será el valor de este campo multiplicado por 100 Kbps. En DSSS PHY se definen 2 modulaciones obligatorias dadas por las palabras: X0A para 1 Mbps con DBPSK y X14 para 2 Mbps con DQPSK.
- Servicio: consta de 8 bits y esta reservado para uso futuro.
- Longitud: es un entero de 16 bits sin signo, indica el número de microsegundos necesarios para la transmisión.
- CRC: realiza la comprobación de los campos anteriores empleando CRC de 16 bits.

Finalmente el campo de datos, que es de longitud variable y contiene la MPDU. En conjunto, el preámbulo PLCP, la cabecera PLCP y los datos MPDU forman la trama PLCP (PPDU).

## Formato de la trama PLCP de IEEE 802.11b

El estándar define dos preámbulos y cabeceras diferentes, que operan con la especificación actual DSSS de 1 y 2 Mbps.

### Preámbulo grande

El formato de la trama con preámbulo grande se muestra a continuación:

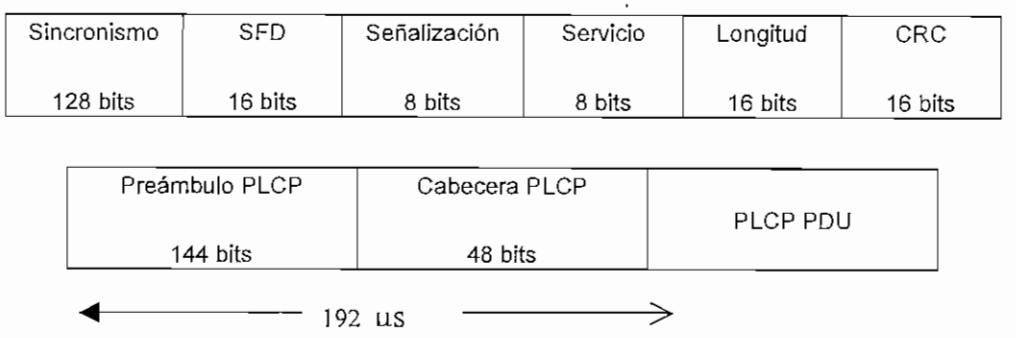



**Figura 1A.1 Trama PLCP con preámbulo grande**

El formato de ésta trama difiere de la trama de IEEE 802.11 en la codificación del campo Señalización y el uso del campo Servicio.

- Señalización: incluye dos modulaciones adicionales, X37 para 5.5 Mbps y X6E para 11 Mbps.
- Servicio: consta de 8 bits, nombrados desde b0 hasta b7, donde b0 se trasmite primero. Tres bits de este campo se utilizan para la extensión de alta velocidad; el bit b7 indica que el campo Longitud ha sido modificado; el bit b3 indica la técnica de modulación a emplear, entre CCK(0) o PBCC[1](1); y el bit 2 se emplea para indicar la frecuencia de transmisión. Los bits b0, b1, b4, b5, y b6 son seteados a 0. La figura 1000 resume lo mencionado.

| b0 | b1 | b2 | b3 | b4 | b5 | b6 | b7 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | Locked clocks bit.<br>0= not<br>1= locked | Mod.<br>0= CCK<br>1= PBCC | 0 | 0 | 0 | Extensión de longitud |

**Figura 1A.2 Campo Servicio de la trama PLCP con preámbulo grande**

**Preámbulo corto**

Este preámbulo fue creado para reducir la sobrecarga de cabecera y con ello conseguir mayor throughput, se lo denomina HR/DSSS/Short. Mediante la siguiente figura se muestra el formato de ésta trama, y los cambios respecto de la trama grande.

[1] Packet Binary Convolutional Coding, esquema de codificación para obtener velocidades de 2, 5.5 y 11 Mbps.

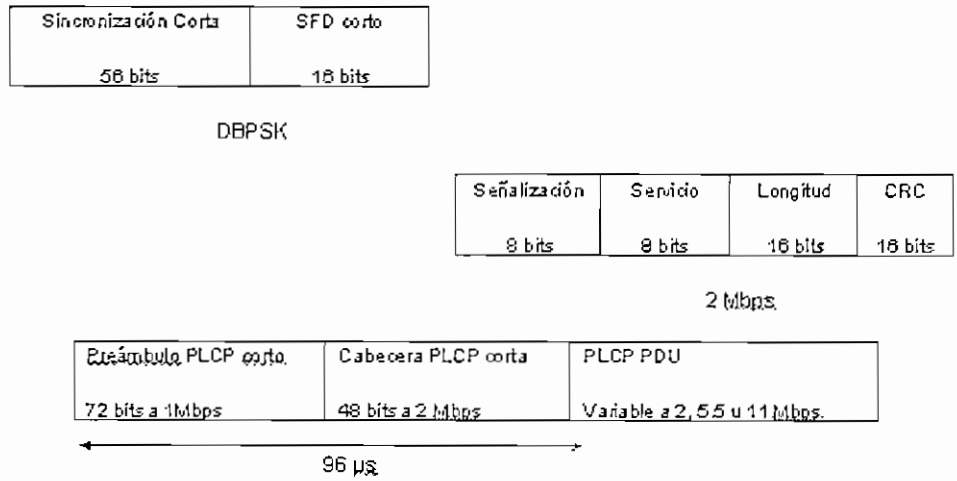



**Figura 1A.3 Trama PLCP con preámbulo corto**

Los campos que han cambiado son:

- Sincronización corta: provee mecanismos de sincronización, esta compuesto por 56 bits.
- Señalización: proporciona tres velocidades, X14 para 2 Mbps, X37 para 5.5 Mbps y X6E para 11 Mbps.

La combinación del campo Señalización y Servicio indicarán la velocidad y modulación de la trama respectivamente.

### Formato de la Trama PLCP de IEEE 802.11a

El estándar IEEE 802.11a define velocidades de hasta 54 Mbps, razón por lo cual incluye diversos mecanismos de modulación como: BPSK, 16QAM o 64QAM y codificación convolucional de tipo FEC a tasas[2] de 1/2, 2/3 o 3/4.

La trama de este estándar incluye, Preámbulo PLCP OFDM, Cabecera PLCP OFDM, PLCP PDU, bits de cola y bits de relleno.

La cabecera PLCP contiene los siguientes campos: velocidad, un bit reservado, longitud, un bit de paridad, bits de cola y bits de servicio. En términos de modulación los bits de velocidad, reservado, longitud, paridad y cola

[2] Esta tasa se conoce como R

constituyen un símbolo OFDM que forma el campo Señalización, el cual es trasmitido mediante una combinación de modulación BPSK y una tasa de codificación convolucional R=1/2.

El campo Servicio de la cabecera PLCP, el campo PLPC PDU, los bits de cola y los bits de relleno, forman el campo de Datos, el cual se transmite a la tasa descrita en el campo Velocidad y constituye varios símbolos OFDM.

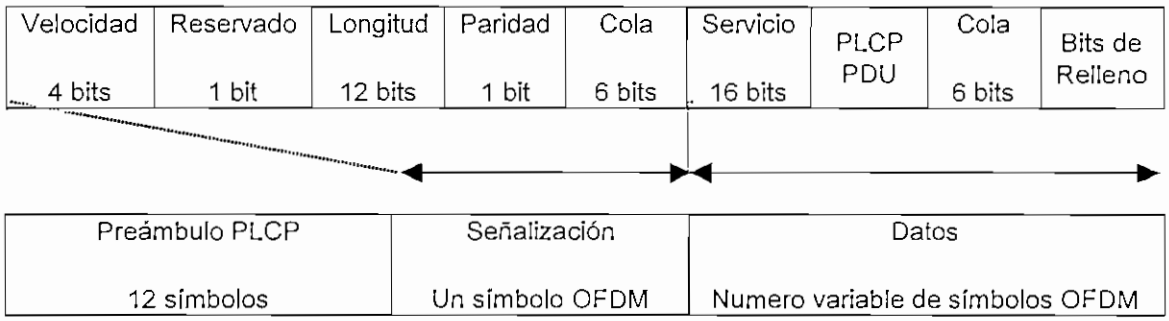



**Figura 1A.4 Detalle de la Cabecera PLCP con preámbulo corto**

El preámbulo PLCP esta compuesto por 12 símbolos, 10 de los cuales son de corta duración y los 2 restantes de larga duración; este se transmite previo a un tiempo de guardia. Cualquier dato recibido luego de los indicadores en el campo de Longitud, se consideran bits de relleno (para completar un símbolo OFDM) y se descartan. Las velocidades establecidas en el estándar se detallan como sigue:

| Velocidad (Mbps) | Tipo de Modulación |
|---|---|
| 6* | BPSK |
| 9 | BPSK |
| 12* | QPSK |
| 18 | QPSK |
| 24* | 16 - QAM |
| 36 | 16 - QAM |
| 48 | 64 -- QAM |
| 54 | 64 – QAM |

**Figura 1A.5 Velocidades para la Trama PLCP con preámbulo grande**

* Velocidades Obligatorias

**Formato de la trama PLCP para IEEE 802.11g**

Este formato de trama es el mismo que de IEEE 802.11b corto, para las velocidades de 1, 2, 5.5 y 11 Mbps, y para alcanzar velocidades adicionales se hacen las siguientes modificaciones:

- La utilización de 1 bit en el campo de Servicio para indicar cuando se utiliza el modo opcional ERP-PBCC.
- La utilización de 2 bits adicionales en el campo de Servicio para evitar ambigüedades en el uso de ERP-PBCC a 22 o 33 Mbps.
- A diferencia de la trama de 802.11b, el bit b3 se utiliza para indicar si se empleará o no ERP-PBCC a 22 o 33 Mbps; los bits b5, b6 y b7 son para evitar ambigüedad en los esquemas ERP-PBCC 11 a ERP-PBCC 33; el bit b7 indica el uso de CCK a 11 Mbps en el cual b3, b5 y b6 son seteados a cero.

La figura 1.8 muestra el campo Servicio de 802.11g.

| b0 | b1 | b2 | b3 | b4 | b5 | b6 | b7 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | Locked clocks bit.<br>0= not<br>1= locked | Mod.<br>0= No ERP-PBCC<br>1= ERP-PBCC | 0 | Extensión de longitud<br>ERP-PBCC | Extensión de longitud<br>ERP-PBCC | Extensión de longitud |

**Figura 1A.6 Campo Servicio del Preámbulo grande PLCP**[3]

En el campo Señalización se definen además tres velocidades opcionales: $XDC_H$ para 22 Mbps ERP-PBCC, $X21_H$ para 33 Mbps ERP-PBCC, $X1E_H$ para velocidades DSSS-OFDM.

[3] STALLINGS, William; *Wireless Comunication and Networks*; Prentice Hall; 2002.


ANEXO 1B

# MAPEO DE SÍMBOLOS A CHIPS EN ZIGBEE

## MAPEO DE SIMBOLOS A CHIPS

| Data Symbol (decimal) | Data Symbol (binary) ($b_0,b_1,b_2,b_3$) | Chip Values ($c_0,c_1,\ldots,c_{30},c_{31}$) |
|---|---|---|
| 0 | 0000 | 1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 |
| 1 | 1000 | 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 |
| 2 | 0100 | 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 |
| 3 | 1100 | 0 0 1 0 0 0 1 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 |
| 4 | 0010 | 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 |
| 5 | 1010 | 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 |
| 6 | 0110 | 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 |
| 7 | 1110 | 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 |
| 8 | 0001 | 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 |
| 9 | 1001 | 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 |
| 10 | 0101 | 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 |
| 11 | 1101 | 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 |
| 12 | 0011 | 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 |
| 13 | 1011 | 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 |
| 14 | 0111 | 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 0 1 1 0 0 |
| 15 | 1111 | 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 |

**Tabla 1B.1 Mapeo de símbolos a chip.**

Al transmitir por medio de una modulación O-QPSK se transmiten los chips intercalados. Los chips pares se transmiten por la fase de entrada (I) y los chips impares por la fase en cuadratura (Q) como se ve en la Figura 1B.1.

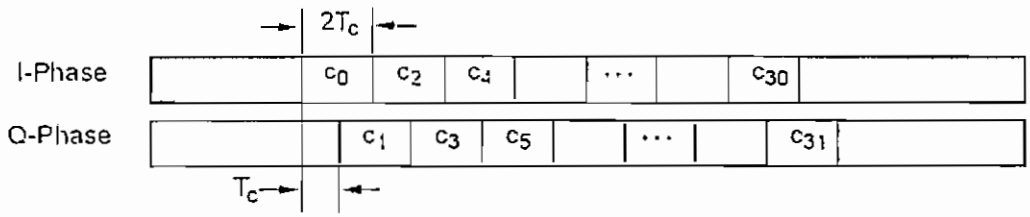



**Figura 1B.2 Transmisión de chip por medio de modulación O-QPSK**

La modulación utiliza el pulso de medio-seno. Para poder introducir el offset se retrasa en Tc los chips de la fase en cuadratura como se ve en la figura anterior. Con esto se logra una velocidad de 2 Mchips/s (Tc es el inverso de la tasa de chips).

El pulso con que se transmite se describe por la Ecuación **¡Error!No se encuentra el origen de la referencia.**. Esta modulación se puede ver en la figura 1B.2

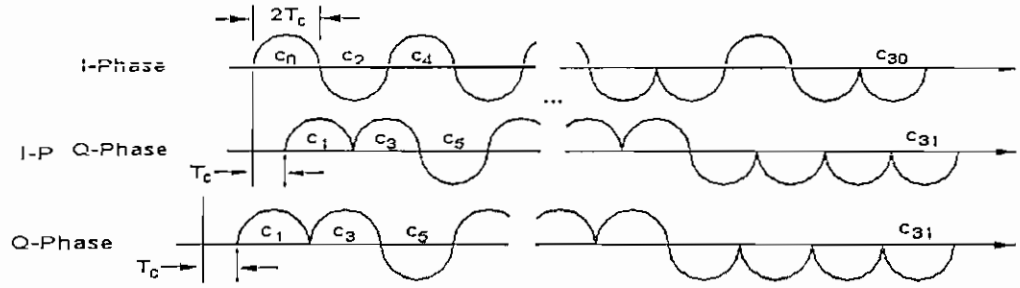



Figura1B.3 Modulación O-QPSK con pulsos de medio-seno.

$$p(t) = \begin{cases} \sin\left(\pi \frac{t}{2T_c}\right), 0 < t < 2T_c \\ 0, en\_cualquier\ otro\ caso \end{cases}$$

Ecuación (1)


ANEXO 2A

# DESCRIPCIÓN PUERTO PARALELO DEL SENSOR MTS300/310

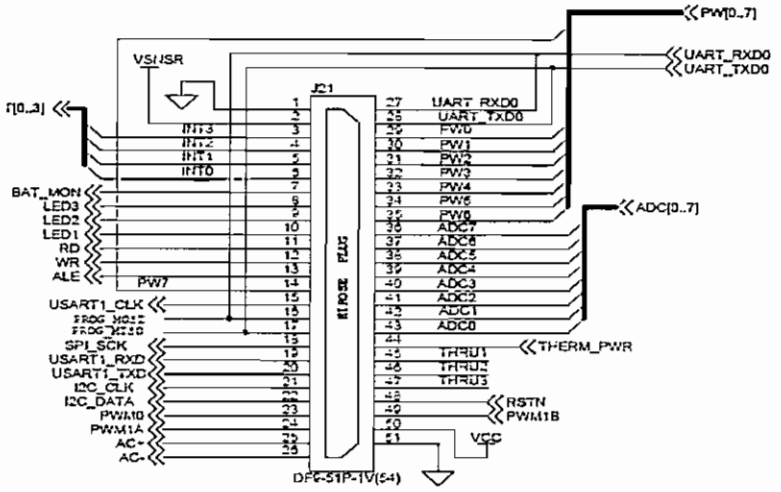



**Fig 2A.1 Puerto Paralelo del sensor MTS300/310**

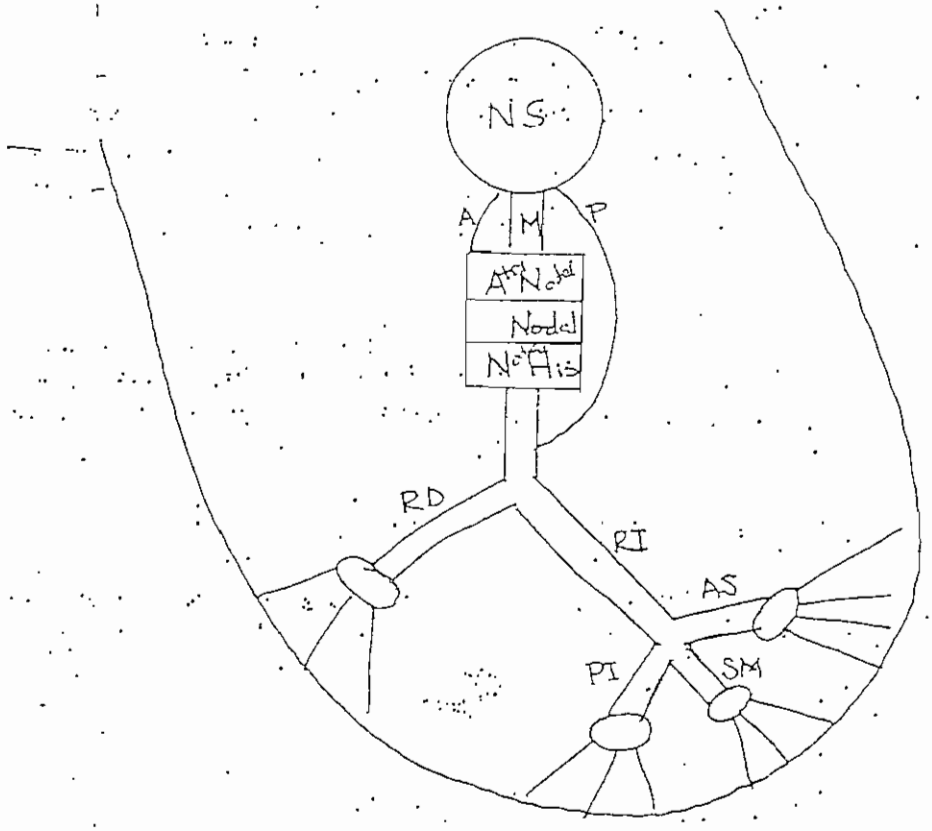
| PIN | Nombre | Descripción |
|---|---|---|
| 1 | GND | Tierra |
| 2 | VSNSR | Alimentación Voltaje de Sensor |
| 3 | INT 3 | GPIO |
| 4 | INT 2 | GPIO |
| 5 | INT 1 | GPIO |
| 6 | INT 0 | GPIO |
| 7 | BAT_MON | Habilita el monitor del voltaje de la batería |
| 8 | LED 3 | LED 3 |
| 9 | LED 2 | LED 2 |
| 10 | LED 1 | LED 1 |
| 11 | RD | GPIO |
| 12 | WR | GPIO |
| 13 | ALE | GPIO |
| 14 | PW 7 | Control de Potencia 7 |
| 15 | USART1_CLK | Reloj USART1 |
| 16 | PROG_MOSI | Programa Serial MOSI |
| 17 | PROG_MISO | Programa Serial MISO |
| 18 | SPI_SCK | Reloj Seria SPI |
| 19 | USART1_RXD | Recepción de Datos USART1 |
| 20 | USART1_TXD | Transmisión de Datos USART1 |
| 21 | I2C_CLK | Bus del Reloj I2C |
| 22 | I2C_DATA | Bus de Datos I2C |
| 23 | PWM0 | GPIO / PWM0 |
| 24 | PWM1A | GPIO / PWM1A |
| 25 | AC + | GPIO / AC + |
| 26 | AC - | GPIO / AC - |

**Tabla 2A.1 Descripción de Pines del Sensor MTS300/310**


ANEXO 2B

# PATRONES DE PULSO Y RITMO CARDÍACO

rama posteroinferior (P.I). y en un pequeño porcentaje que no llega al 40% hay un fasciculo llamado septal medio (S.M).




El latido cardiaco se origina en el nódulo sinusal de este a través de tres haces se comunica con el nódulo auriculoventricular: Hay un haz anterior o de Torel, un haz medio o de Venkebag y un haz posterior o de James. El impulso cardiaco normal se produce por el haz medio o de Venkebag.. Cuando pasa por el haz anterior o por el haz posterior, no es normal constituyendo así lo que se llama el sistema de pre-exitación o Wolf Parkinson Wuif, que ya implica una patología.

El nódulo sinusal está ubicado en la aurícula derecha, para pasar a la aurícula izquierda lo hace a trabes del haz de Bachman y si hubiera un disturbio de conducción intraauricular o interauricular quiere decir que este haz de Bachman está dañado.

El nódulo auriculoventricular tiene tres partes, la llamada parte *atrionodal, nodal o funcional y nodal His.* Este nódulo A.V se está comunicando con el tronco del haz de His, esta parte troncular del haz de His va por encima de la porción membranosa del septo interventricular, penetra aquí y da sus dos ramas, la llamada rama derecha y la llamada rama izquierda. La rama derecha es una rama única de un trayecto subendocardico y que termina en la base del músculo papilar anterior del ventrículo derecho y de aquí da varias ramas hasta la pared de los ventrículos anterior, media y posterior, es decir la rama derecha desde su inicio hasta que se inserta no da otras ramas. La rama izquierda en cambio en el anillo fibroso que se constituye o que se forma por la unión de la mitral con la aorta se divide en sus dos ramas, la anterosuperior que va hasta el músculo papilar anterior del ventrículo izquierdo y la posteroinferior que va hacia el músculo papilar posterior del ventrículo izquierdo. En el 40% hay una tercera rama llamada rama septal media cuya presencia o ausencia no representa ruptura del fisiologismo es decir no implica patologia cardiaca alguna. De aquí de los músculos papilares dan varias ramificaciones hacia el músculo ventricular.

¿Por qué si hay tres nódulos, solo se manifiesta uno?. Existe un mecanismo de inhibición selectiva ante las más altas frecuencias. Ej: Si el nódulo sinusal esta latiendo a 80 x min. El momento en que quiere el nódulo AV latir a 50 x min. no le da tiempo y ya se produce una nueva despolarización del nódulo sinusal. es decir hay un mecanismo que en ingles es Over Dravf Süpretion. este mecanismo suprime las frecuencias más altas a las frecuencias más bajas, inhibiendo su presentación como latido cardiaco. es por esto que siempre se tiene un estímulo sinusal. excepto que se deprima o deje de funcionar el nódulo sinusal, solo en este evento asume su acción el siguiente foco. en este caso el nódulo AV y si eventualmente deja de funcionar el nódulo AV asume su acción el siguiente foco que es el músculo ventricular.

El que ninguno de estos mecanismos funcione nos lleva a pensar que el paciente fallezca, actualmente se puede evitarlo mediante el implantamiento de marcapasos definitivo que toman su función. ahora existen incluso los llamados marcapasos bicamerales, es decir que un estimulo esta en auriculas y el otro esta en ventrículos dándole un latido exactamente y casi fisiológico por parte del equipo.

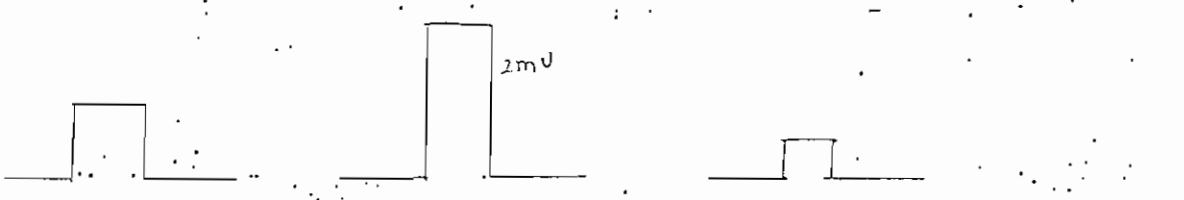
Es necesario manejar dos termino, la llamada bradicardia y la llamada taquicardia. Cuando el estímulo es sinusal y la frecuencia está entre 60 y 100 esto es lo normal, pero bajo 60 es una bradicardia sinusal y sobre 100 es una taquicardia sinusal, con el foco en el nódulo AV bajo 40 será una bradicardia AV o una taquicardia nodal AV si está sobre 59, con estimulo en ventrículos bajo 20 será una bradicardia ventricular y sobre 39 será una taquicardia ventricular.

El diagnostico de donde esta el foco de estimulación es electrocardiográfico. Los bloqueos cardiacos se refieren a la alteración en la conducción. Cuando esta alteración o retrasamiento en la conducción entre el nódulo sinusal y el nódulo AV es el bloqueo AV de primer grado, cuando esta bloqueada la conducción por la rama derecha es el bloqueo de rama derecha, cuando esta bloqueada la conducción por la rama izquierda es el llamado bloqueo de rama izquierda, si la alteración es por el anterosuperior es el bloqueo anterosuperior o es el bloqueo posteroinferior cuando esta bloqueada la rama posteroinferior o el bloqueo septal medio. Si existen dos bloqueos, es un bloqueo bifasicular o con tres bloqueo es trifasicular.

En cuanto a la innervación, el parasimpático inerva el nódulo sinusal y el nódulo AV, y el simpático predominantemente a los ventrículos, un estimulo vagal o parasimpático libera acetilcolina esta tiene una acción depresora en el sistema de His Purkinge, consecuentemente disminuyen la frecuencia de descarga del nódulo sinusal provocando bradicardia, disminuye la, contractilidad del nódulo
Y la acción fisiológica es por que permite una rápida salida de potasio.

Lo contrario. el estimulo simpático libera adrenalina y noradrenalina, la acción del simpático en el sistema de His Purkinge es estimulante de sus funciones intrínsecas, aumentará la frecuencia del nódulo sinusal consecuentemente puede producir taquicardia, aumenta la contractilidad cardiaca y aumenta la frecuencia o la velocidad de la transmisión del impulso en todo el sistema de His Purkinge. el efecto es por un aumento de la permeabilidad al sodio. El estimulo simpático generalmente va asociado de arritmias cardiacas ligadas a taquicardia, como puede ser una fibrilación.

la calibración es a *2N*. pero puede darse lo contrario que haya un gran crecimiento cavitario y las ondas serán muy grande. para esto se calibra el equipo a *N/2* que se logra reduciendo a 0.5 mV la calibración del equipo. o sea a la mitad de lo normal(1 mV)




*N* o normal

1 mV

*2N*

Cuando son pequeñas y la ganancia del

*N/2*

cuando las ondas son demasiado grandes

Todos los cálculos tienen que hacerse en *N*, si se calibra a *2N* para ver cuanto dura y cuanto mide una onda el resultado se debe dividir para dos y. si los cálculos se hace en *N/2* el resultado se habrá que multiplicar por dos o aumentar el doble.

La velocidad normal en la toma de un E.K.G. es a 25 mm/sg, para efectos de electrofisiologia se puede aumentar a 50 o 100 mm/sg. Pero normalmente todo E.K.G. debe tomarse a 1 mV de calibración y a 25 mm de velocidad.

Para proceder a tomar el E.K.G. se colocan los electrodos en las cuatro extremidades. *Einthoven,* la persona que ideó la lectura y la toma del E.K.G. consideró que el organismo es un circuito eléctrico serrado y puso electrodos en las cuatro extremidades. aVR en brazo derecho, aVL en brazo izquierdo. aVF en pierna izquierda y para cerrar el circuito eléctrico también hay un electrodo en la pierna derecha. Es necesario que el paciente este tranquilo, se coloca gel o alcohol para quitar la resistencia de piel en las 4 extremidades, es preferible solicitarle a la persona que se quite todo lo que tenga de metal (joyas, relojes, monedas, llaves, etc) por que como es un sistema muy sensible podría alterar y dar vibración cuando el paciente está con muchas cosas de metal. Colocamos en las 4 extremidades y procedemos primero a la calibración tanto de *N* como de la velocidad y allí se toma el electro.

Las derivaciones son de tres tipos: las llamadas *Unipolares, bipolares y precordiales.*

Las derivaciones *Unipolares* como su nombre lo indica captan la diferencia potencial en cada una de las extremidades: habrá derivación unipolar aVR, aVL y aVF. Una característica especial de estas derivaciones es que donde captan la diferencia de potencial el vector es siempre positivo y el otro lado será negativo.

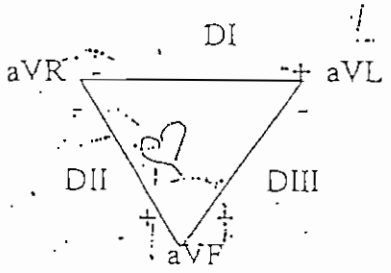



Fig. 1

Entre las anteriores derivaciones tenemos las llamadas *derivaciones bipolares* que captan las diferencias de potencial entre las dos extremidades, se las nombran con las letras DI, DII y DIII

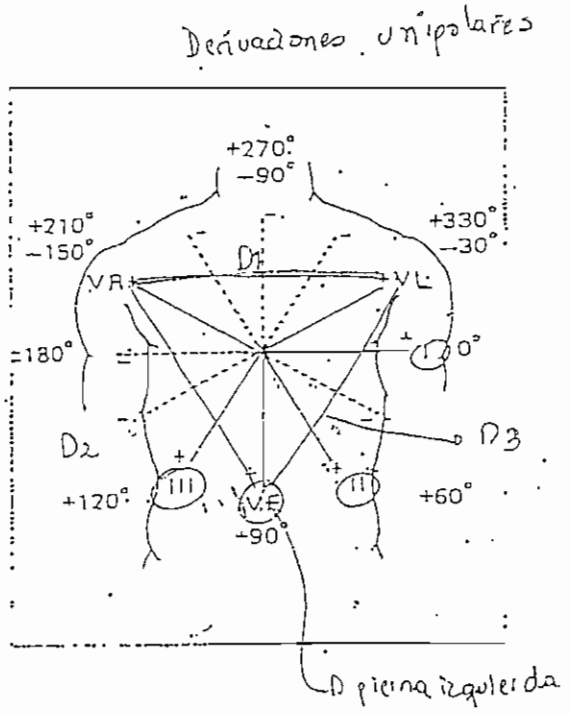
Para aprender a leer un electrocardiograma normal, se debe cumplir 4 fases o 4 subestudios:

El análisis de las ondas.
El diagnostico de la frecuencia cardiaca.
El diagnostico del ritmo cardiaco.
El diagnostico del eje eléctrico.

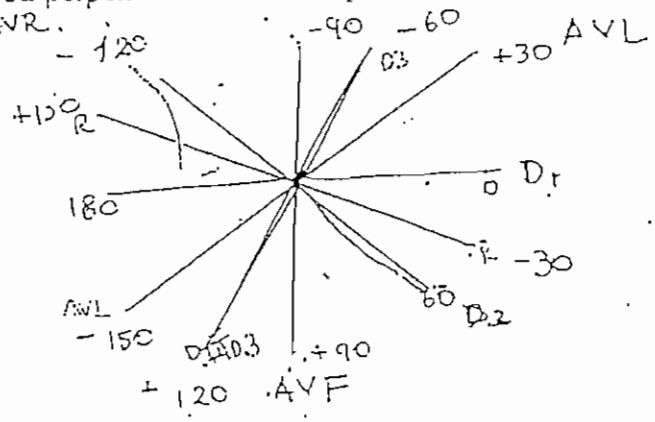
Diagnostico del eje eléctrico. El eje eléctrico normal máximo va entre –30 hasta +120 de la orientación de los ventriculos. Este eje esta orientado hacia la izquierda. Para su estudio se debe observar el llamado sistema Exaxial dividiendo a los 360 grados en 180 hacia arriba y 180 hacia abajo. la mitad inferior es siempre positiva y la mitad superior es siempre negativa. Cada unipolar esta ubicada en perpendicularidad con una bipolar así:

| | | |
|---|---|---|
| DI | - | aVF |
| DII | - | a VL |
| DIII | - | aVR |

Con lo anteriormente repasado podemos dibujar el sistema exaxial.

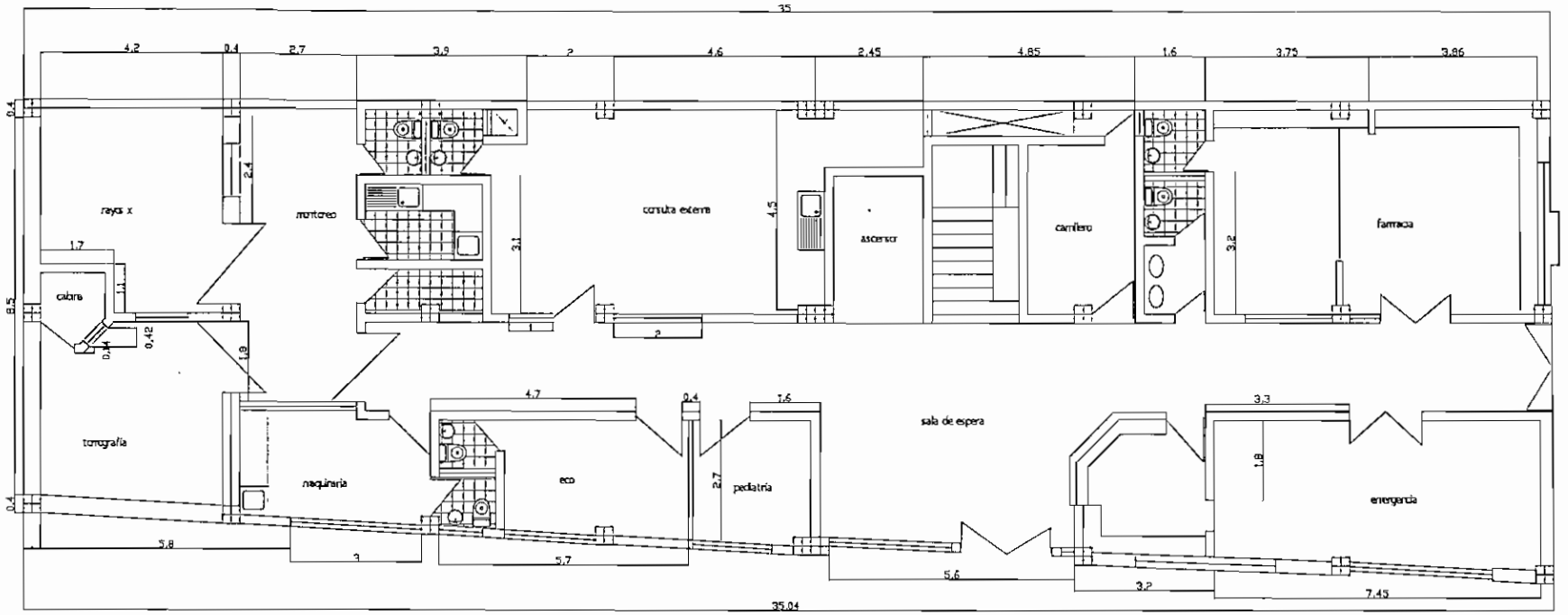



DI es positivo y va de 0 a +180, la perpendicular de DI (que hace ángulo de 90 grados) es aVF que va de +90 a –90. cada 60 grados hay una nueva bipolar en este caso DII que abajo es positiva o sea que va de +60 a –120. su perpendicular es aVL que es positiva por eso va de +30 a –150, nuevamente 60 grados y habrá una derivación bipolar DIII que abajo es positivo o sea que va de +120 hasta –60. su perpendicular es aVR que será de +150 hasta –30. Así se construye el sistema exaxial.




ANEXO 2C

# PLANOS DE LA EDIFICACIÓN

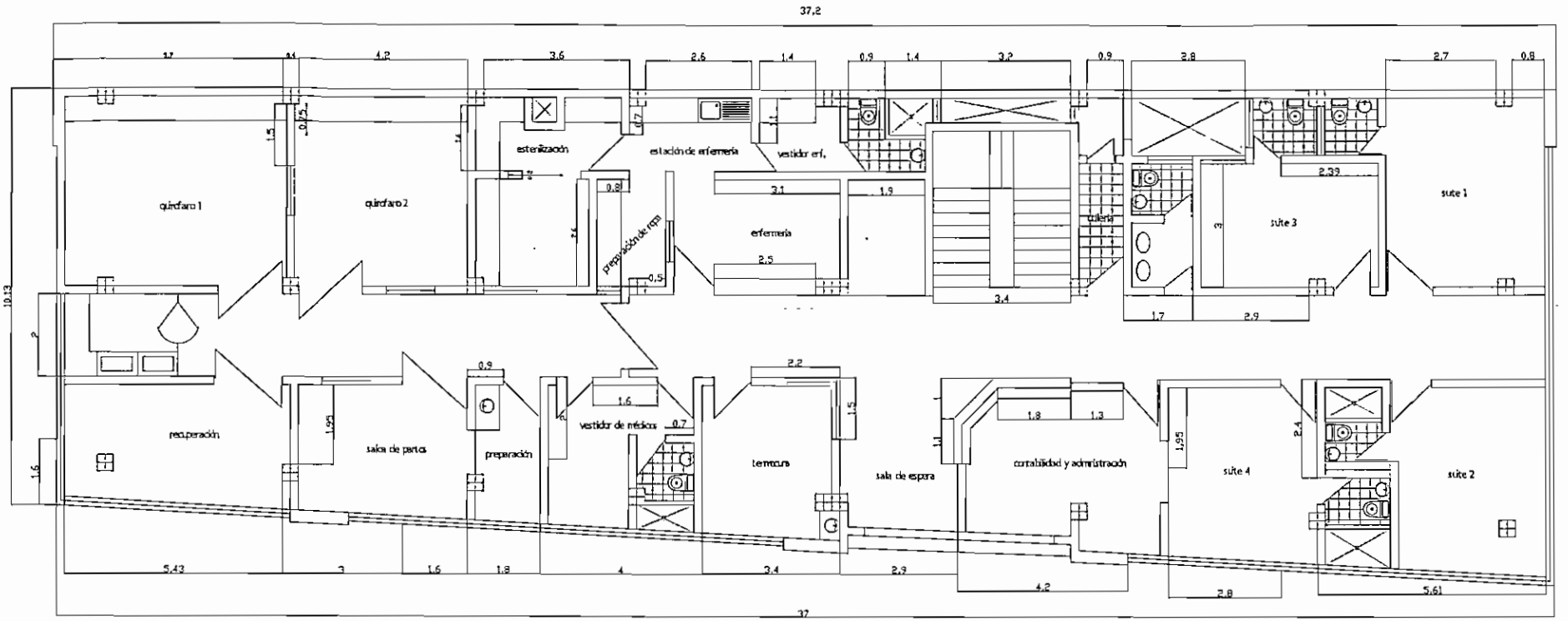



CABILDEO ESTRUCTURADO

CLINICA
DURAN

| | |
|---|---|
| CLAVE CATASTRAL | PREDIO A |
| UBICACION | Av. Pastor e Italia |
| CONTENIDO | – PLANTA BAJA |
| LAMINA | 7 |
| PROYECTISTA I | |
| PROYECTISTA II | |
| FECHA | OCTUBRE / 2006 |
| ESCALA | H |

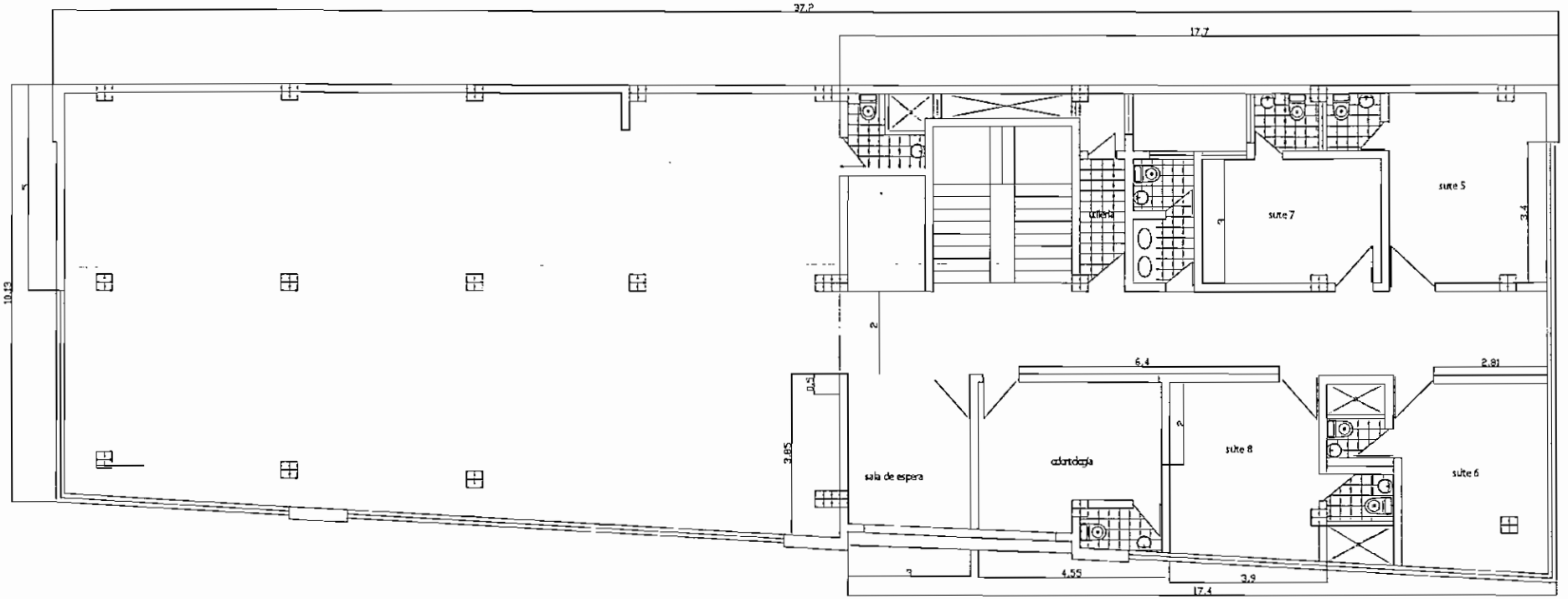
OBSERVACIONES




CLINICA DURÁN

| | |
|---|---|
| CLAVE CATASTRAL | PREDIO # |
| UBICACIÓN: Av. Pasteur e Italia | |
| CONTIENE: - PRIMER PISO | LÁMINA: 2 DE 4 |
| PROYECTISTA 1: LAURA GUZMÁN | PROYECTISTA 2: JAIDER MORAN |
| FECHA: OCTUBRE / 2014 | ESCALA: 1/100 |

OBSERVACIONES:




CABILDO ESTRUCTURADO

CLINICA DURAN

CLAVE CATASTRAL: PREDIO #:

UBICACION: Av. Pasteur e Italia

CONTIENE: - SEGUNDO PISO

LAMINA: 3

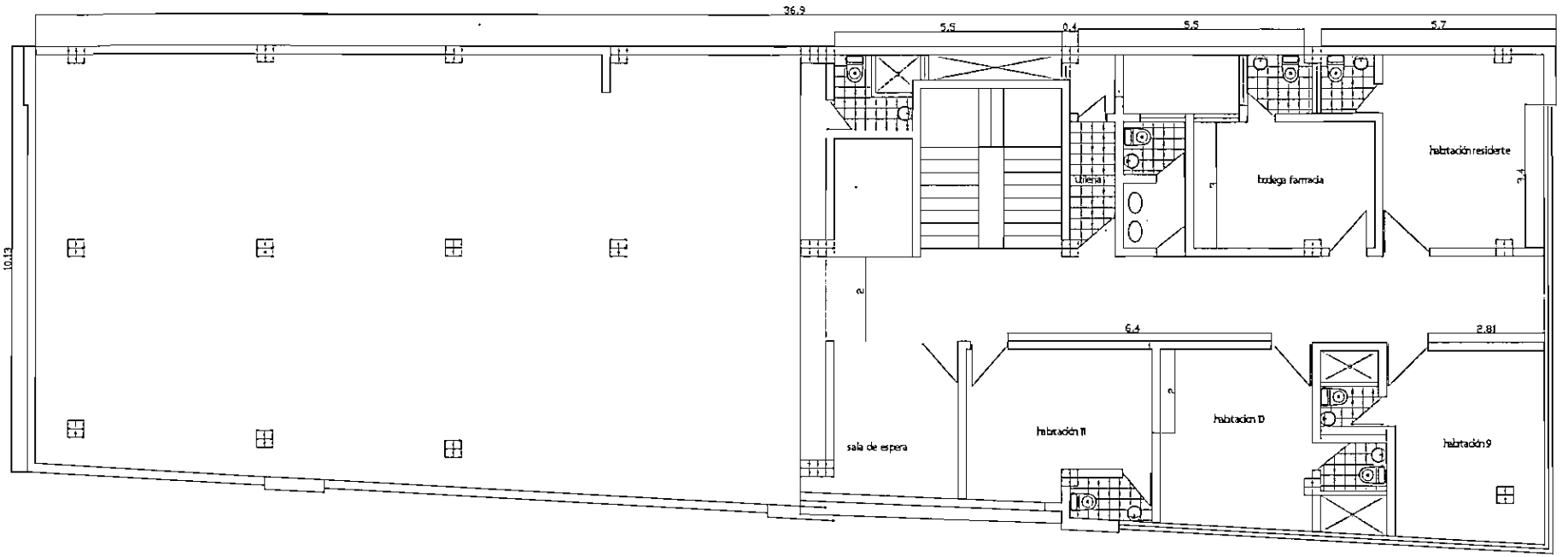
PROYECTISTA 1: DARIA GLEIMER

PROYECTISTA 2: JAIRO PRADO

FECHA: OCTUBRE / 2004

ESCALA: M

OBSERVACIONES:




CALIDAD ESTRUCTURADO

CLINICA
DURAN

CLAVE CATASTRAL: PREDIO P-

UBICACIÓN: Av. Pasteur e Italia

CONTIENE:
- TERCER PISO

LAMINA: 4

PROYECTISTA 1: KARINA QUIÑONEZ

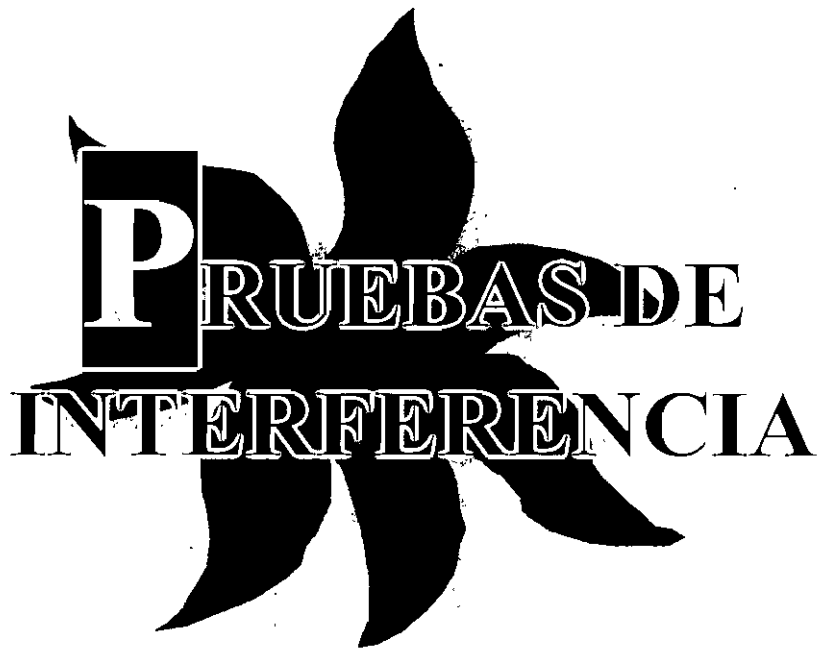
PROYECTISTA 2: JASMIN PRADO

FECHA: OCTUBRE / 2014

ESCALA: S/E

OBSERVACIONES:


ANEXO 2D


PRUEBAS DE
INTERFERENCIA

## Primer Piso

| NORTE | | | SUR | | |
|---|---|---|---|---|---|
| Red | Canal | V (Mbps) | Red | Canal | V (Mbps) |
| | | | EMAPA 03 | 6 | |
| | | | SPEEDY | 5 | |
| | | | PLASTIWAN | 11 | |
| | | | BELKIN54G | 2 | |

Tabla 2B.1 Redes Inalámbricas cercanas al Primer Piso por Norte y Sur

| ESTE | | | OESTE | | |
|---|---|---|---|---|---|
| Red | Canal | V (Mbps) | Red | Canal | V (Mbps) |
| EMAPA 03 | 6 | | EMAPA 03 | 6 | |
| SPEEDY | 3 | | | | |
| FREEDOM | 2 | | | | |
| WAVELAN | 8 | | | | |
| PLASTIWAN | 11 | | | | |
| CEN | 8 | | | | |
| BELKIN54G | 2 | | | | |

Tabla 2B.2 Redes Inalámbricas cercanas al Primer Piso por Este y Oeste

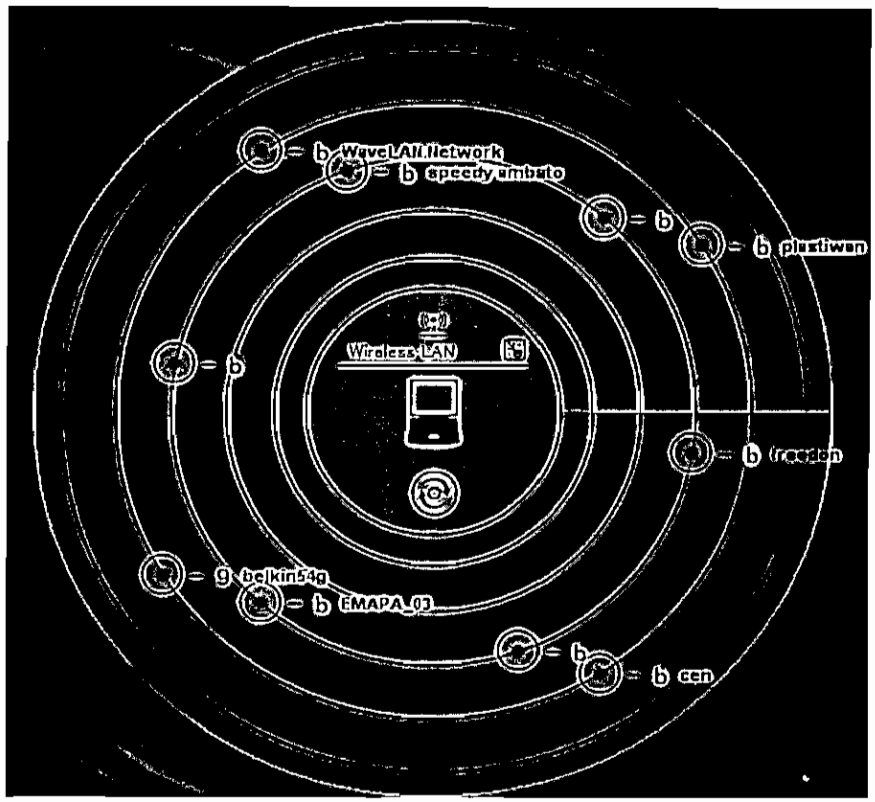



Figura a: Norte

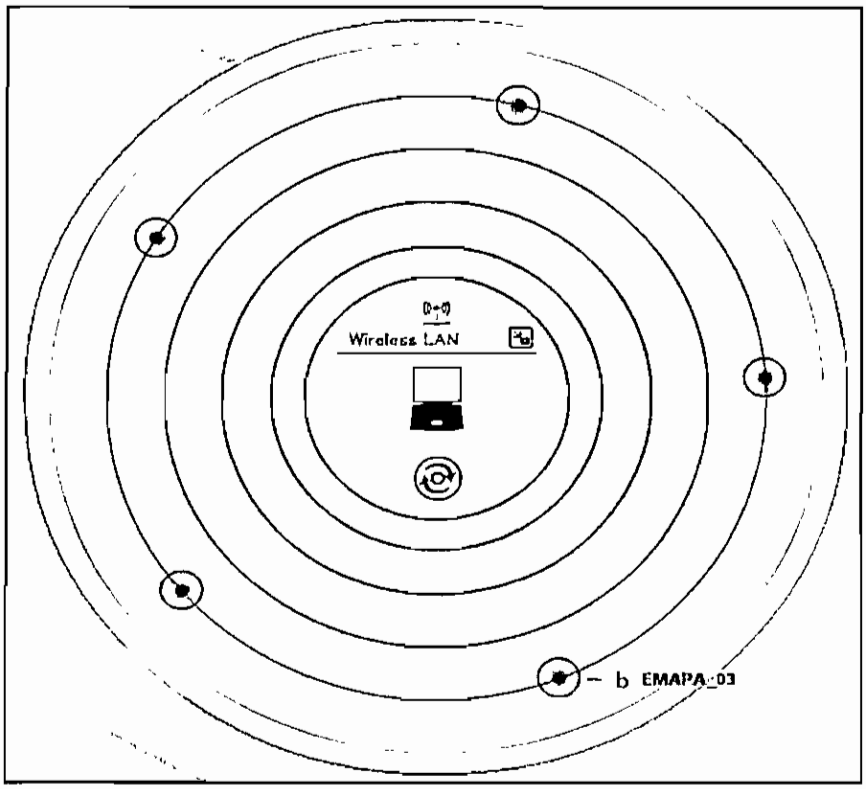



Figura b: Sur

## Segundo y Tercer Piso

| NORTE | | | SUR | | |
|---|---|---|---|---|---|
| Red | Canal | V (Mbps) | Red | Canal | V (Mbps) |
| EMAPA 03 | 6 | | | | |
| PLASTIWAN | 11 | | | | |
| EMAPA 01 | 5 | | | | |
| FREEDOM | 2 | | | | |

Tabla 2B.3 Redes Inalámbricas cercanas al 2do y 3er Piso por Norte y Sur

| ESTE | | | OESTE | | |
|---|---|---|---|---|---|
| Red | Canal | V (Mbps) | Red | Canal | V (Mbps) |
| EMAPA 03 | 6 | | EMAPA 03 | 6 | |
| SPEEDY | 3 | | PLASTIWAN | 11 | |
| EMAPA 01 | 5 | | EMAPA 01 | 5 | |
| WAVELAN | 8 | | FREEDOM | 2 | |
| FREDOOM | 211 | | | | |

Tabla 2B.4 Redes Inalámbricas cercanas al 2do y 3er Piso por Este y Oeste

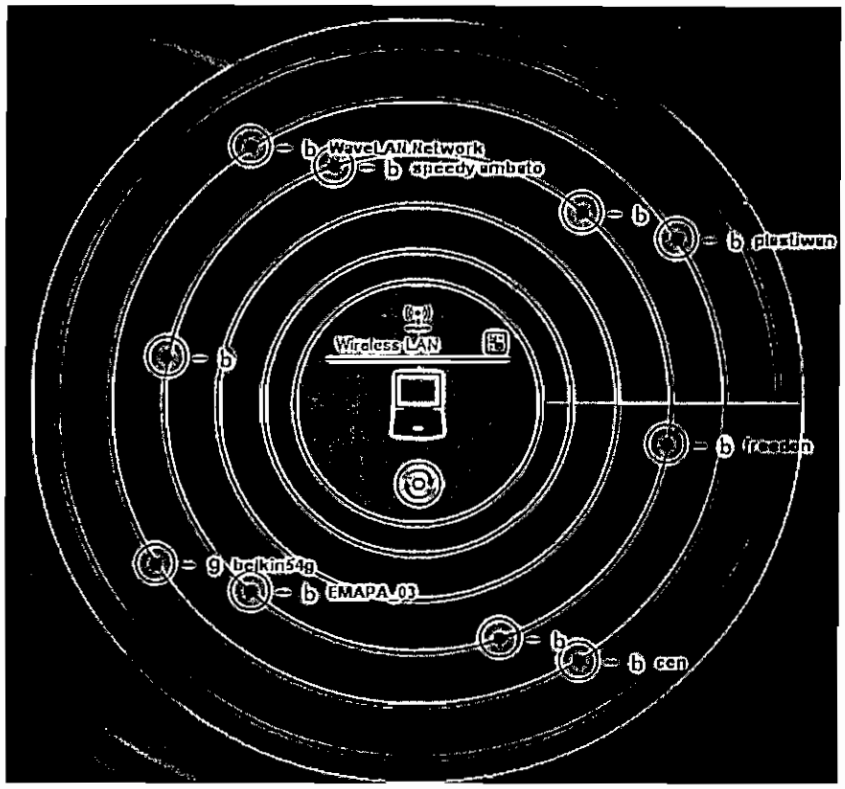



Figura a: Este

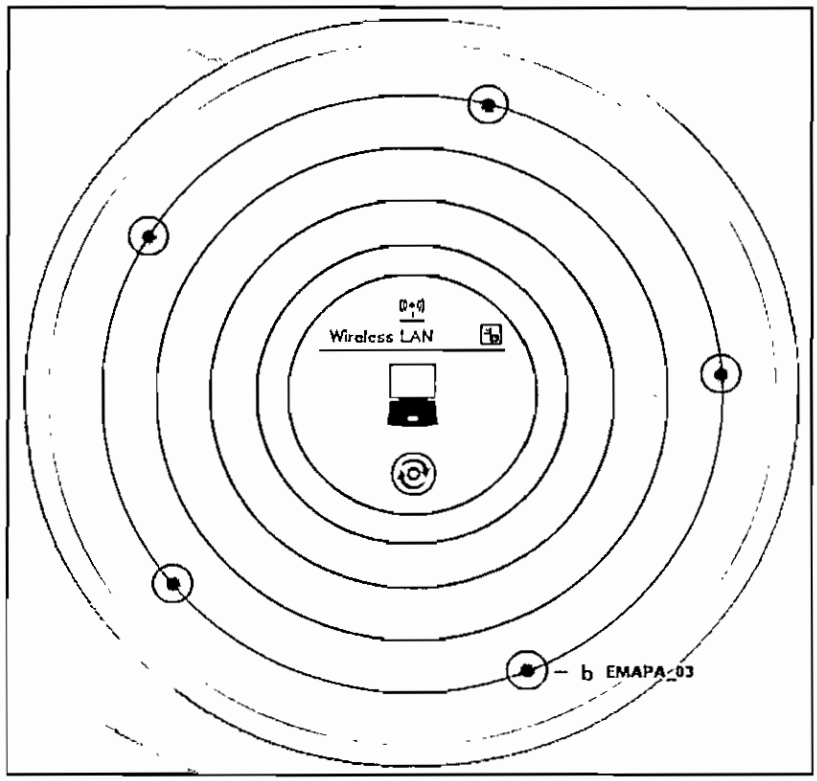


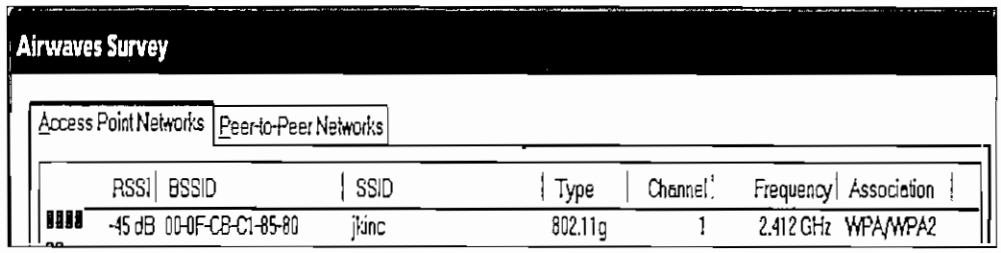

Figura b: Oeste


ANEXO 2E

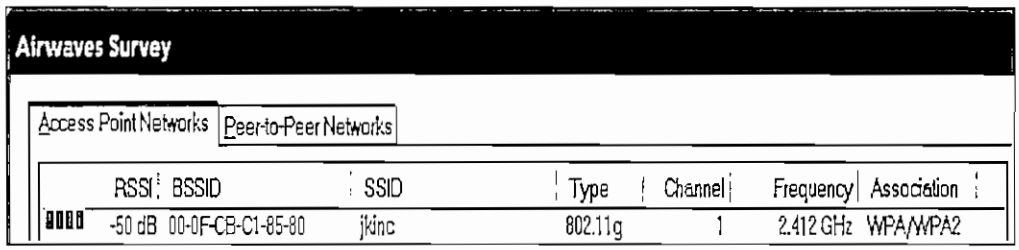
# PRUEBAS DE CALIDAD DE SEÑAL

## Planta Baja

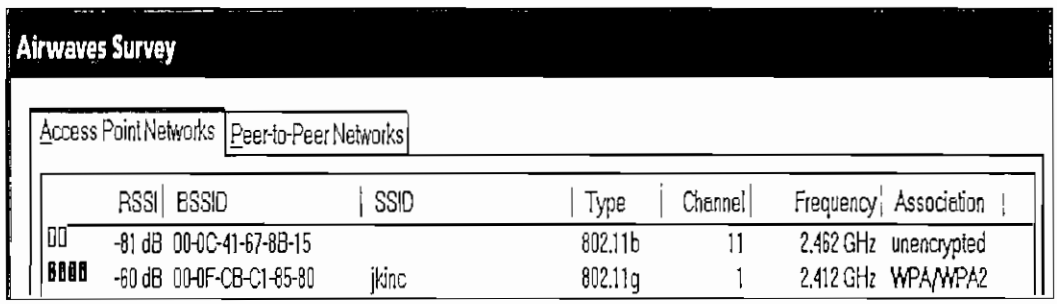
- Emergencia



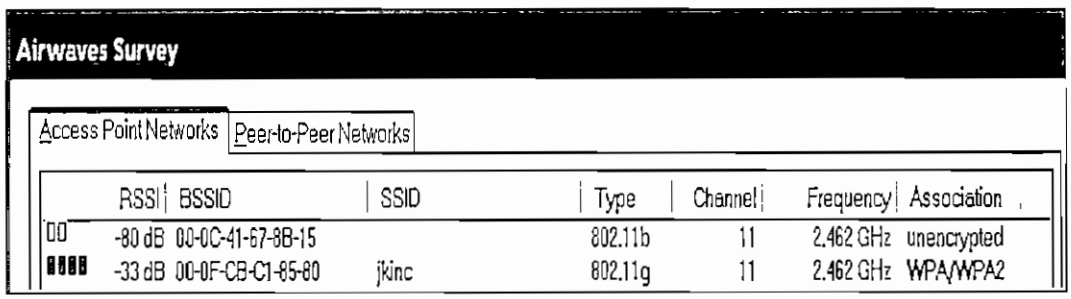

- Farmacia



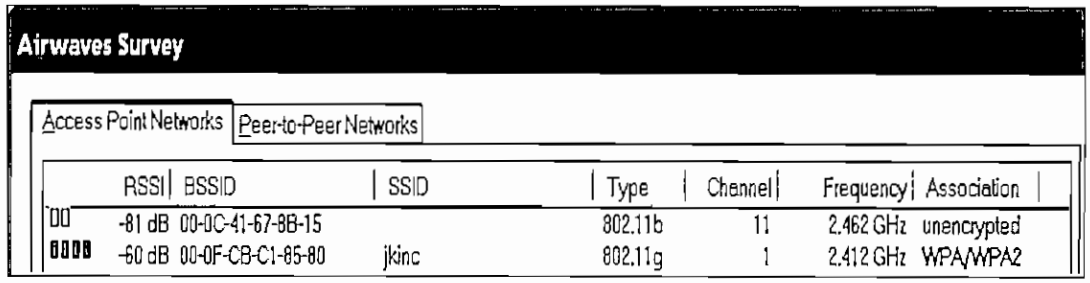

- Información



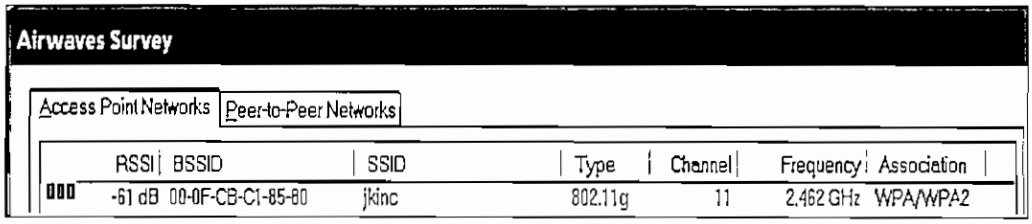

- Sala de Espera



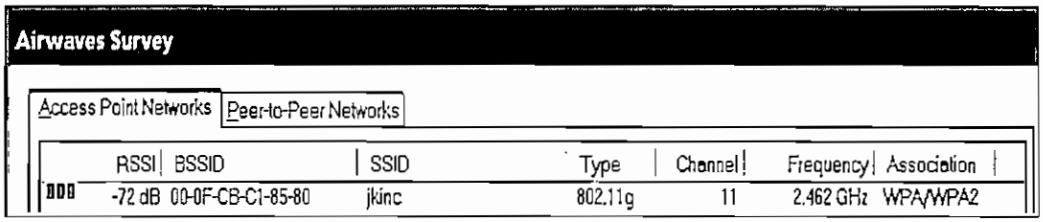
- Pediatría

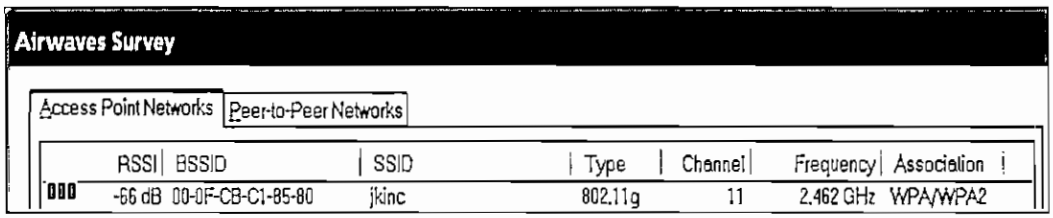



- Eco

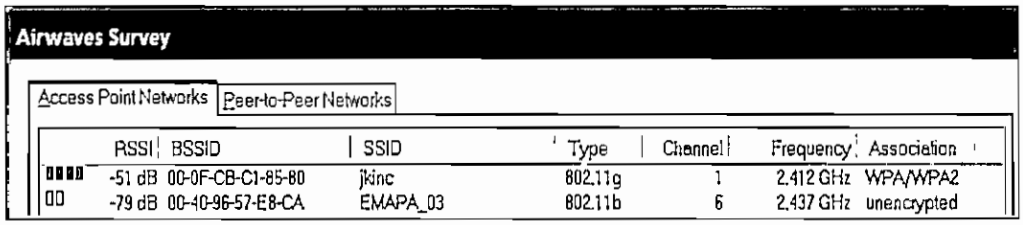



- Consulta Externa



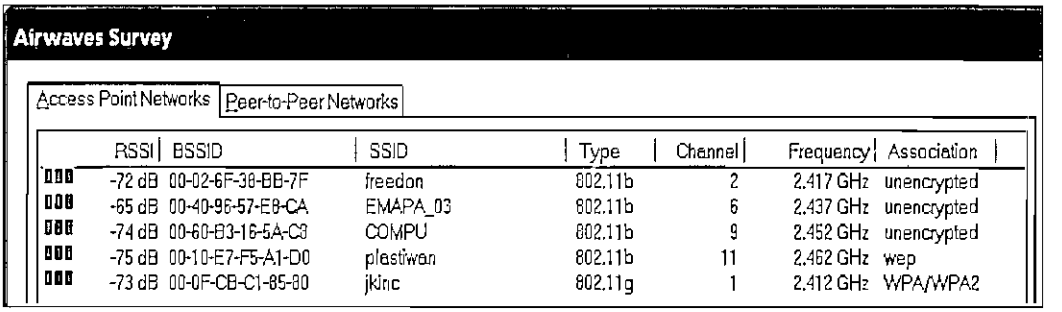




- Tomografía y Rayos X

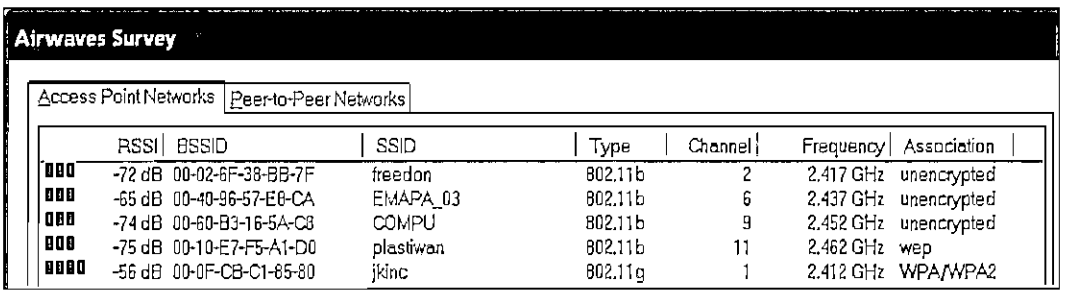


## Primer Piso

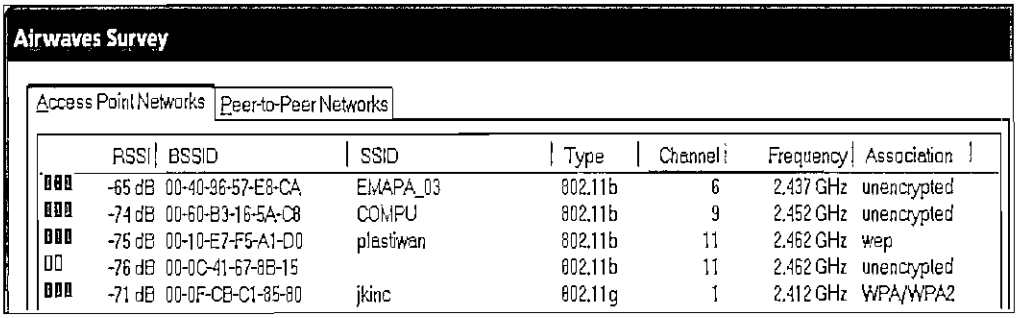
- Suite 1



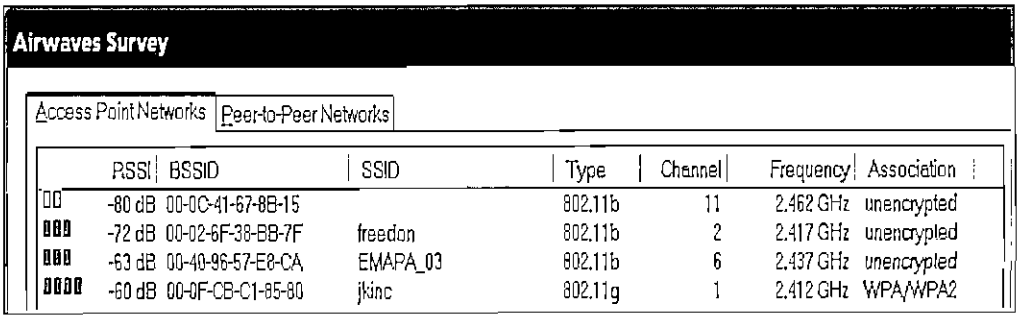

- Suite 2



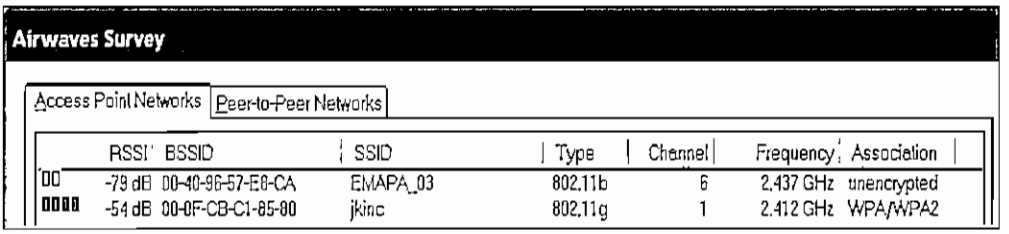

- Suite 3

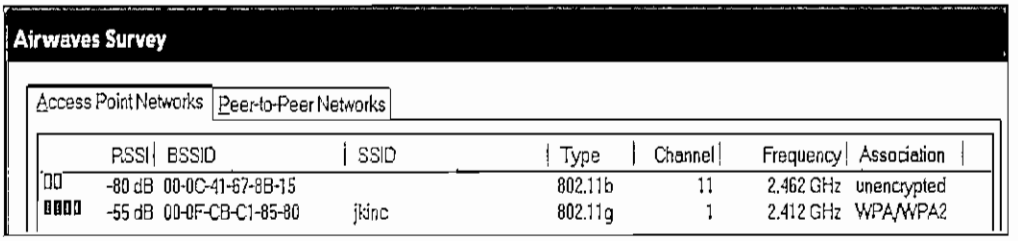



- Suite 4

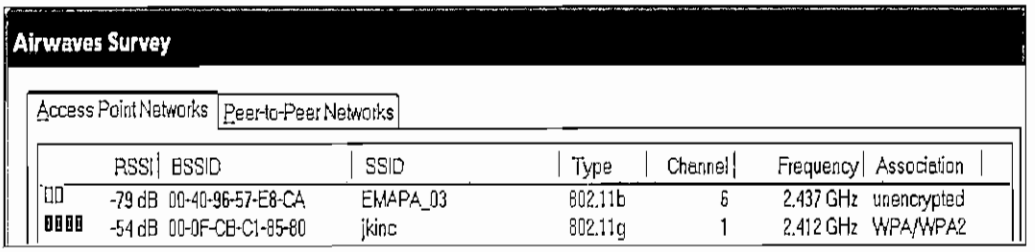


- Contabilidad y Administración

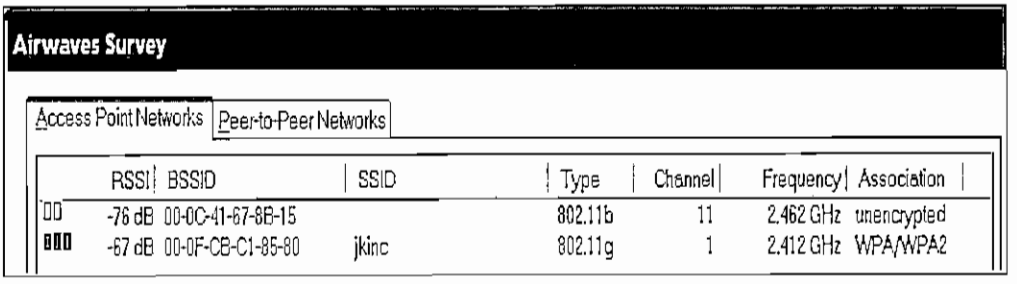


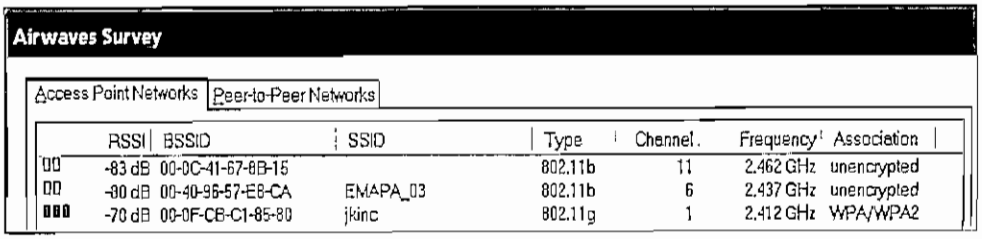

- Sala de Espera



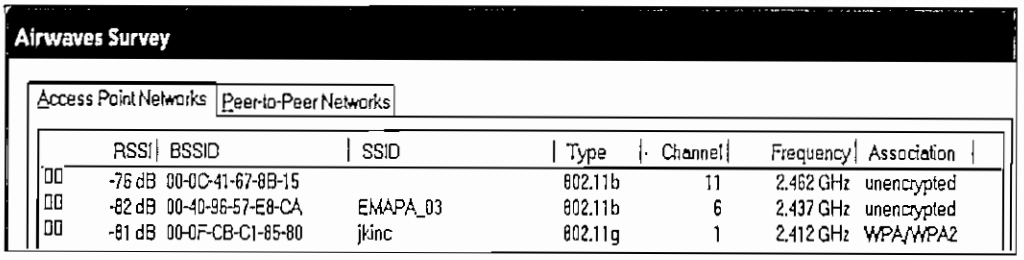

- Enfermería



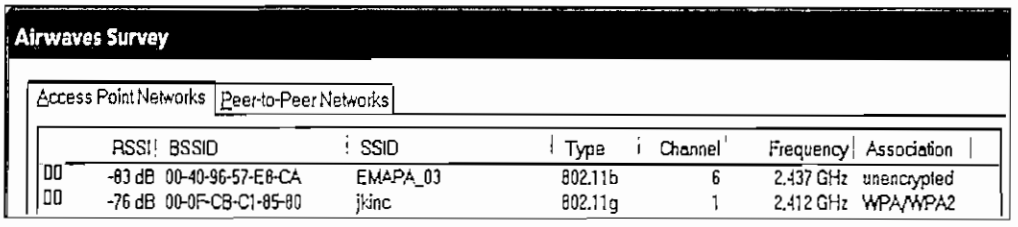

- Termo cuna



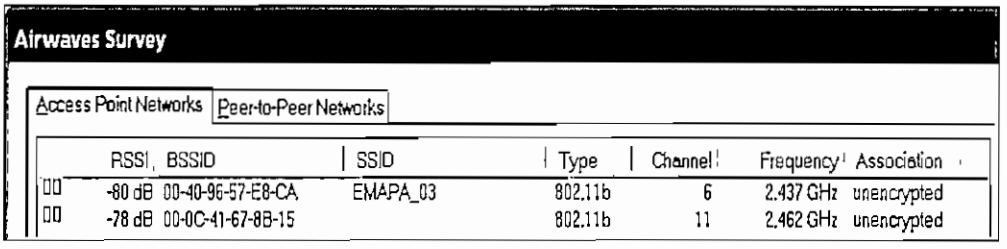
- Esterilización




- Preparación de Ropa

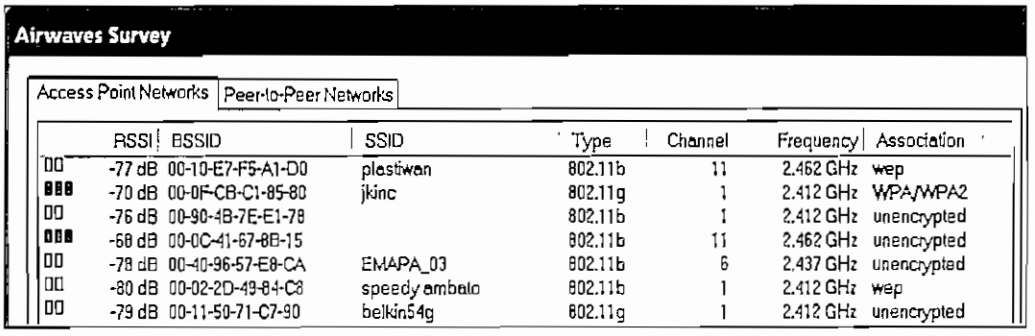



- Sala de Partos, Quirófanos y Recuperación

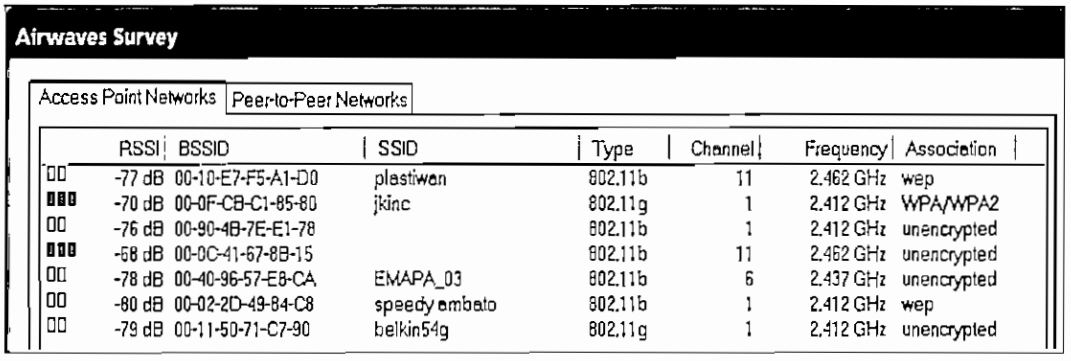



Segundo Piso

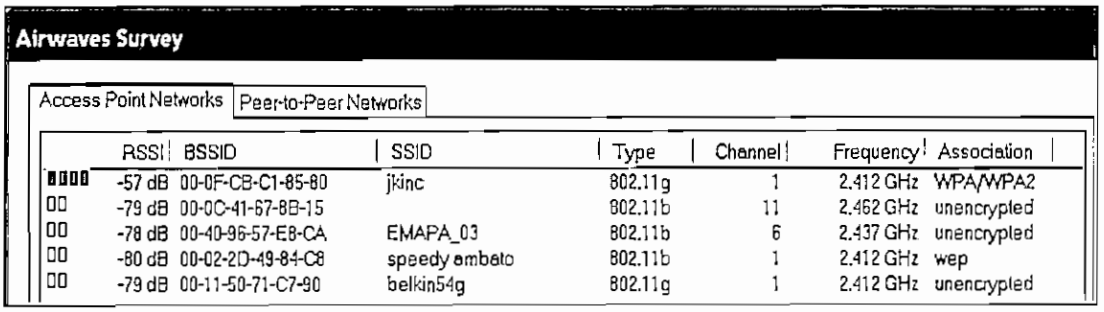
- Suite 5



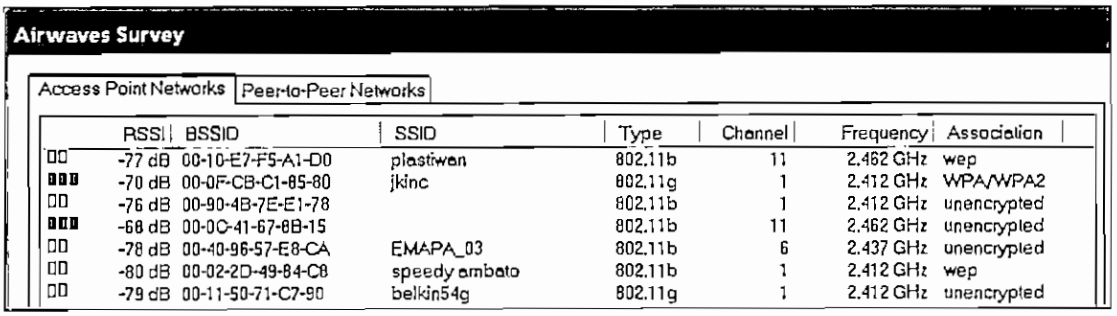
- Suite 6



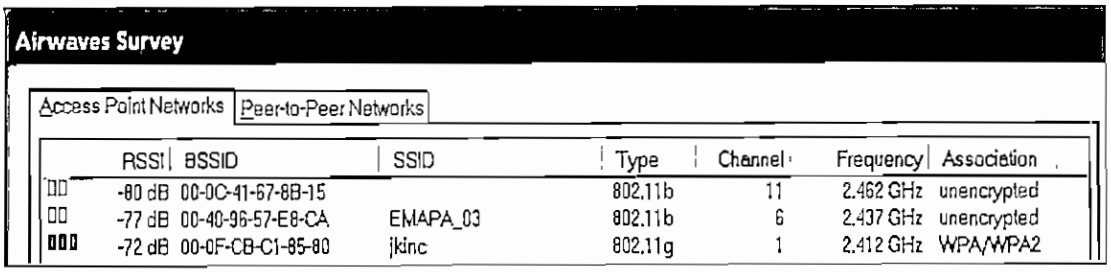

- Suite 7



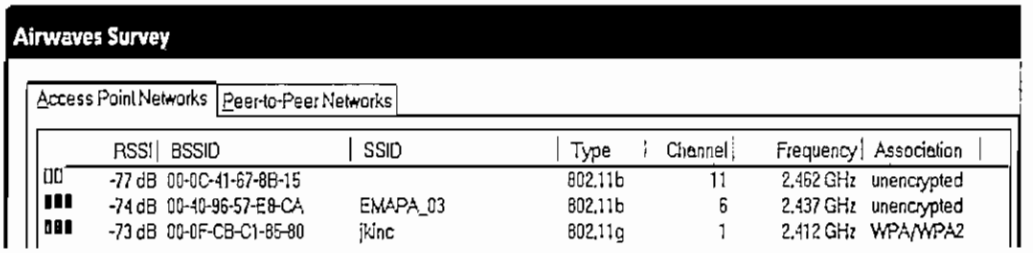

- Suite 8




- Odontología

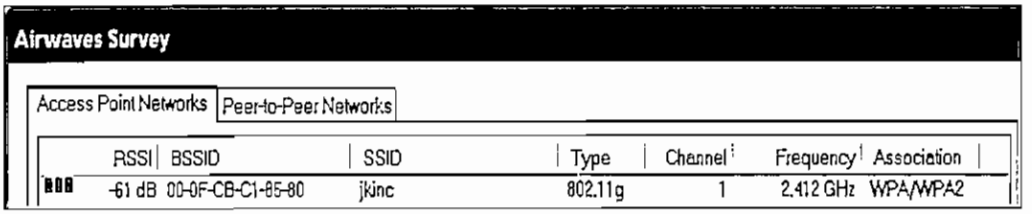


- Sala de Espera

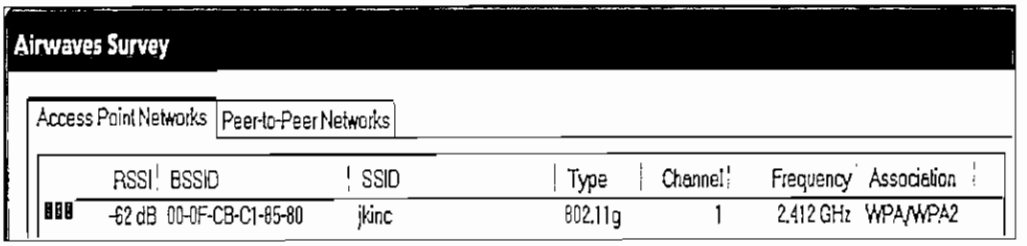



Tercer Piso

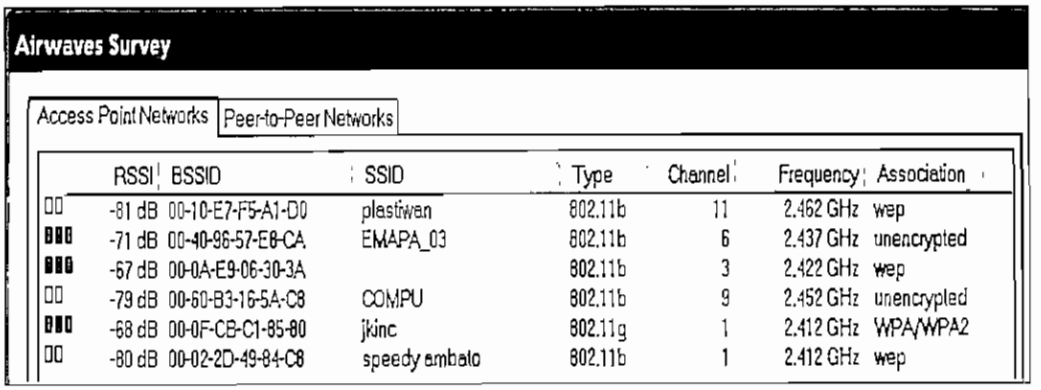
- Habitación 9



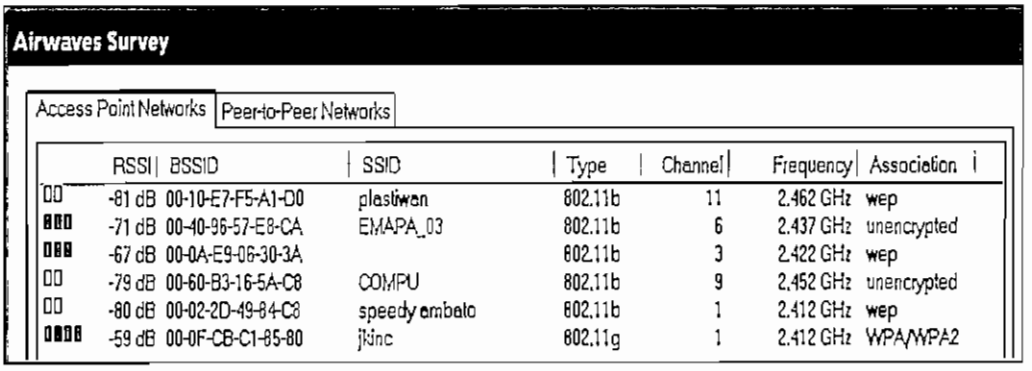

- Habitación 10




- Habitación 11



- Bodega Farmacia

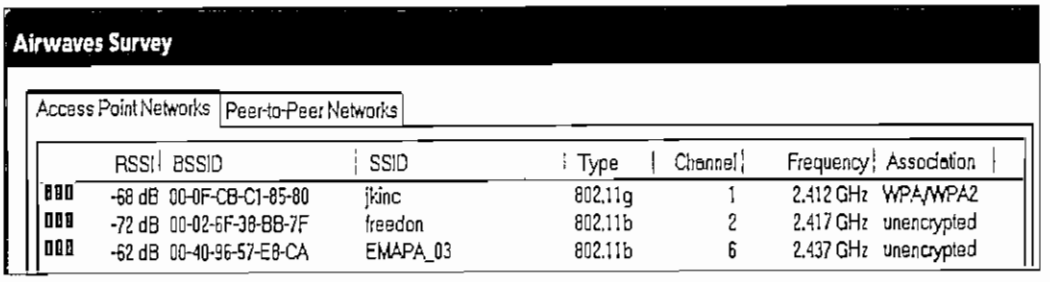


**Airwaves Survey**

Access Point Networks | Peer-to-Peer Networks

| RSSI | BSSID | SSID | Type | Channel | Frequency | Association |
|---|---|---|---|---|---|---|
| -81 dB | 00-10-E7-F5-A1-D0 | plastiwan | 802.11b | 11 | 2.462 GHz | wep |
| -71 dB | 00-40-96-57-E8-CA | EMAPA_03 | 802.11b | 6 | 2.437 GHz | unencrypted |
| -67 dB | 00-0A-E9-06-30-3A | | 802.11b | 3 | 2.422 GHz | wep |
| -79 dB | 00-60-B3-16-5A-C8 | COMPU | 802.11b | 9 | 2.452 GHz | unencrypted |
| -80 dB | 00-02-2D-49-84-C8 | speedy ambato | 802.11b | 1 | 2.412 GHz | wep |
| -59 dB | 00-0F-CB-C1-85-80 | jkinc | 802.11g | 1 | 2.412 GHz | WPA/WPA2 |

- Sala de Espera



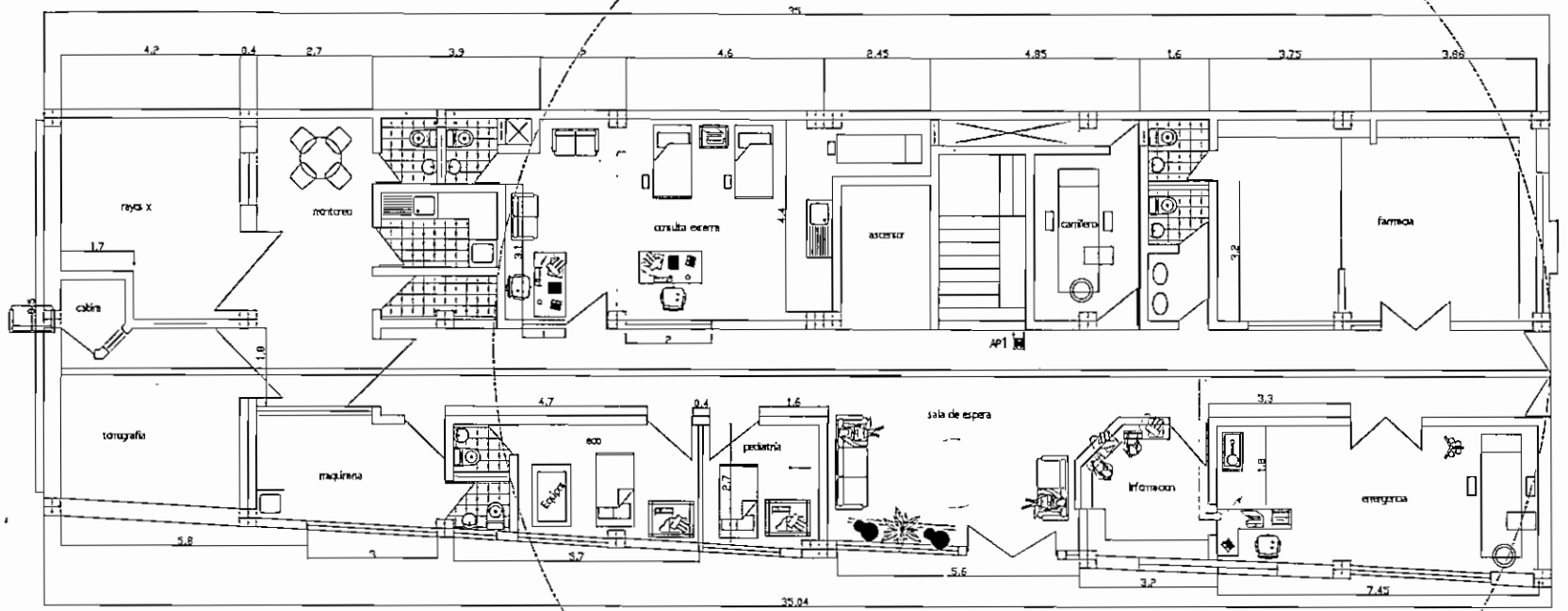
**Airwaves Survey**

Access Point Networks | Peer-to-Peer Networks

| RSSI | BSSID | SSID | Type | Channel | Frequency | Association |
|---|---|---|---|---|---|---|
| -68 dB | 00-0F-CB-C1-85-80 | jkinc | 802.11g | 1 | 2.412 GHz | WPA/WPA2 |
| -72 dB | 00-02-6F-38-BB-7F | freedon | 802.11b | 2 | 2.417 GHz | unencrypted |
| -62 dB | 00-40-96-57-E8-CA | EMAPA_03 | 802.11b | 6 | 2.437 GHz | unencrypted |


ANEXO 2F

# UBICACIÓN DE APs Y COBERTURA TEÓRICA




| SIMBOLOGÍA | |
|---|---|
| | ACCESO ZONE |
| | CANALETA 15x7 cm |
| | BARRA 3/4" + CANALETA PLASTICA |
| | LAPTOP |
| | DESKTOP |
| | IMPRESORA |
| | ZONA DE COBERTURA |

DISEÑO DE WLAN

CLINICA DURAN

CLAVE CATASTRAL: PREDIO #:

UBICACIÓN: Av. Pastaza y Stalin

CONTENIDO: – PLANTA BAJA

LAMINA: 1

PROYECTISTA 1: KARINA GUERRON

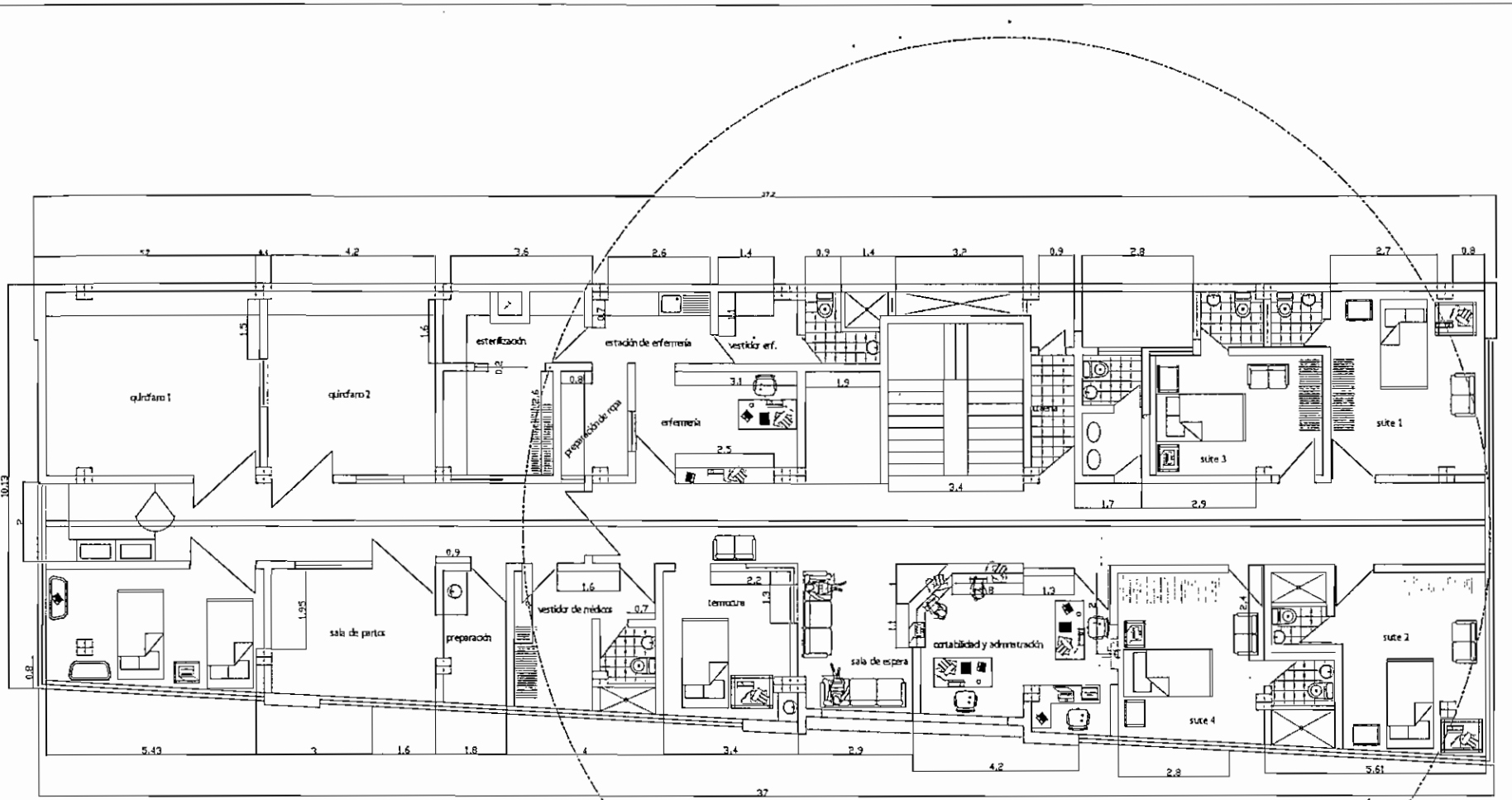
PROYECTISTA 2: JAIRO PICARO

FECHA: OCTUBRE / 2014

ESCALA: M

OBSERVACIONES

Todos los dispositivos de la red incluyen tarjetas de red inalambrica e integradores de red inalambrica




## SIMBOLOGÍA

| | |
|---|---|
| | ACCESS POINT |
| | CANALETA 16x7 cm |
| | TUBERIA 3/4" + CANALETA PLASTICA |
| | LAPTOP |
| | DESKTOP |
| | IMPRESORA |
| | ZONA DE COBERTURA |

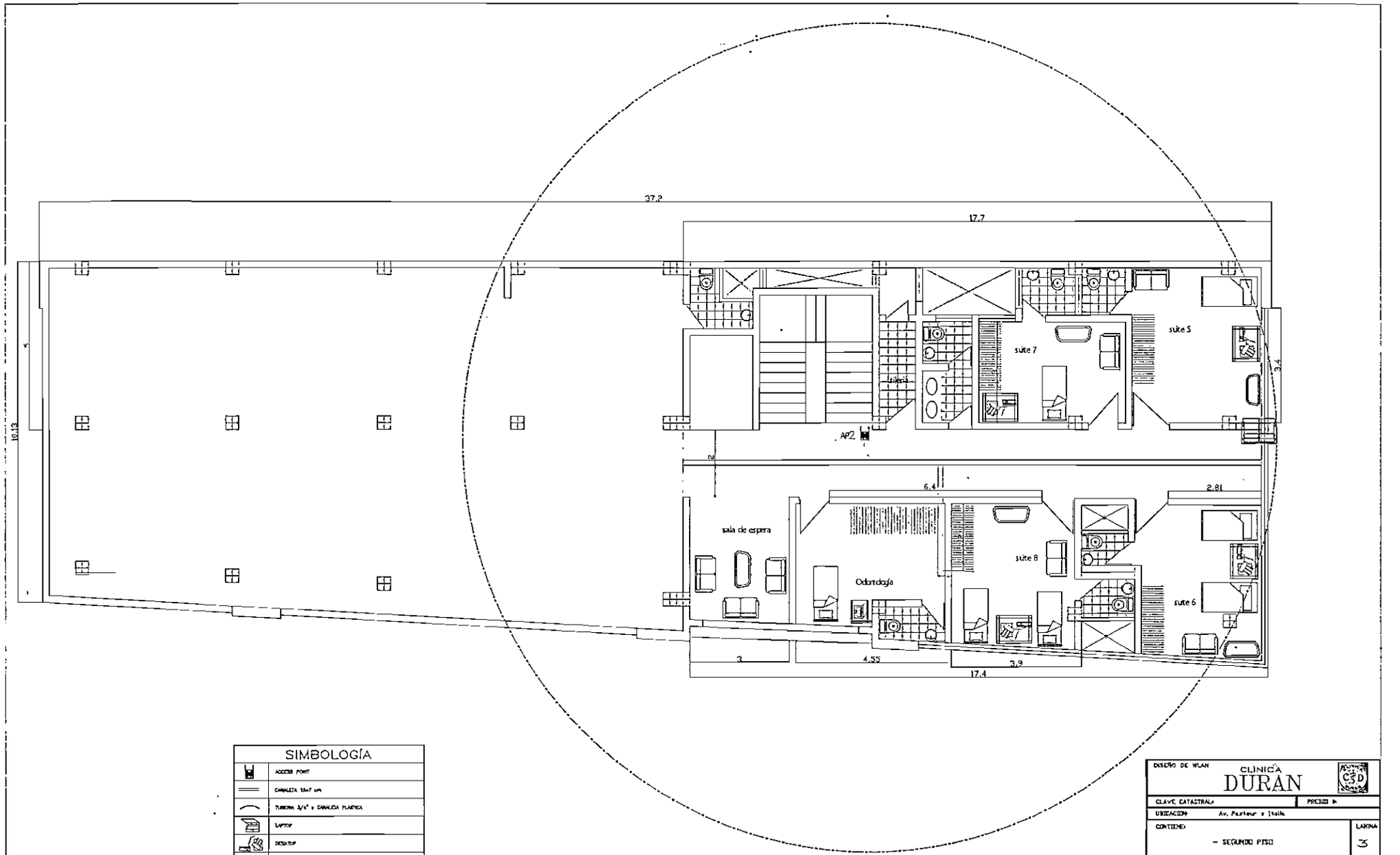
DISEÑO DE WLAN

CLINICA DURAN

| | |
|---|---|
| CLAVE CATASTRAL: | PREDIO N: |
| UBICACION: | Av. Pasteur e Italia |
| CONTENIDO: | LAMINA: |
| – PRIMER PISO | 2 |
| PROYECTISTA 1: | PROYECTISTA 2: |
| | FECHA: OCTUBRE / 2015 |
| | ESCALA: S/ |

OBSERVACIONES:

Todos los dispositivos de la red incluyen tarjetas de red inalambricas y adaptadores de red inalambricas




| SIMBOLOGÍA | |
|---|---|
| | ACCESS POINT |
| | CANALETA 15x7 cm |
| | TUBERIA 3/4" + CANALETA PLASTICA |
| | LAPTOP |
| | DESKTOP |
| | IMPRESORA |
| | ZONA DE COBERTURA |

DISEÑO DE WLAN

CLINICA DURAN

CLAVE CATASTRAL: PREDIO #:

UBICACIÓN: Av. Pasteur e Italia

CONTIENE: – SEGUNDO PISO

LAMINA: 3 DE 4

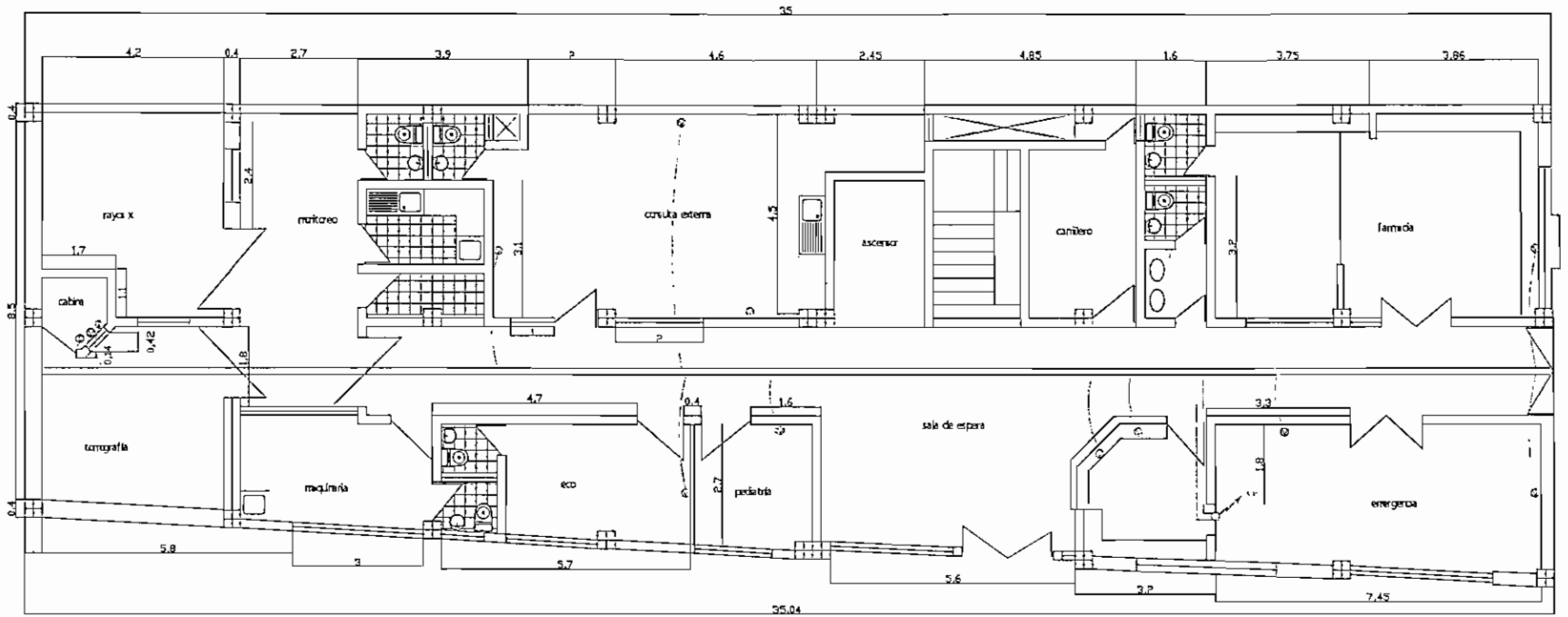
| PROYECTISTA 1 | PROYECTISTA 2 | FECHA: OCTUBRE / 2006 |
|---|---|---|
| KARINA GUERRON | JAIRON PROAÑO | ESCALA: S/E |

OBSERVACIONES:

Todos los dispositivos de la red incluyen tarjetas de red inalambricas o adaptadores de red inalambricos


ANEXO 2G

# DISEÑO DEL CABLEADO ESTRUCTURADO




| SIMBOLOGÍA | |
|---|---|
| | RACK |
| | CANALIZA 13x7 cm |
| | TUBERIA 3/4" o CANALETA PLASTICA |
| | PUNTO DE VOZ |
| | PUNTO DE DATOS |

CAMILO CIENCIAMAGO

# CLINICA DURAN

CLAVE CATASTRAL: PREDIO #:

UBICACION: Av. Pasteur e Italia

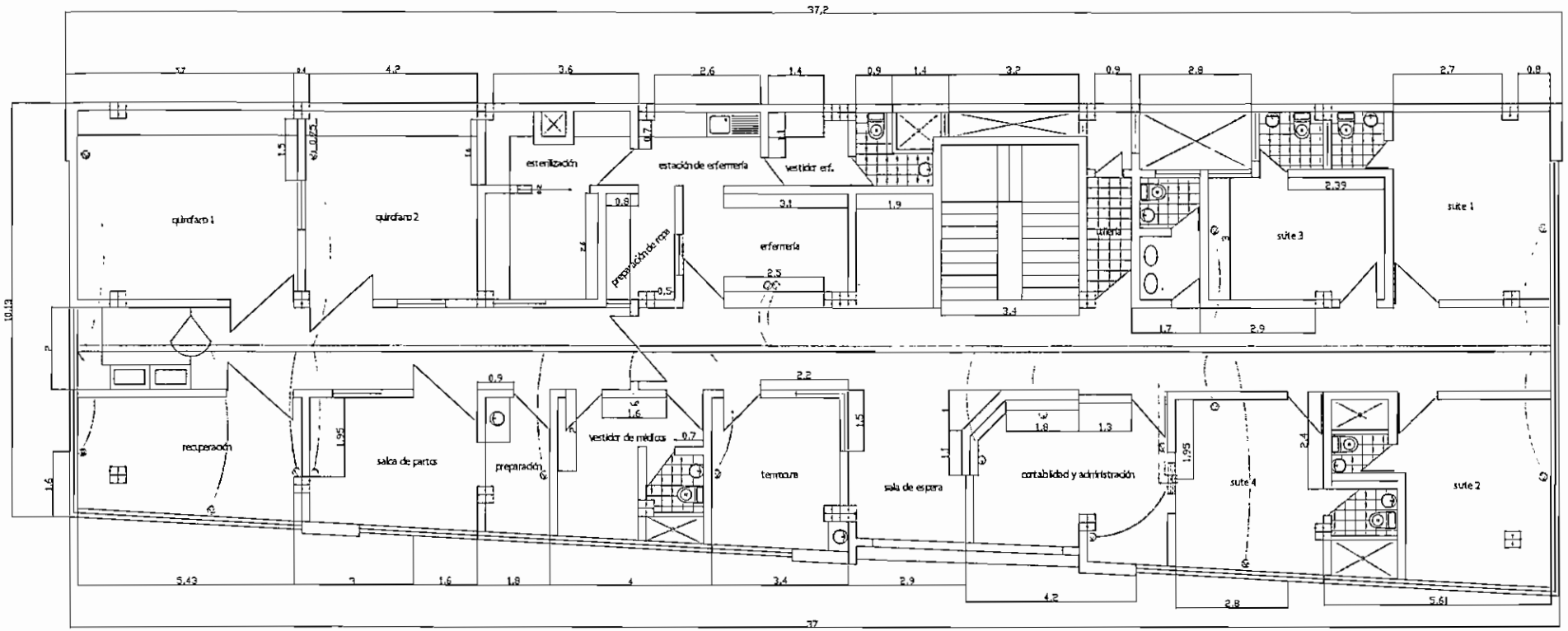
CONTIENE: – PLANTA BAJA

LAMINA: 1 de 4

| PROYECTISTA 1 | PROYECTISTA 2 | FECHA |
|---|---|---|
| RAMON GUERRON | JAIRA PRADO | OCTUBRE / 2006 |

ESCALA: 1:

OBSERVACIONES:




| SIMBOLOGÍA | |
|---|---|
| | MURO |
| | CANALETA 15x7 cm |
| | TUBERIA 3/4" + CANALETA PLASTICA |
| | PUNTO DE VOZ |
| | PUNTO DE DATOS |

CLINICA DURAN

CLAVE CATASTRAL: PREDIO N.

UBICACION: Av. Pasteur e Italia

CONTIENE: - PRIMER PISO

LAMINA: 2 DE 4

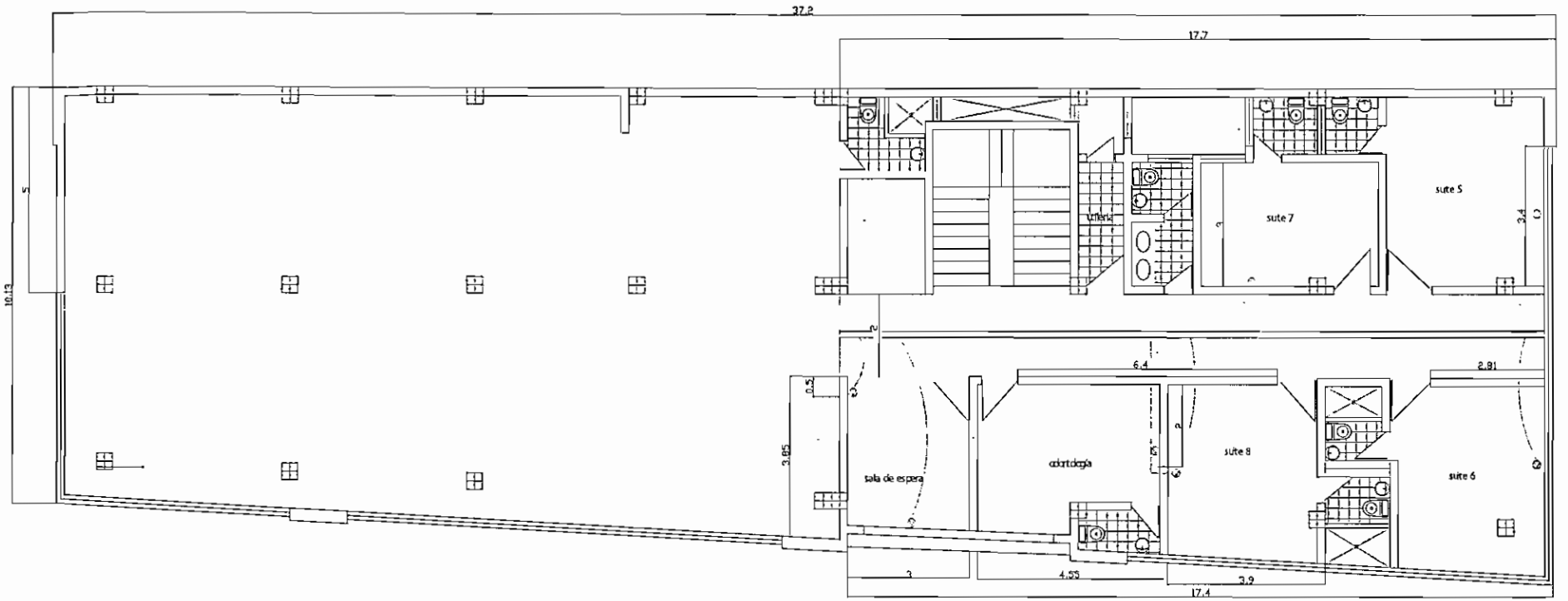
PROYECTISTA 1: KARINA QUICHIMBO

PROYECTISTA 2: ANDREA PROAÑO

FECHA: OCTUBRE / 2016

ESCALA: 1:1

OBSERVACIONES:




| SIMBOLOGÍA | |
|---|---|
| | MUROS |
| | CANALETA 10x7 cm |
| | TUBERIA 3/4" + CANALETA PLASTICA |
| | PUNTO DE VOZ |
| | PUNTO DE DATOS |

CABLEADO ESTRUCTURADO

CLINICA DURAN

CLAVE CATASTRAL: PREDIO N

UBICACION: Av. Pasteur e Italia

CONTIENE: - SEGUNDO PISO

LAMINA: 3

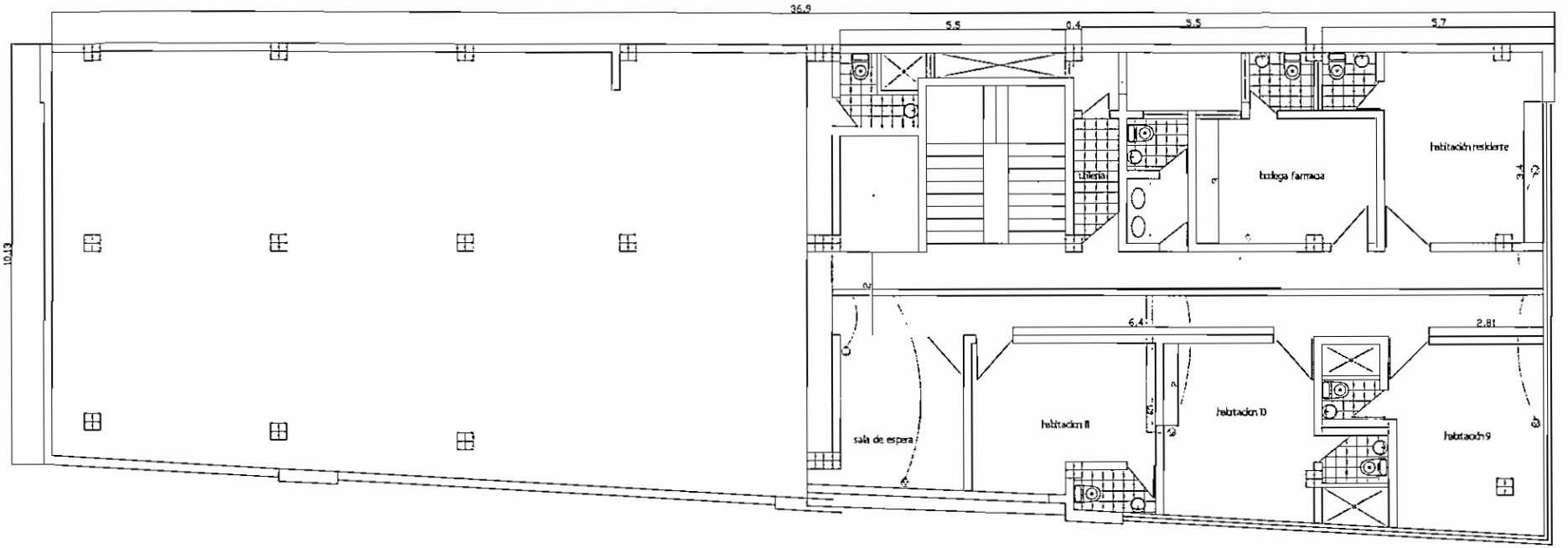
PROYECTISTA 1: [illegible]

PROYECTISTA 2: [illegible]

FECHA: OCTUBRE / 2006

ESCALA: S/

OBSERVACIONES




| SIMBOLOGÍA | |
|---|---|
| | BACH |
| | CANALETA 13x7 cm |
| | TUBERIA 3/4" + CANALETA PLASTICA |
| | PUNTO DE VOZ |
| | PUNTO DE DATOS |

CABLEADO ESTRUCTURADO

CLINICA
DURAN

CLAVE CATASTRAL: PREDIO #:

UBICACION: Av. Pasteur e Italia

CONTIENE: - TERCER PISO

LAMINA: 4 DE 4

PROYECTISTA 1: KARINA GUERRERO

PROYECTISTA 2: JAZMIN PINCAY

FECHA: OCTUBRE / 2006

ESCALA: S/

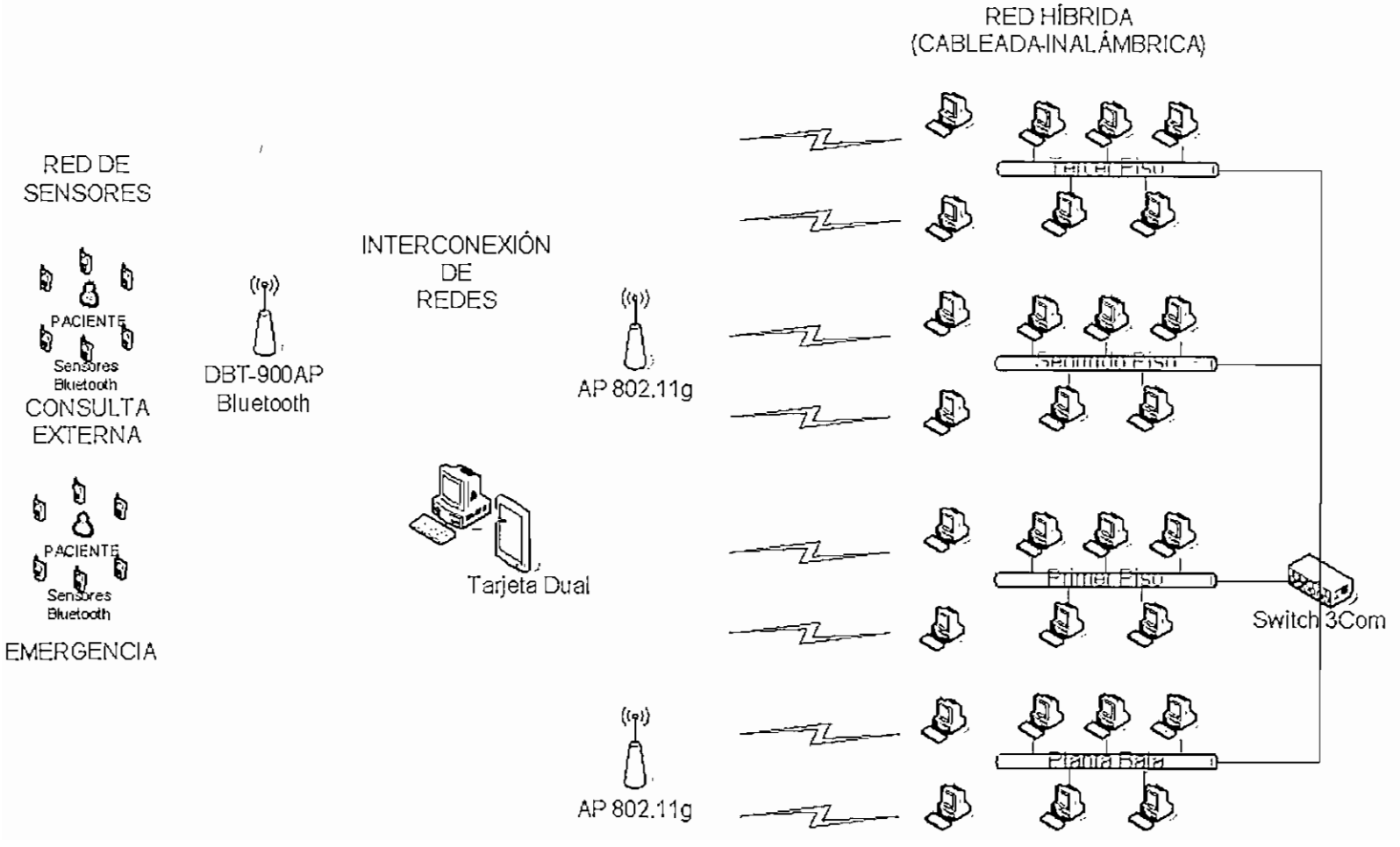
DESCRIPCIONES


ANEXO 2H

# DISEÑO DE LA RED HÍBRIDA

# DISEÑO DE RED CLÍNICA DURÁN

*AMBATO-ECUADOR*




ANEXO 4A

# CONFIGURACIÓN DEL SERVIDOR Y CLIENTE RADIUS

Configuración del Servidor RADIUS

El Servidor RADIUS a emplear es "*Odyssey Server*" versión 2.01.00.653. Se configuran sus parámetros básicos de funcionamiento, tal como se muestra a continuación. Primero se realiza la configuración del RADIUS, accediendo a la opción *Settings/RADIUS Settings*.

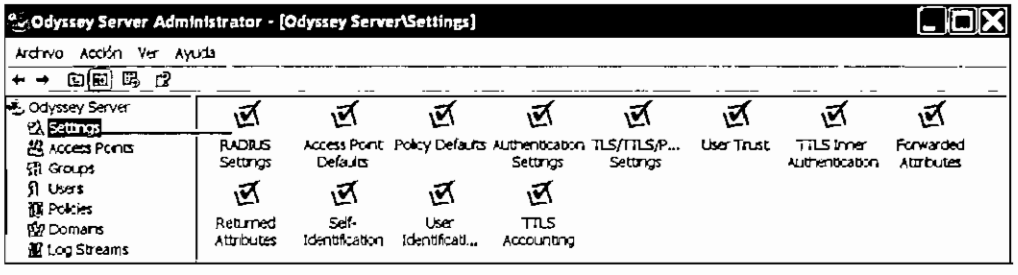



Figura 4A.1 Pantalla Inicial de Odyssey Server

Ahora se configuran los puertos 1812 y 1813, para realizar la autenticación y las peticiones de acceso respectivamente.

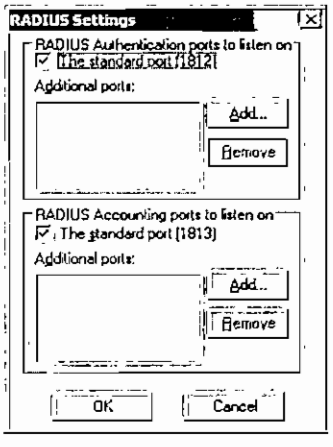



Figura 4A.2 Configuración RADIUS

Siguiendo con las opciones de configuración mostradas en la figura 4.28, se procede a configurar el Punto de Acceso, para lo cual primero se lo agrega, mediante la opción *Access Point/Add Access Point*.

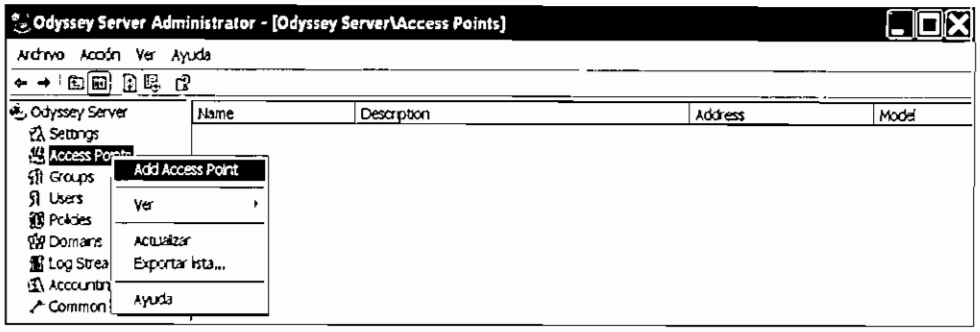



Figura 4A.3 Agregación de un Punto de Acceso

Para agregar el Punto de Acceso, se incluye su nombre y dirección IP, adicionalmente es importante y necesario determinar una clave compartida para el AP y el Servidor RADIUS, de tal modo que se garantice el acceso al servidor únicamente a los Administradores de la red.

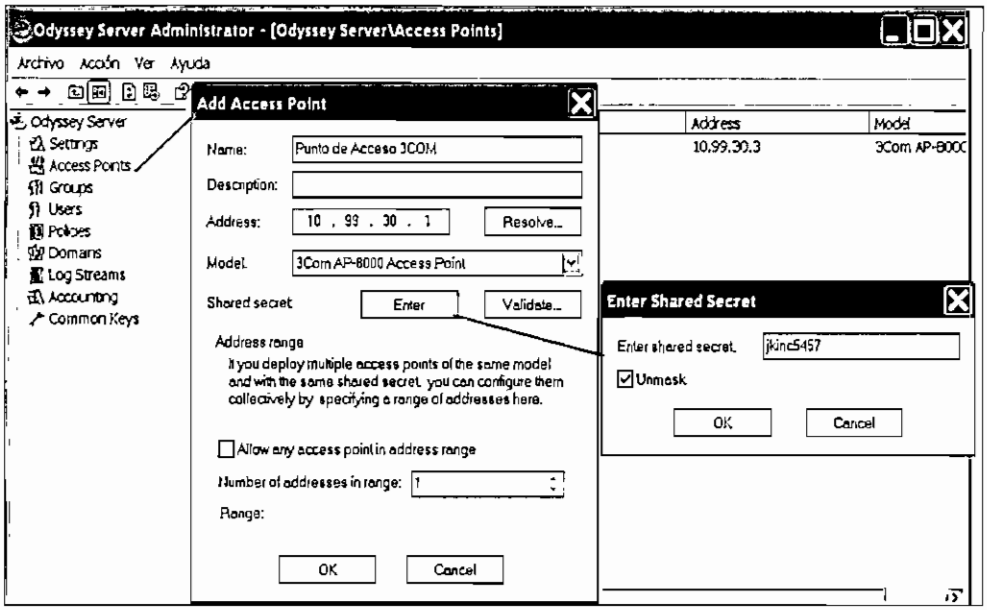



Figura 4A.4 Datos del AP a agregar

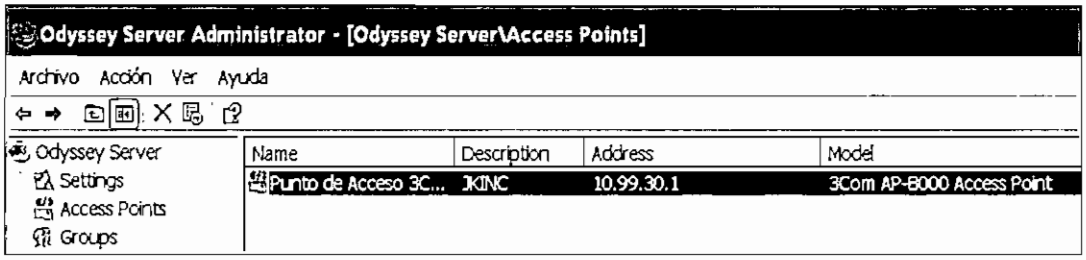



Figura 4A.5 Punto de Acceso agregado

Este servidor define 3 políticas de acceso a la red: Permitir, Negar y por Defecto.

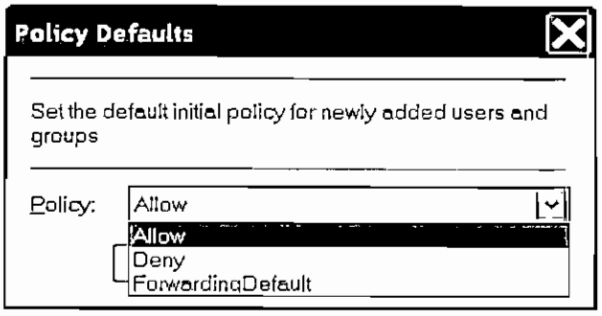



**Figura 4A.6 Permisos de Acceso a la Red**

Estas políticas de acceso, se aplican a los grupos y/o usuarios a autenticarse mediante el servidor. Para concluir la configuración de la primera sección, finalmente se agrega el dominio con el cual va a trabajar el servidor para la autenticación.

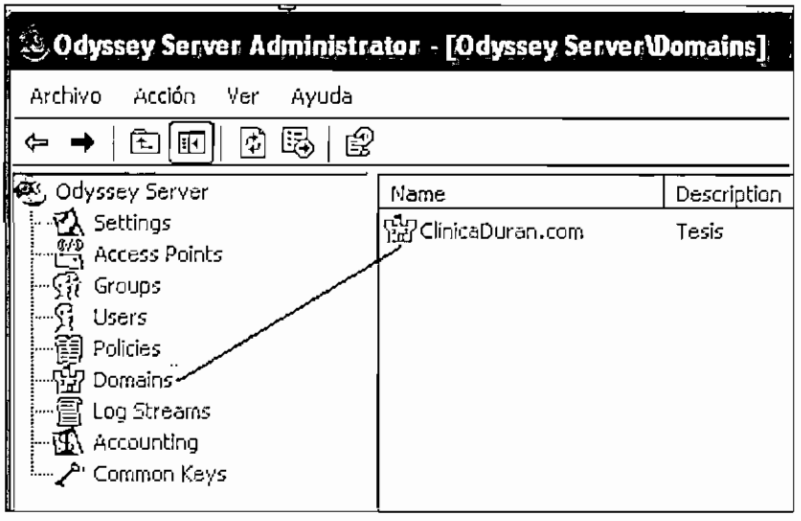



**Figura 4A.7 Configuración del Dominio para el Servidor RADIUS**

Ahora se procede a configurar el servidor de autenticación propiamente dicho, para cual se accede a la opción *Authentication Settings*, y se define el protocolo de autenticación a emplear, TTLS, como se muestra en la siguiente figura.

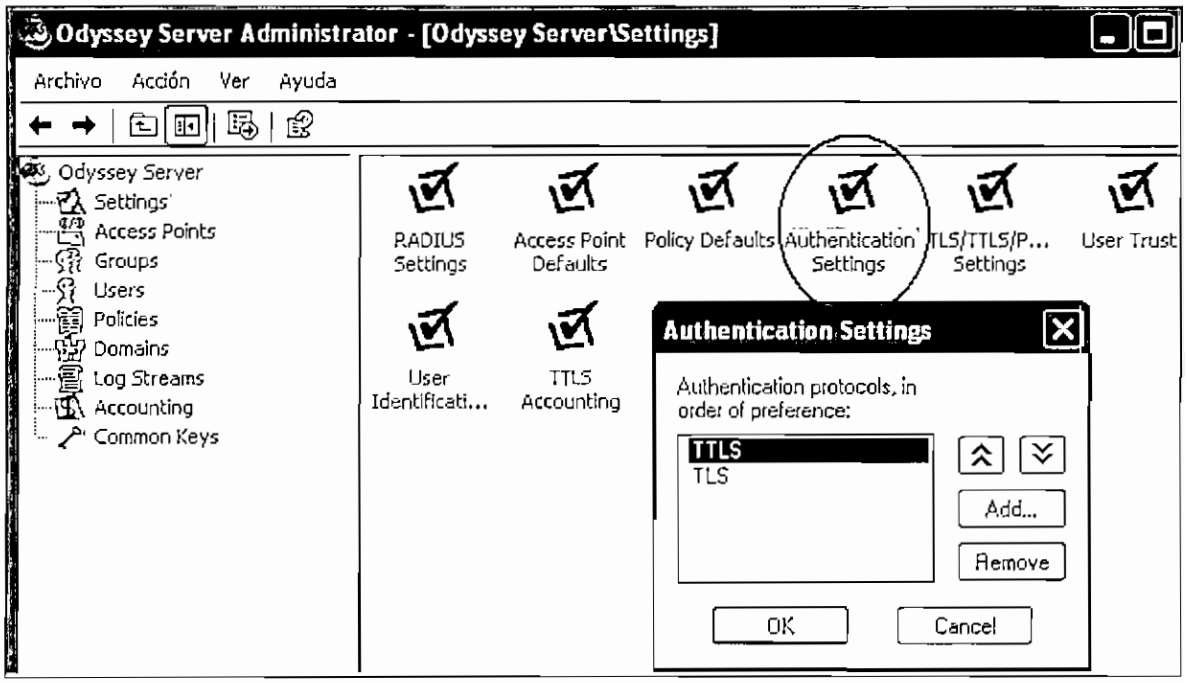



Figura 4A.8 Mecanismo de Autenticación

Seguidamente se configura el protocolo de Autenticación TTLS, para que acepte a EAP – MD5, como mecanismo de cifrado.

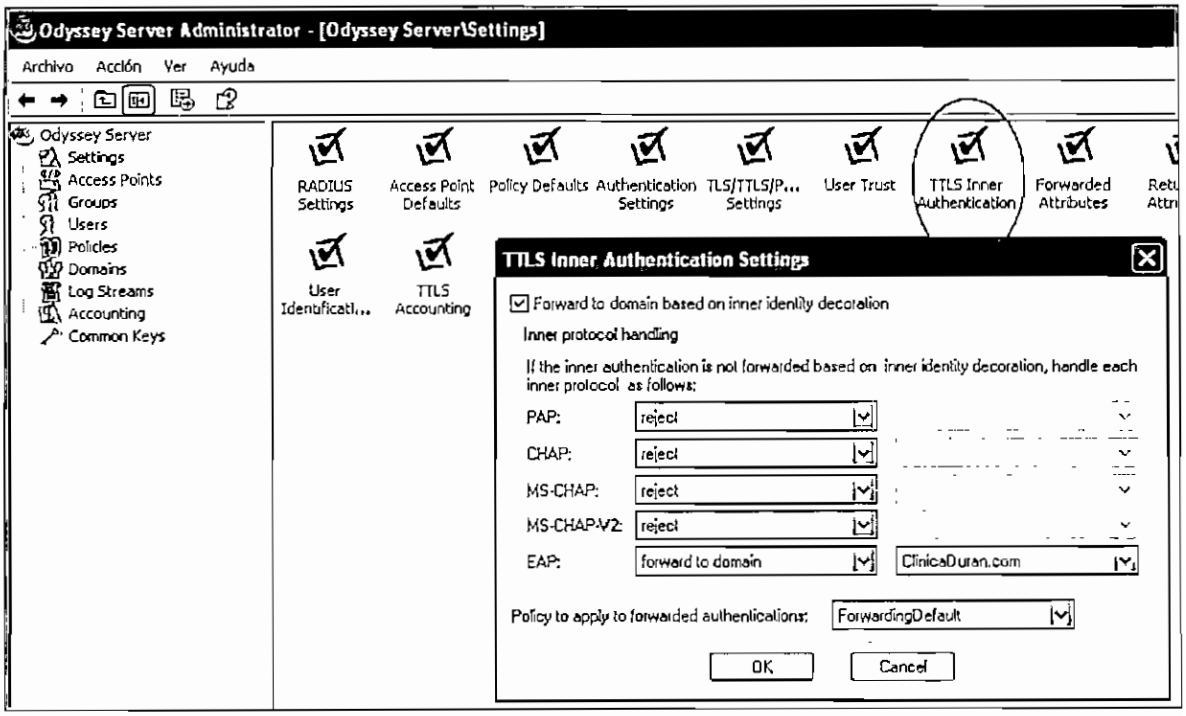



Figura 4A.9 Cifrado del Servidor RADIUS

Finalmente se configura la asignación de cuentas TTLS, para lo cual todas las peticiones de cuentas que llegan al AP son enviadas al servidor, el cual maneja una única clave, para proteger la identidad de los usuarios

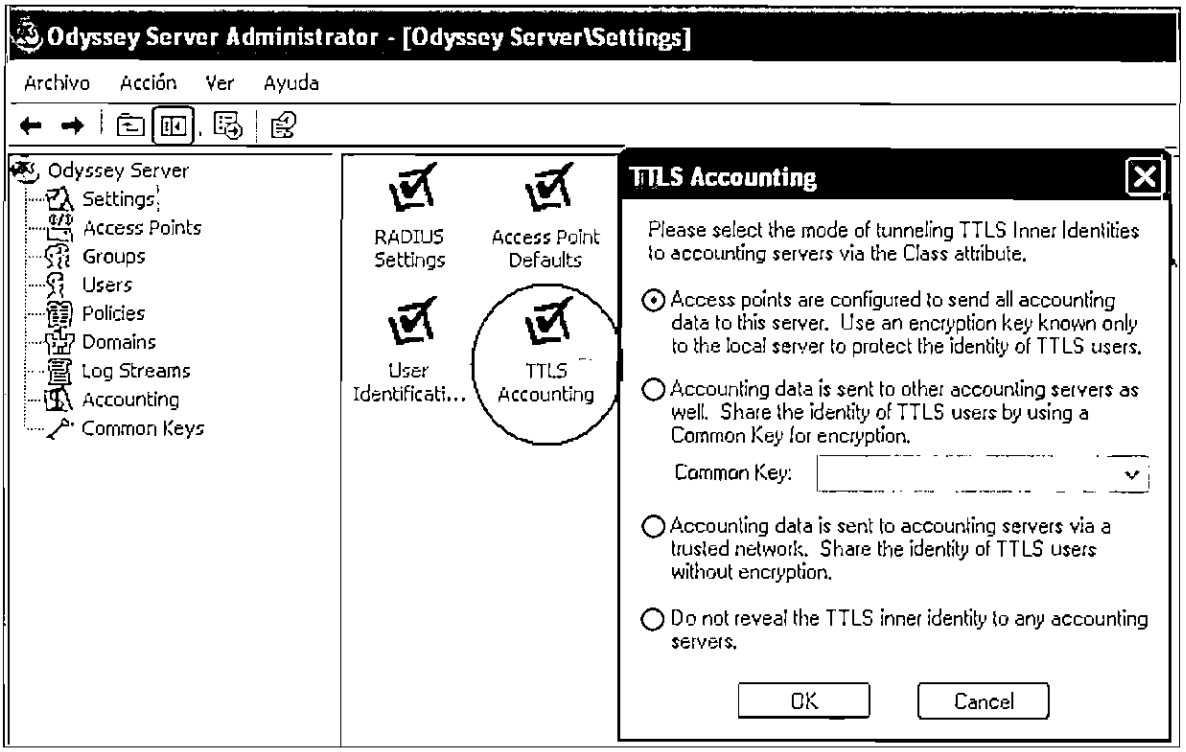



Figura 4A.10 Asignación de cuentas TTLS

Configuración del Cliente RADIUS

Para que cualquier estación pueda conectarse con el Punto de Acceso y acceder a la red inalámbrica, es necesario trabajar con una aplicación cliente, que permita determinar las características de conexión y seguridad.

El cliente a emplear es "*Odyssey Client Manager*" versión 4.32.0.2416, y acorde a lo establecido en el AP, se emplea TTLS y EAP – MD5 mediante un servidor RADIUS, como mecanismo de seguridad. Primero, se debe agregar la red inalámbrica a la cual se conectará el cliente, ingresando el SSID empleado en el Punto de Acceso y el mecanismo de autenticación con su clave, tal como se muestra en la siguiente figura.

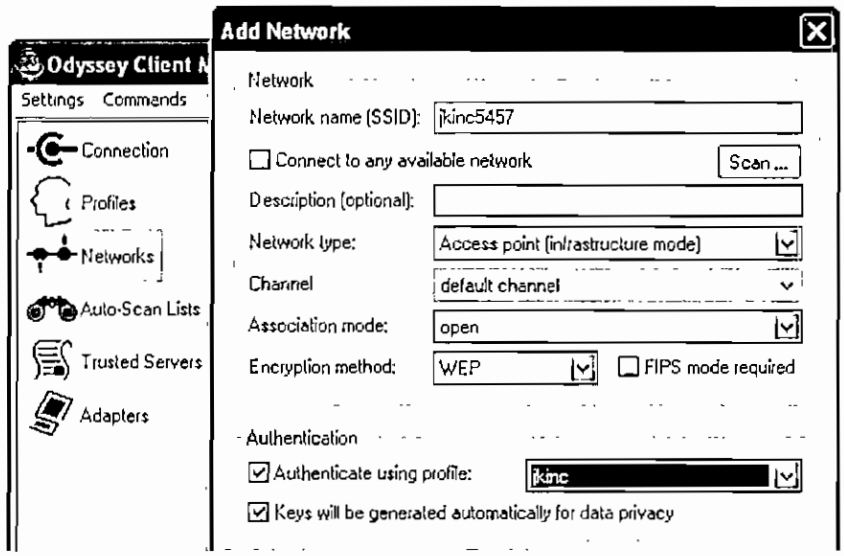



Figura 4A.11 Agregación de la Red Inalámbrica a Conectarse

Luego se crea un perfil de conexión, detallando el usuario de acceso, su password, y mecanismo de autenticación, acorde a un perfil especifico, como se muestra a continuación.

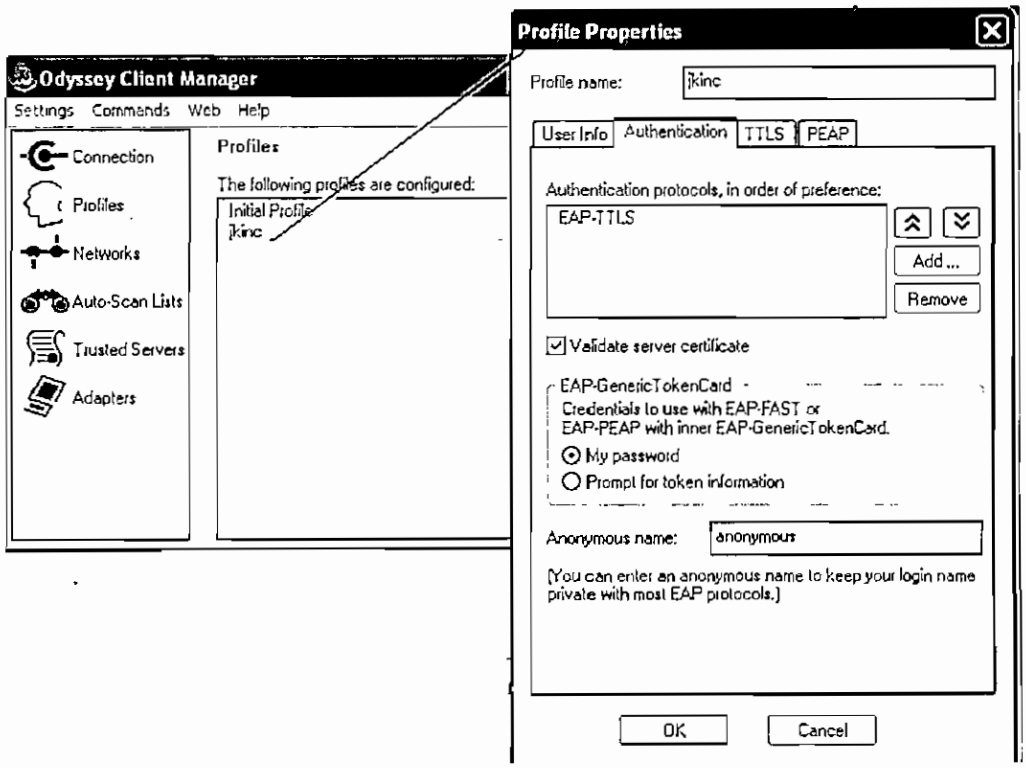



Figura 4A.12 Creación de un Perfil de Acceso a la Red

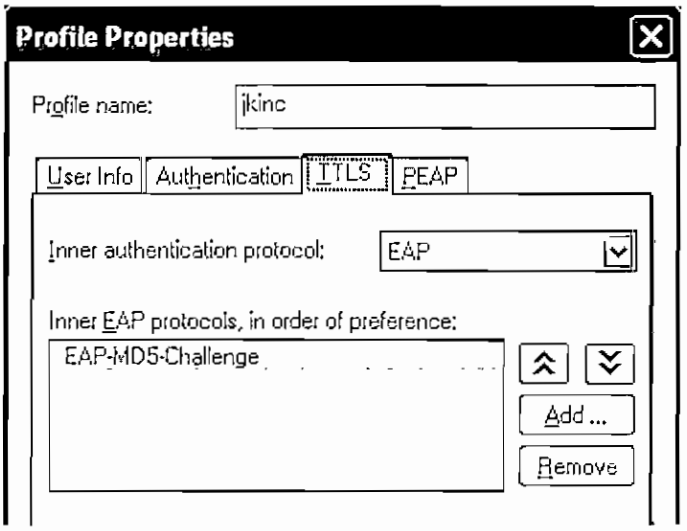



**Figura 4A.13 Configuración del Perfil de Acceso a la Red**

Finalmente se inicializa la conexión, se ingresa el password de seguridad y se accede a la red inalámbrica.

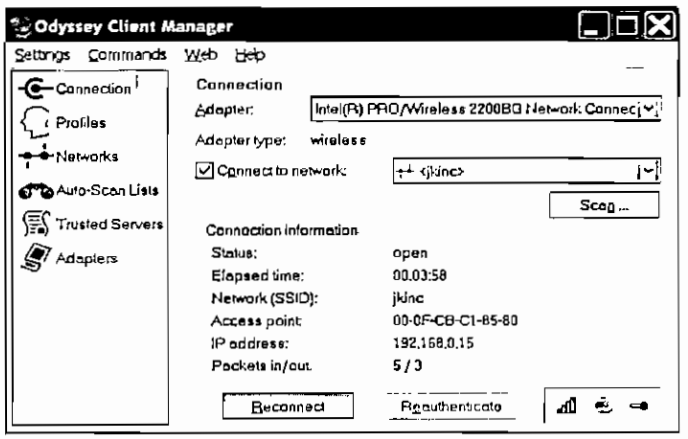



**Figura 4A.14 Conexión establecida con la Red Inalámbrica**


ANEXO 4B

# CONFIGURACIÓN DEL SERVIDOR MYSQL

## Configuración del Servidor MySQL Server

Se ingresa a *MySQL Server Instance Configuration*, para crear una instancia que permita acceder al Administrador MySQL como usuario root (raíz), el cual tiene asignado todos los privilegios de acceso y permite crear nuevos perfiles de usuarios.

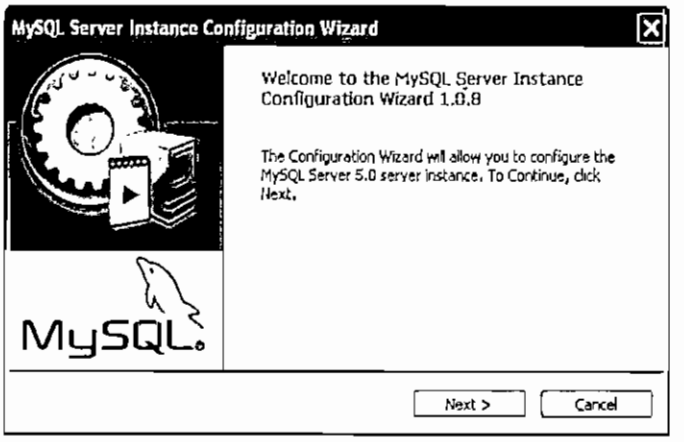



Figura 4B.1 Creación de una Instancia de Acceso a la BDD

Primero, se debe escoger el tipo de servidor que se requiere, en este caso se elige *Developer Machine,* ya que éste hace uso mínimo de la memoria, beneficiando el desempeño del servidor de aplicaciones.

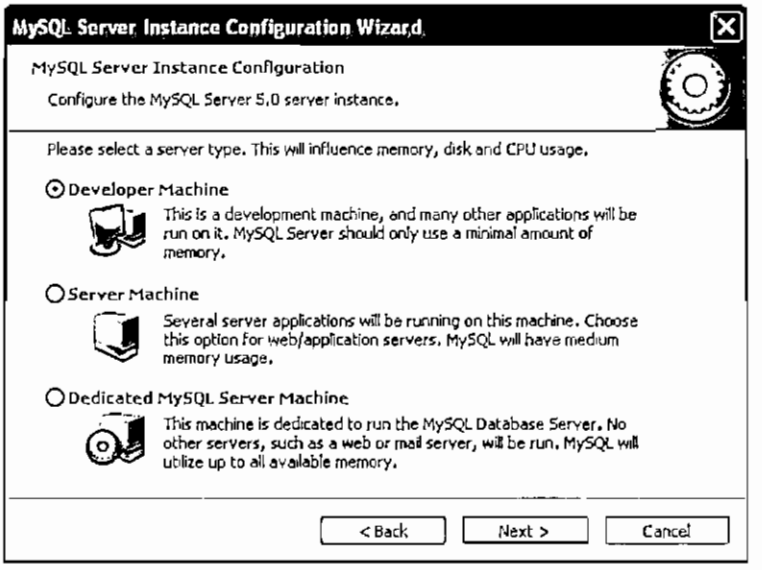



Figura 4B.2 Configuración de la Instancia – Tipo de Servidor de BDD

Luego se establece el tipo de uso que tendrá la Base de Datos, en este caso se utiliza la opción *Multifunctional Database*, por la optimización de transacciones rápidas y alta velocidad de almacenamiento que éste presta.

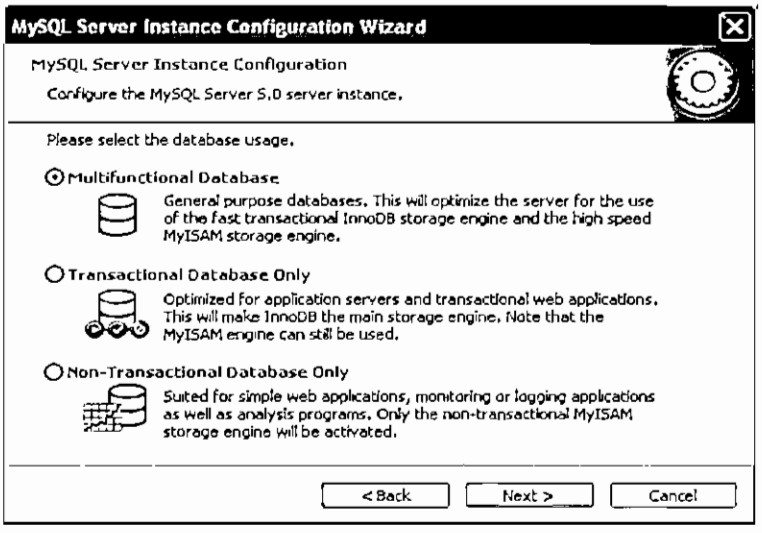



Figura 4B.3 Configuración de la Instancia – Tipo de BDD

En el siguiente paso se procede a establecer el número de conexiones concurrentes al servidor. En la clínica se estima tener un promedio bajo de conexiones concurrentes, por tanto se ha elegido la primera opción *Decision Support.*

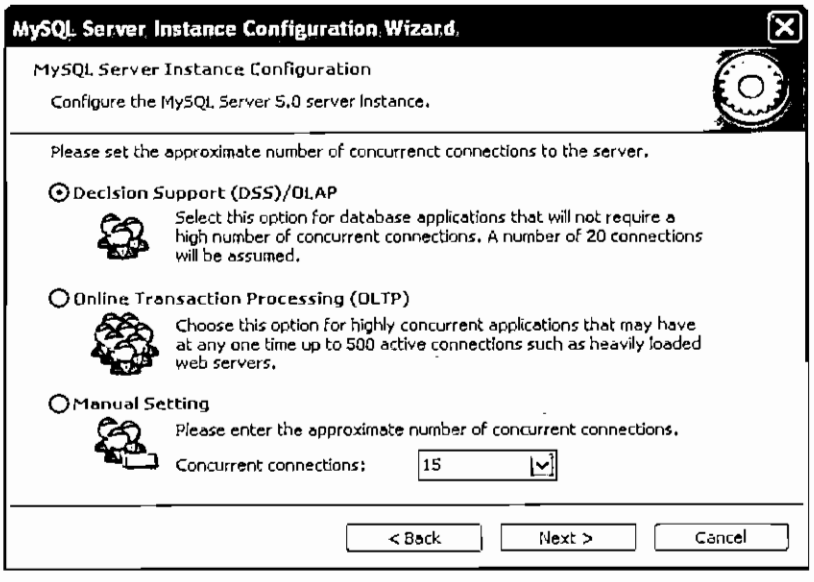



Figura 4.B4 Configuración de la Instancia – Conexiones Concurrentes

Dentro de las opciones de red, se habilita las conexiones por protocolo TCP/IP a través del puerto 3306 que es el preestablecido para conexión a Base de Datos. También se habilita el modo estricto de conexión, que obliga al servidor a comportarse como un Servidor de Base de Datos Tradicional.

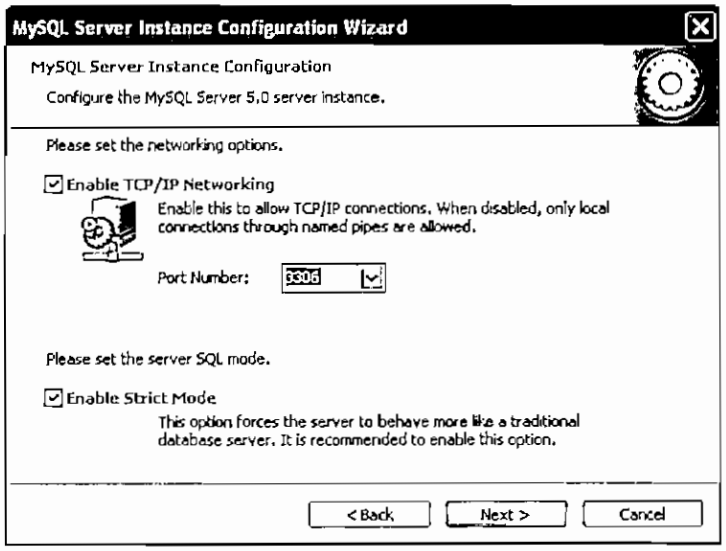



Figura 4B.5 Configuración de la Instancia – Tipo de Conexión

Luego se configura el tipo de caracter a utilizarse, en este caso se utiliza el tipo Latin 1.

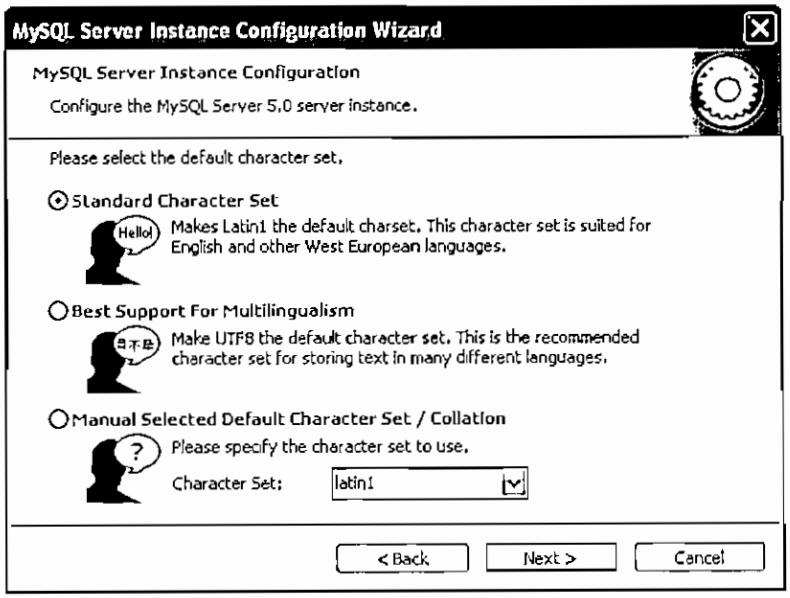



Figura 4B.6 Configuración de la Instancia – Tipo de Caracter

Finalmente se configura las opciones de seguridad para el usuario raíz, ingresando el password y reconfirmándolo.

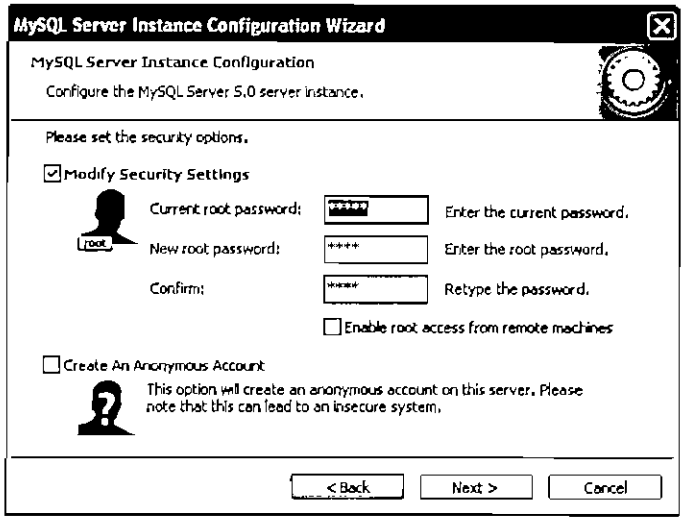



Figura 4B.7 Configuración de la Instancia – Usuario y Password

Se da un clic en *Excecute* para procesar la configuración, con lo cual se procede a la restauración del servicio con el Servidor, incluyendo la instancia creada con la cual se accede al Administrador MySQL.

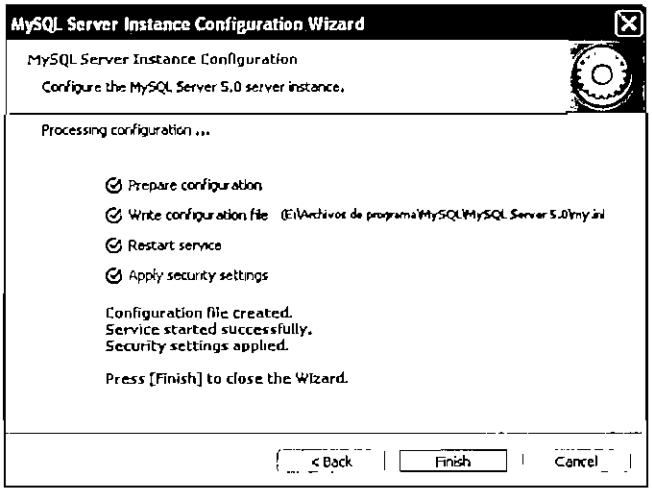



Figura 4B.8 Instancia Establecida

## Configuración de Usuarios en el Administrador MySQL

Luego de creada la instancia en el Servidor, se puede acceder con el nombre raíz y el password al *MySQL Administrator*, para agregar usuarios y darles el perfil

correspondiente (asignándoles privilegios), en la opción *User Administration.* Por ejemplo se procede a establecer un usuario kguerron, asignándole user, password, e información adicional.

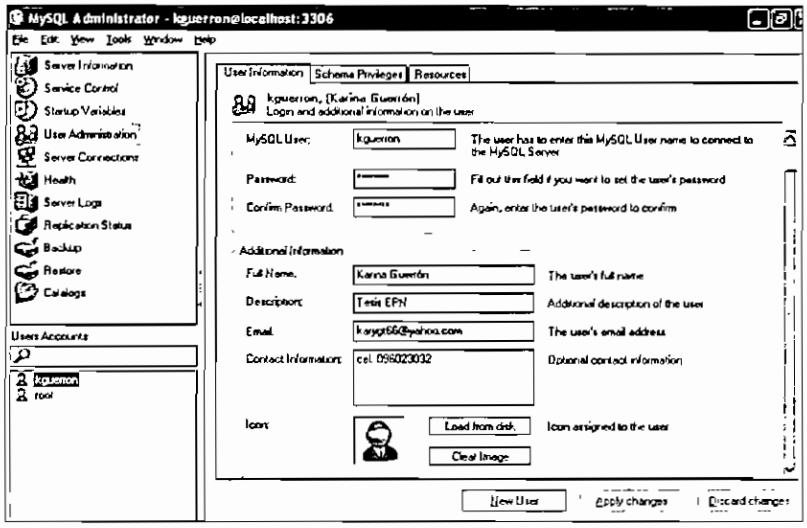



Figura 4B.9 Creación de Usuarios para Acceder a la BDD

Luego se establece el tipo de acceso para la conexión de este usuario, se elige el ingreso como *localhost*:

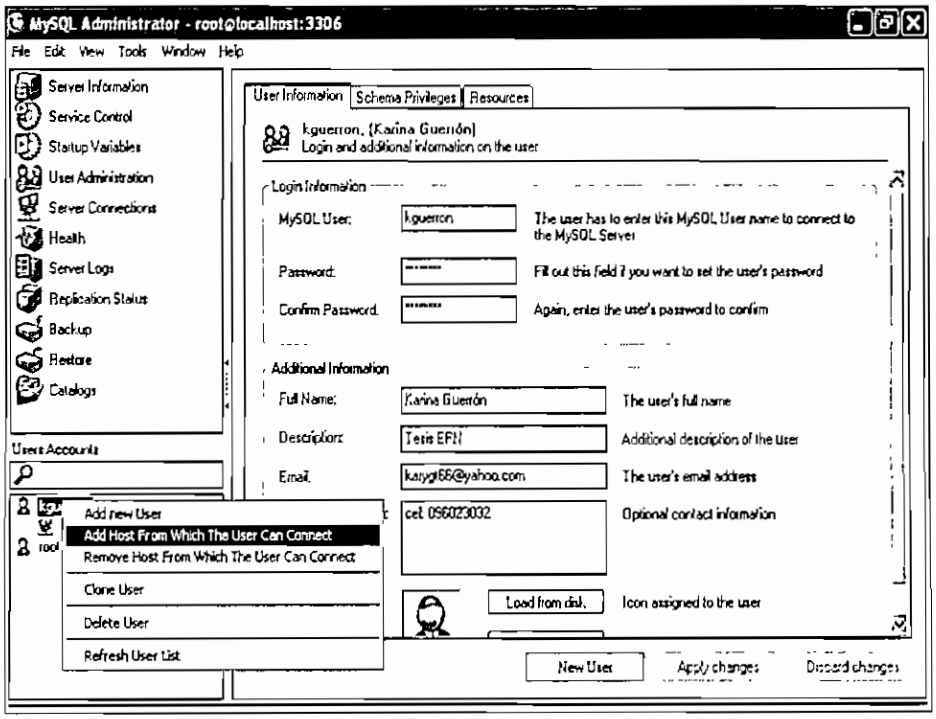



Figura 4B.10 Tipo de Ingreso a la BDD para el Usuario creado

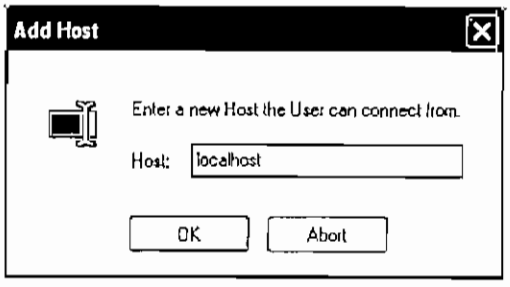



Figura 4B.11 Acceso a la BDD como *localhost*

Creado el tipo de acceso para el usuario, se procede a asignar los privilegios de la base de datos (tesis) creada previamente en *MySQL Query Browser*.

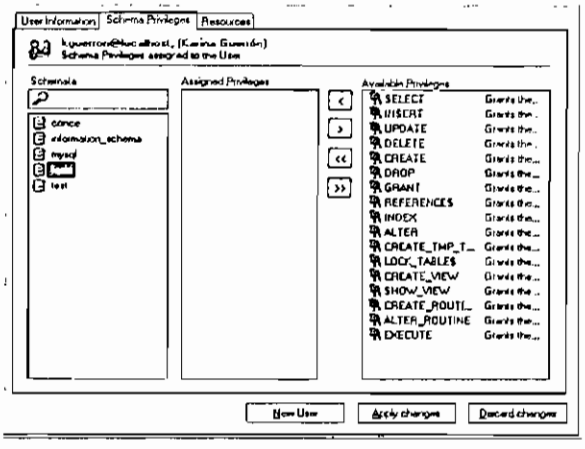



Figura 4B.12 Permisos de Acceso a la BDD

Finalmente para terminar la configuración de usuario, se accede a la pestaña de Recursos, y se establece el número de conexiones, consultas, conexiones de usuario, etc.

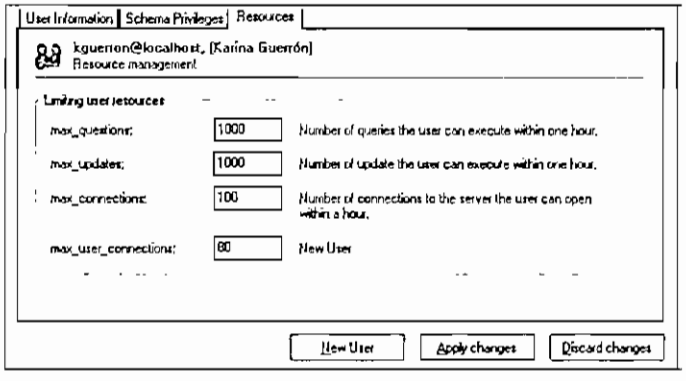



Figura 4B.13 Numero de Conexiones Permitidas para un Usuario

## Conexión MyODBC

Al tener MySQL Server 5.0 como servidor de Base de Datos, se procede a instalar el driver MyODBC-3.51 que nos servirá como puente para establecer la conexión.


Luego de realizar la instalación del puente y la configuración de cuentas en el Administrador, se accede al Panel de Control de Windows, luego a la opción de Herramientas Administrativas, y se selecciona Opciones de Datos (ODBC), con lo cual se presenta la pantalla de Administración de datos ODBC:

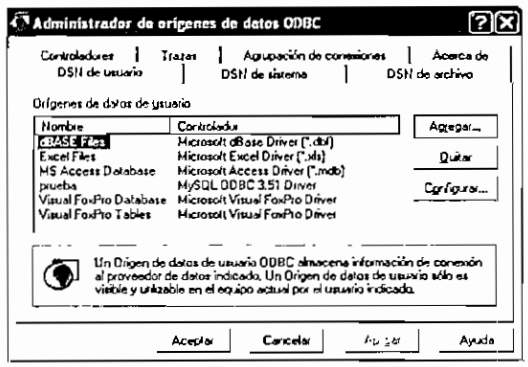



Figura 4B.14 Configuración del ODBC para MySql

Se elige entonces, Agregar un nuevo controlador, para luego seleccionar el que ya fue instalado (*MySQL ODBC 3.51 Driver*), así:

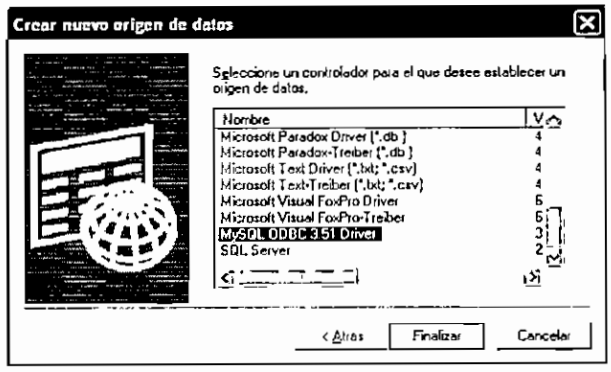



Figura 4B.15 Selección del Driver ODBC para MySql

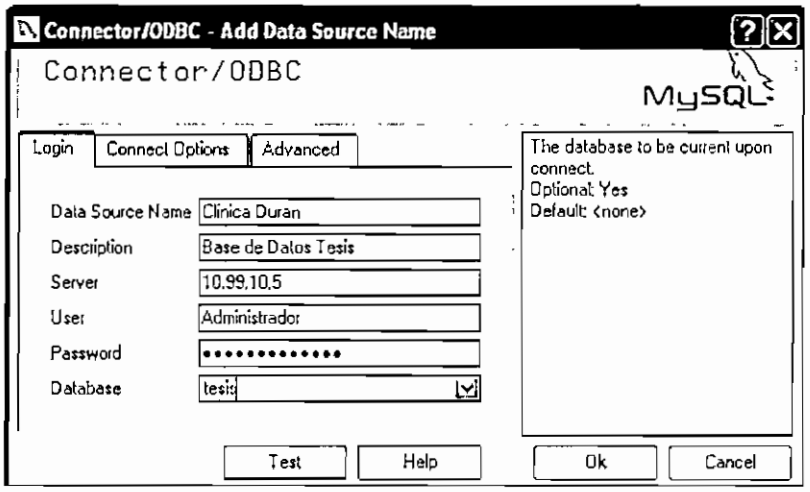
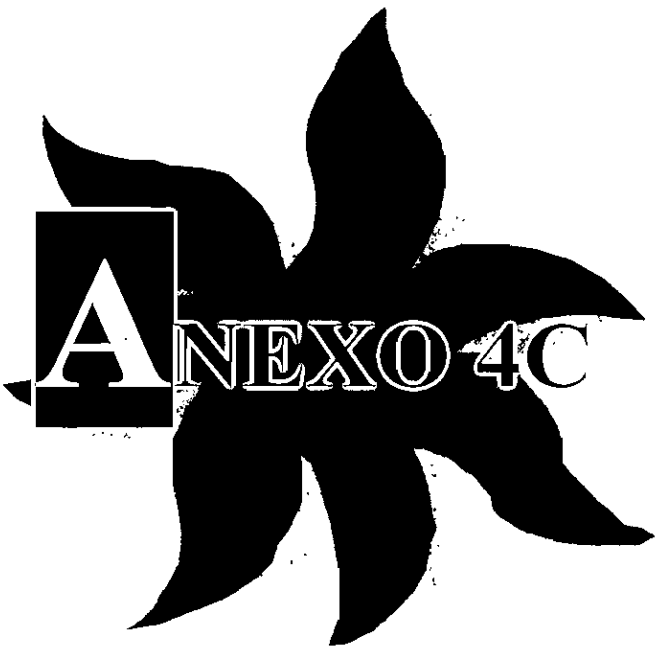



Figura 4B.16 Parámetros del puente JDBC-ODBC


ANEXO 4C

# MANUAL DE USUARIO DEL SISTEMA "JK INC"

# MANUAL DE USUARIO

## INTRODUCCIÓN

El sistema JK INC se constituye en una herramienta de trabajo para el ambiente de una unidad médica, llámese ésta Clínica u otro centro para atención médica, esta aplicación permite manejar diferentes perfiles de usuarios, registrar datos de los doctores, administrar citas médicas, historiales y toma de signos vitales a pacientes, registrar datos en emergencias y obtener reportes de las citas y emergencias atendidas. Todo esto haciendo uso de tecnología de punta en conexiones que se adaptan a ambientes inalámbricos.

## REQUERIMIENTOS DE HARDWARE

Para ejecutar el sistema se requiere disponer de los siguientes equipos y elementos, con las siguientes características mínimas:

- Un computador: procesador 2.4 GHz, 256 MB RAM, espacio en el disco duro de 1 GB, tarjeta de red.
- Un receptor *Bluetooth*.
- Un Pulso – Oxímetro NONIN AVANT 4100 tipo *Bluetooth*.
- Equipo de Interconectividad cableado o inalámbrico.*

## REQUERIMIENTOS DE SOFTWARE

Previo a la instalación de la aplicación, se debe contar con las siguientes aplicaciones:

- *MySQL Server* 5.0.
- *MySQL Administrator* 1.1.9.
- Maquina Virtual de Java 1.5.7.
- Software de manejo del receptor *Bluetooth*.

## INSTALACIÓN

* El acceso y almacenamiento de los datos por defecto, se realiza en un equipo Servidor, con lo cual se necesitarían 2 computadores y el equipo de interconectividad.

Antes de realizar la instalación del software, asegúrese de tener instalada la Maquina Virtual de Java 1.5.7 y el Servidor de Base de Datos *MySQL Server* 5.0, caso contrario la aplicación no podrá instalarse ni ejecutarse correctamente.

En primera instancia, se procede a recuperar la base de datos del sistema, mediante el *MySQL Administrador*, para lo cual debe tener configurada una instancia de ejecución del motor de Base de Datos, con privilegios de Administrador.

Ingrese al Administrador *MySQL*, y seleccione la opción *Restore*, luego *Open Backup File* y elija el archivo "bddtesisJKINC.sql"

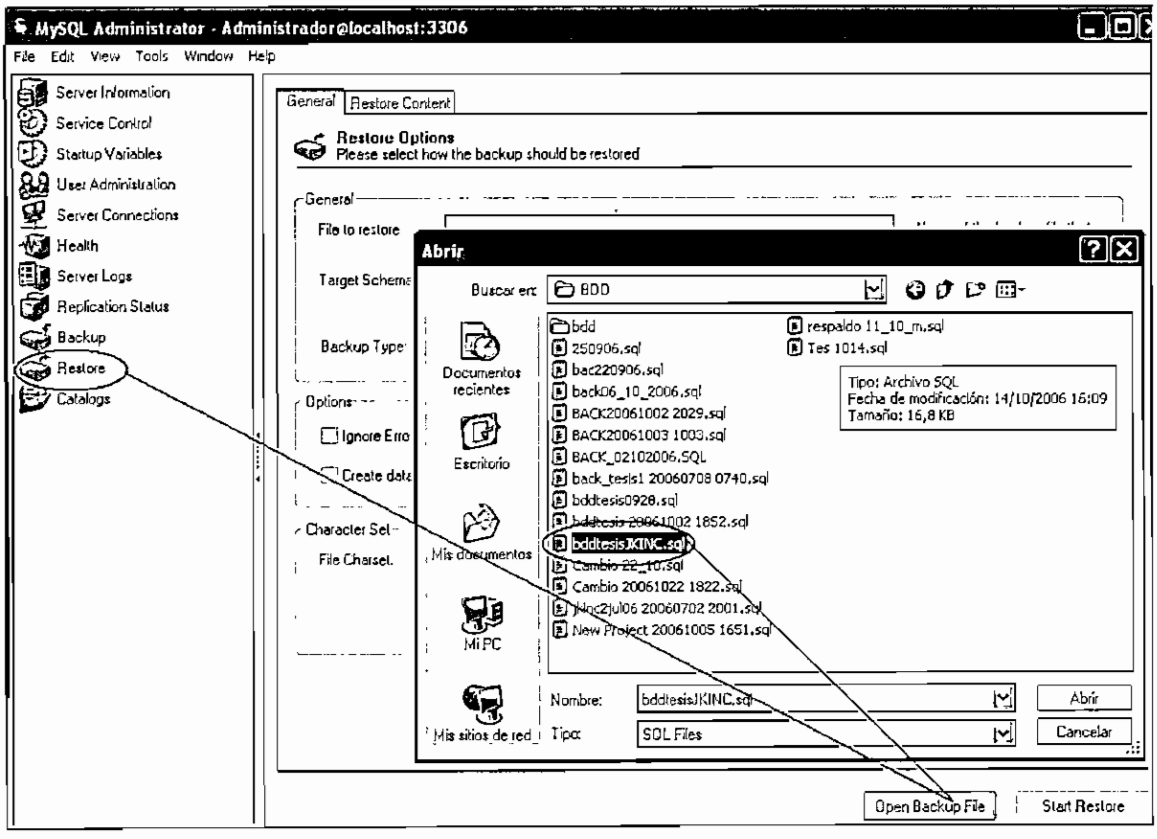



**Figura 4C.1 Restauración de la Base de Datos**

Seguidamente elija la opción *Star Restore*, y la base de datos es recuperada automáticamente; si existe algún error, intente de nuevo este procedimiento.

En el caso de utilizar el sistema a nivel individual, se debe configurar el puente JDBC – ODBC en el equipo, caso contrario el servidor de Base de Datos debe estar previamente instalado y corriendo en el mismo.

Los parámetros de acceso a la BDD, mediante el equipo servidor, con el puente, se muestran en la siguiente pantalla.

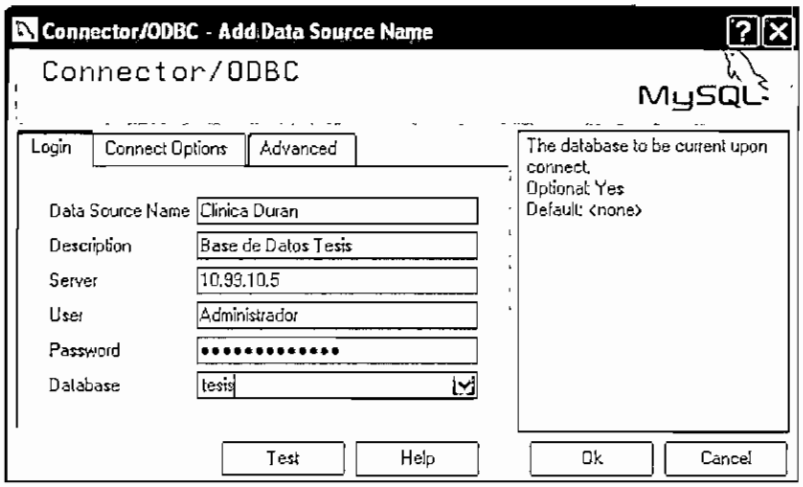



**Figura 4C.2 Configuración del puente JDBC-ODBC**

Para el funcionamiento del sistema en su totalidad, se requiere incluir el archivo de java para comunicaciones seriales, por lo cual se muestra el proceso de su agregación, para el caso del sistema operativo Windows.

- Descargar el paquete de java para comunicaciones (javacomm20-win32.zip).
- Descomprimir el archivo y guardar los siguientes archivos en las rutas especificadas:

  - win32com.dll: guardarlo en la carpeta ..\Java\jdk1.5.0_07\jre\bin
  - javax.comm.properties: copiarlo en la carpeta ..\Java\jdk1.5.0_07\jre\lib
  - comm.jar: copiarlo en la carpeta ..\Java\jdk1.5.0_07\jre\lib\ext

- Finalmente se debe agregar en el path (variables de entorno de Windows) ..\Java\jdk1.5.0_07\jre\lib\ext\comm.jar. Los dos puntos (..) corresponde a la raíz donde está instalado java (incluye la unidad).

Para instalar el sistema, haga doble clic sobre el icono de la figura 1.


Figura 4C.3 Icono de instalación del Software JK INC

Seguido aparece la pantalla de bienvenida a la instalación del sistema (Figura 2); conforme avanza la misma, acepte todas las opciones de definidas por defecto, como el Acuerdo de Licencia y el directorio de instalación, entre otros.

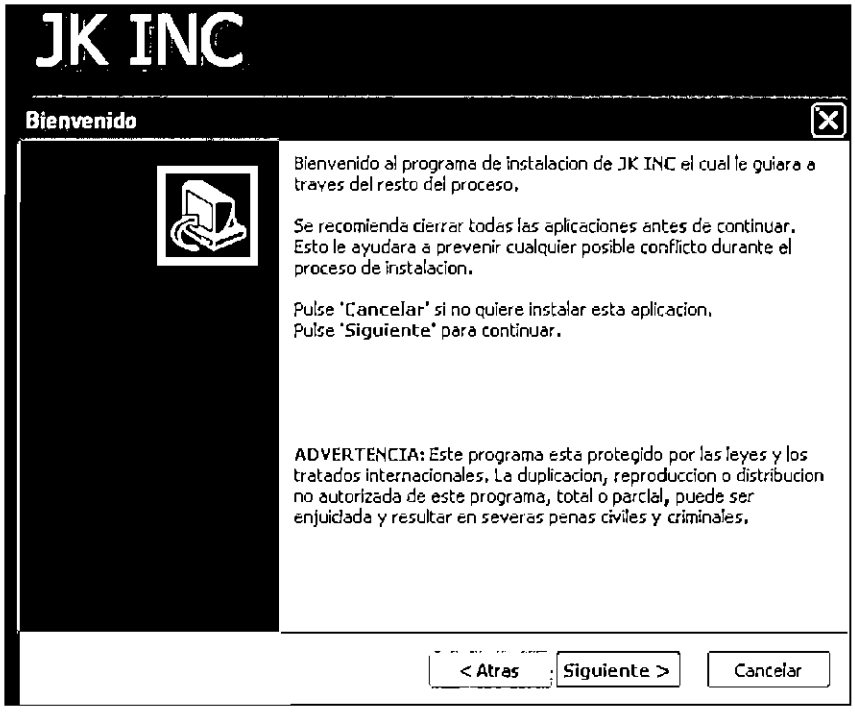



Figura 4C.4 Instalación del Software JK INC

Finalizado este proceso, se ejecuta automáticamente el sistema.

## TRABAJANDO CON JK INC

La aplicación inicia con la validación de un usuario permitido, es necesario ingresar en la primera pantalla el usuario y contraseña asignados, en caso de ingresar los datos correctos, comenzará el usuario a trabajar en el sistema.

Se permite el ingreso incorrecto de 2 intentos, en caso de fallar, el sistema se cierra para evitar más intentos de ingreso.

A continuación se muestra la pantalla inicial del sistema, y a continuación la pantalla principal del mismo (figuras 4C.5 y 4C.6)

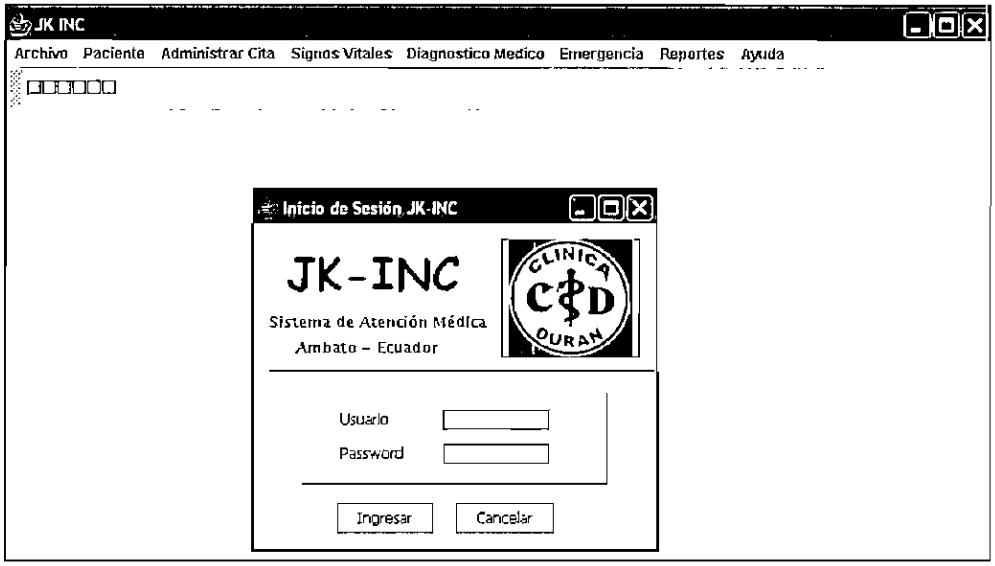



Figura 4C.5 Ingreso de Usuario y Contraseña

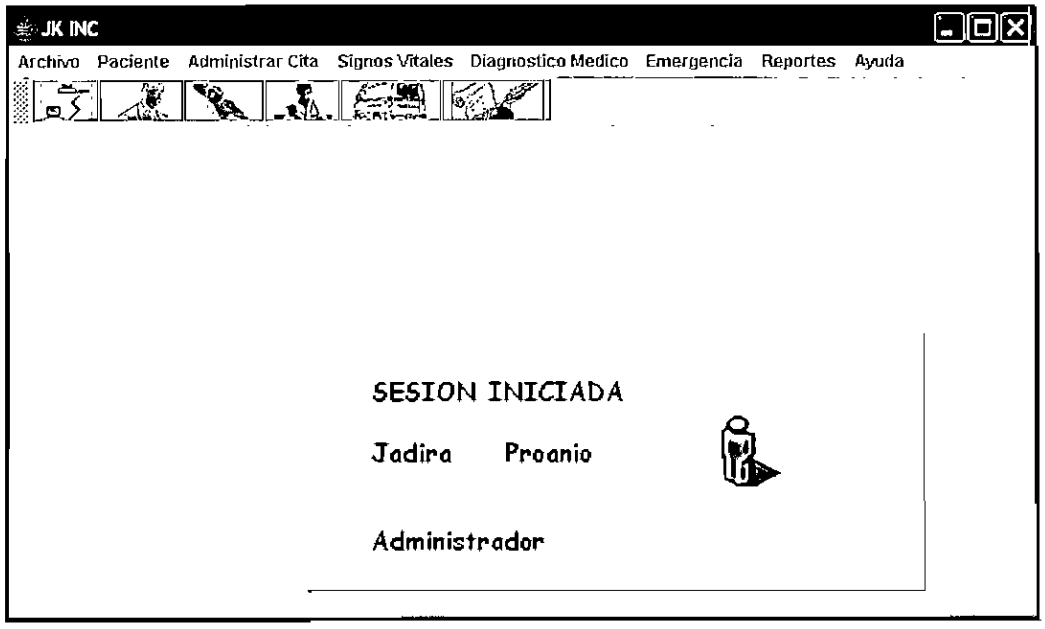



Figura 4C.6 Pantalla Principal

En el sistema se han agrupado las capacidades de manera tal que el usuario utilizará el siguiente esquema de menú:

**Archivo**
- Administración
  - *Gestionar Usuario*
  - *Gestionar Doctor*
- Cambio de Sesión
- Salir

**Paciente**
- Gestionar Paciente

**Administrar Cita**
- Disponibilidad Médica
- Establecer Cita
- Pago Cita

**Signos Vitales**
- Gestionar Signos Vitales

**Diagnostico Médico**
- Consulta Ext erna
- Emergencia

**Reportes**
- Reportes Consulta Externa
- Reportes Emergencia

**Ayuda**
- Acerca de...

**Administrando Usuarios**

El sistema utiliza usuarios creados en el mismo para controlar el acceso y funcionalidad de acuerdo a roles que llevarían en un ambiente de una institución de salud.

Para trabajar con los usuarios en el sistema se puede buscar un usuario existente, para poder ejecutar esta consulta se dirige por el menú (**Archivo → Administración → Gestionar Usuario**) y en la pantalla que aparece se ingresa el nombre del usuario a buscar, tal como se muestra en una imagen de la pantalla de gestión (figura 4C.7).

Ingresado el login (nombre de usuario) se puede mandar a buscar con el botón **Buscar**, en caso de no existir, se puede crear en ese momento uno, presionando el botón **Nuevo.**

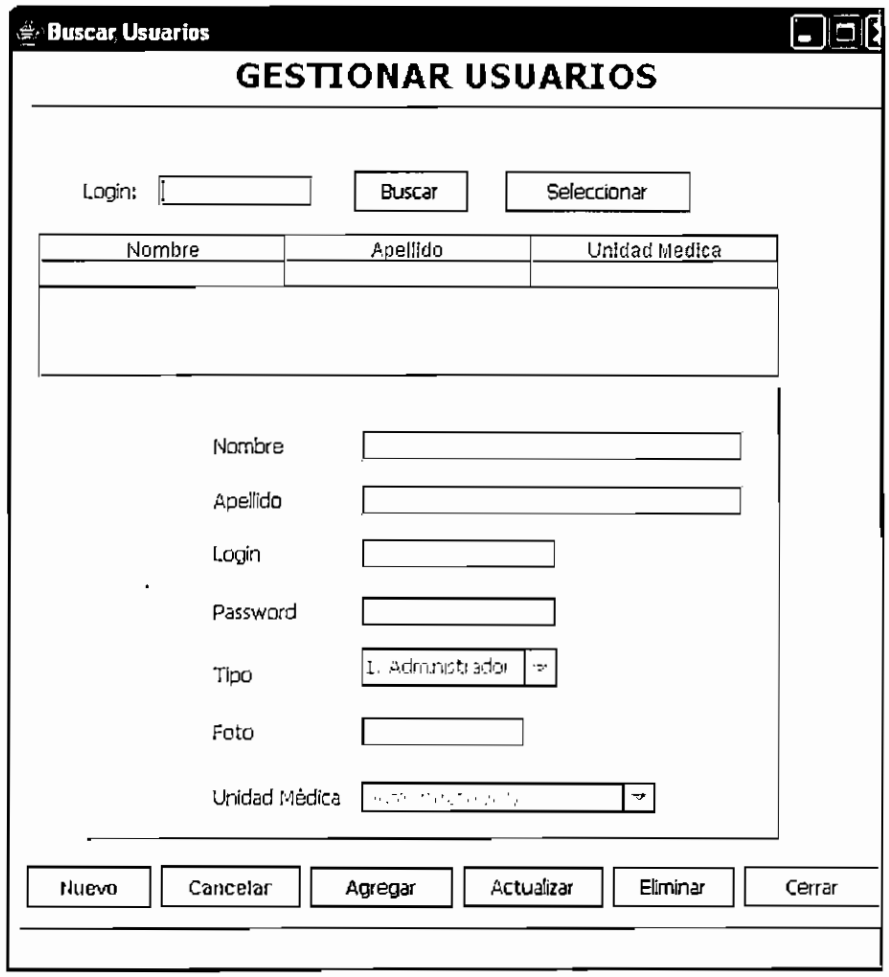



Figura 4C.7 Gestionarr Usuarios en el Sistema

En el caso de crear un nuevo usuario, se ingresan los datos del nuevo usuario y se selecciona una Unidad Medica en la cual éste trabaja., luego de ingresados los datos se los almacena con el botón **Agregar**, o si no desea hacerlo, se presiona el botón **Cancelar**.

En el caso de existir el usuario se pueden modificar sus datos, para ello seleccione el usuario en la tabla, y presione **Seleccionar**, luego realice los cambios requeridos y almacénelos mediante el botón **Actualizar**.

Si desea eliminar un usuario del sistema, luego de buscarlo, selecciónelo de la tabla y presione el botón **Eliminar**, con lo cual queda borrado de los registros del sistema Finalmente el botón **Cerrar**, cierra el formulario.

### Administrando Doctores

Para trabajar con los datos de los Doctores en el sistema, se puede buscar un doctor existente, para poder ejecutar esta consulta se dirige por el menú (**Archivo → Administración → Gestionar Doctor**) y en la pantalla que aparece se ingresa el nombre del doctor a buscar.

A continuación se muestra una imagen de la pantalla para búsqueda (figura 4C.8).

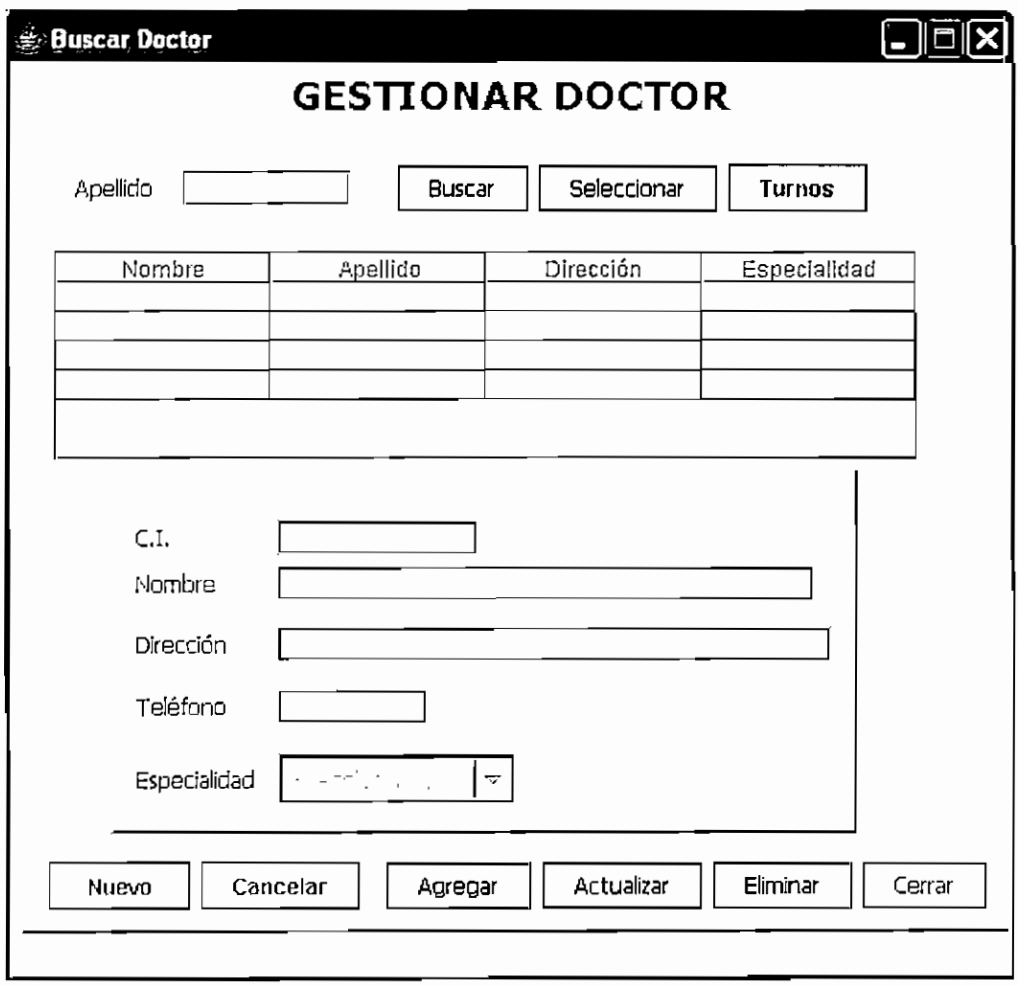



Figura 4C.8 Gestionar Doctor en el Sistema

Si se está familiarizado con la funcionalidad del manejo de usuarios, este comportamiento es muy similar.

Ingresado el apellido del doctor se puede mandar a buscar con el botón **Buscar**, en caso de no existir, se puede crear en ese momento uno, presionando el botón

**Nuevo**. En el caso de crear un nuevo doctor, se ingresan los datos del nuevo registro, se selecciona una especialidad en la cual trabaja, y se presiona el botón **Agregar**, caso contrario presione **Cancelar**.

Si se desea modificar la información almacenada de determinado Doctor, seleccione el mismo de la tabla y presione el botón **Seleccionar**, cambie la información deseada y almacénela con el botón **Actualizar**.

Para eliminar un registro de Doctor del sistema, búsquelo, y una vez seleccionado, presione el botón **Eliminar**.

Una de las tareas más importantes por parte de los doctores es establecer su disponibilidad médica, es decir definir turnos que pueden más adelante ser tomados para las citas de los pacientes. Para acceder a este formulario, presione el botón **Turnos** y aparece la siguiente imagen de la pantalla.

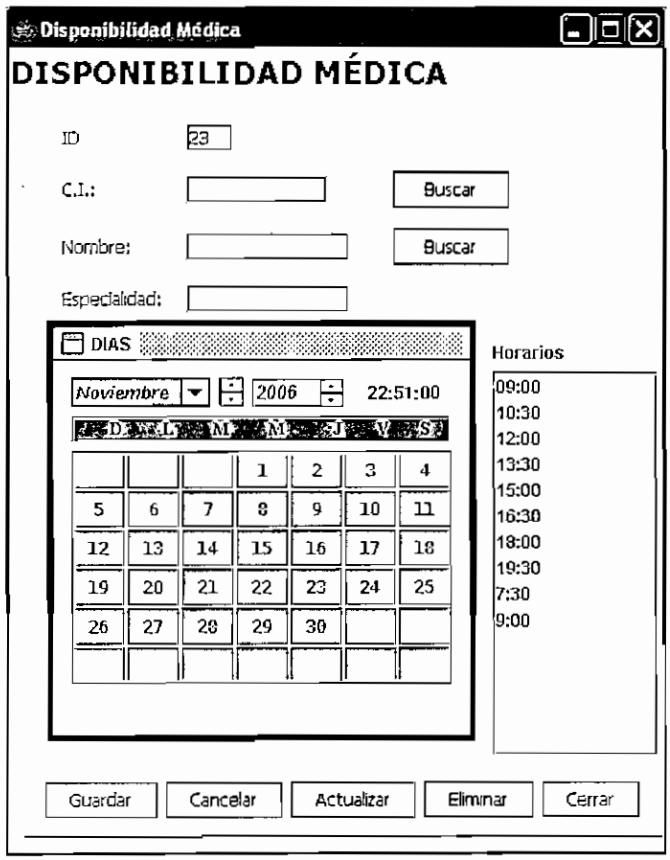



**Figura 4C.9 Disponibilidad Médica**

Se ingresa el número de cédula del doctor, se presiona el botón **Buscar**, una vez que aparecen los datos del médico, seleccionar un horario de disponibilidad y cerrar la pantalla.

### Trabando con los Pacientes

Para trabajar con los pacientes el sistema cuenta con la gestión de pacientes, en la que se dispone de la opción de agregar uno en el caso de no existir previamente, para esto se puede dirigir en el menú: **Paciente → Gestionar Paciente**, donde aparecerá la pantalla que se muestra a continuación (figura 4C.10), donde se manda a consultar la información de un paciente al colocar el apellido y presionar el botón **Buscar**.


Figura 4C.10 Manejo de Datos de los Pacientes

Para añadir un registro, se presiona el botón **Nuevo**, donde se habilitan los campos de información del paciente a ingresar, para almacenarlos presione el botón **Agregar**, caso contrario el botón **Cancelar**. Para el resto de funciones, siga el procedimiento descrito en los formularios de gestión de usuario y doctor.

### Administrando Citas

Una vez que el paciente ya existe en el sistema, cuando este quiera establecer, pagar, y asistir a una cita, el sistema cuenta con herramientas que ayudarán al personal a llevar dichas tareas.

Así para establecer una cita, se dirige a través del menú: **Administrar Cita** → **Establecer Cita** en donde aparece la pantalla para registrar una cita (figura 4C.11), en base a la búsqueda del paciente luego de digitar su número de cédula, y en los combos se debe seleccionar un doctor y un turno existente.

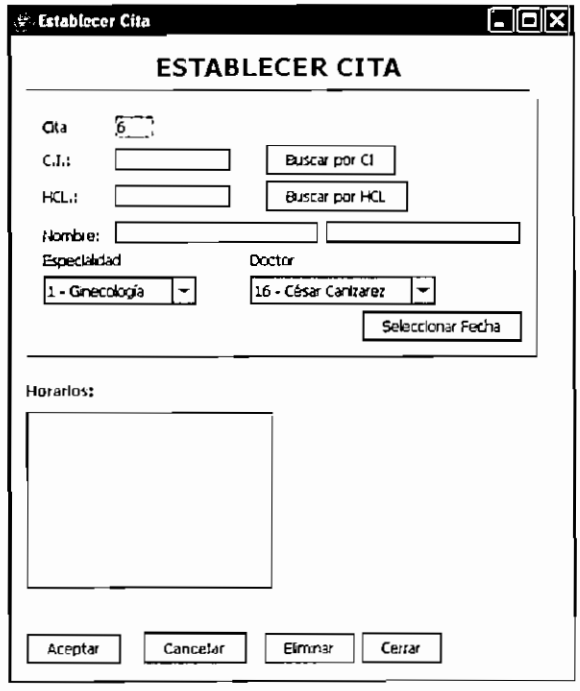



Figura 4C.11 Establecer una Cita

El la lista de turnos médicos se seleccionaría la fecha de la cita, y con el botón **Seleccionar Fecha**, se la presenta en un recuadro de la pantalla, si desea agregar la cita, presione **Agregar**, caso contrario **Cancelar**.

Un paciente puede cancelar su cita, y el sistema permite almacenar esta incidencia a través de la pantalla (figura 4C.12) que aparece al dirigirse en el menú: **Administrar Cita → Pago Cita**

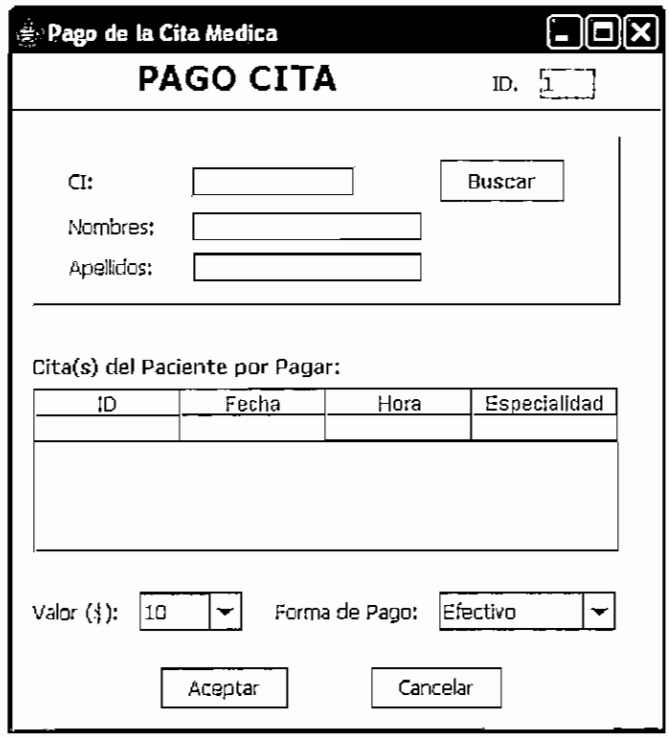



**Figura 4C.12 Pago Cita**

Al ingresar la cédula del paciente y presionar la tecla **Enter**, o en su defecto el botón **Buscar**, aparecen en la parte media las citas pendientes de pago que posea el paciente, es posible entonces, seleccionar un monto y una forma de pago para dejar registrado a través del botón **Aceptar.**

Ya en la cita, el sistema permite la toma de signos vitales, para esto se dirige a través del menú: **Signos Vitales → Gestionar Signos Vitales** donde se muestra una lista con los pacientes que están autorizados para capturar los signos vitales a través de los dispositivos inalámbricos que la aplicación permite, luego de haber cancelado el pago de la cita.

A continuación se muestra une ejemplo de la pantalla de gestión de Signos Vitales (figura 4C.13) y luego la pantalla de captura de signos vitales (figura 4C.14).

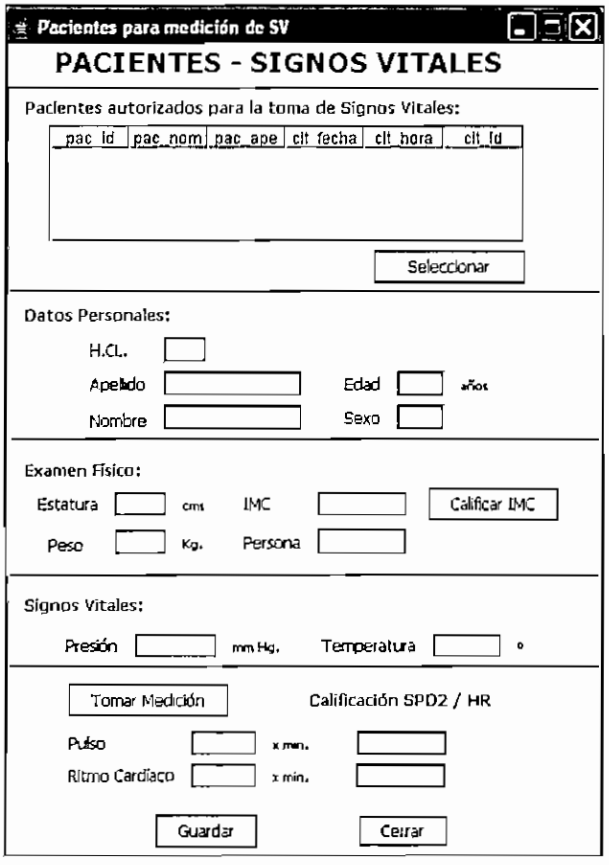



Figura 4C.13 Gestión de Signos Vitales

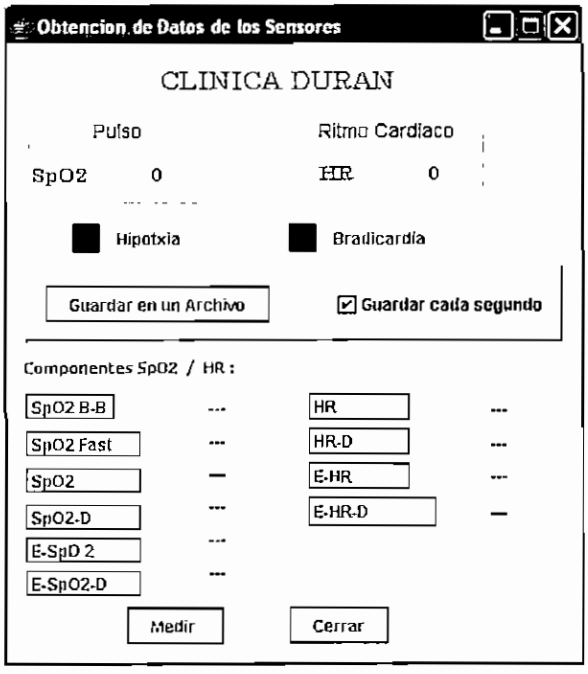



Figura 4C.14 Obtención de los Datos de los Sensores

El diagnostico médico de un paciente se puede revisar e ingresar a través de la pantalla de la siguiente figura, que se abre a través del menú: **Signos Vitales → Gestionar Signos Vitales.**

En esta pantalla se hace una búsqueda de un paciente existente al digitar el número de cédula y presionar el botón **Buscar**, con esto aparecen los datos del paciente, se permite revisar su último registro médico y almacenar uno nuevo, esta pantalla también incluye la capacidad de registrar la próxima cita con el paciente.

A continuación se muestra una imagen de la pantalla para este efecto.

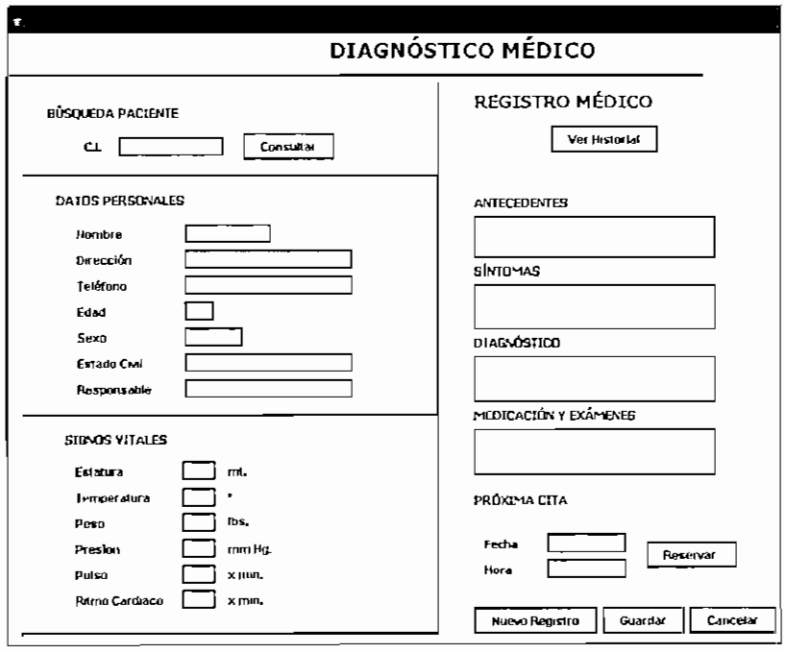



Figura 4C.15 Historial Médico

## Manejando Emergencias

Cuando un paciente ingresa en emergencias, es posible buscar en el sistema si existe este paciente, al digitar el número de cédula y mandar a buscar, pero también se puede ingresar un nuevo paciente y luego registrar signos vitales, datos de la atención médica para un historial de atención. En este formulario (figura 4C.16), además se registra el médico que le atendió al paciente y su estado en el momento de arribar a la unidad médica.

Para atender a un paciente en emergencia, se dirige por el menú: **Diagnóstico Médico → Hoja Emergencia**

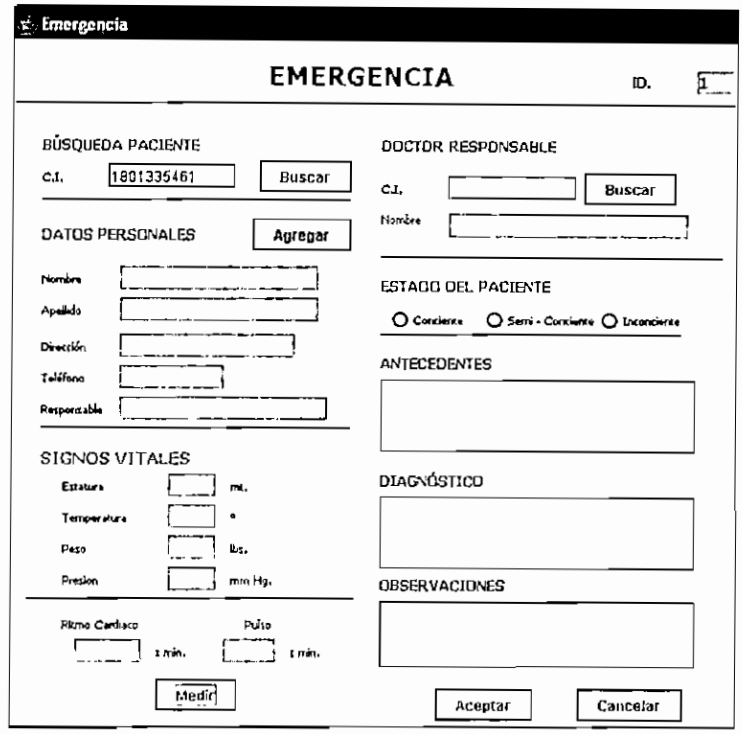



Figura 4C.16 Hoja de Emergencia

## Reportes del Sistema

El sistema permite obtener reportes de las consultas externas tratadas en una fecha determinada, como se muestra en la figura a continuación (figura 4C.17).

Para llegar a esta opción, se dirige a través de la ruta de menú: **Reportes → Reportes Consulta Externa**

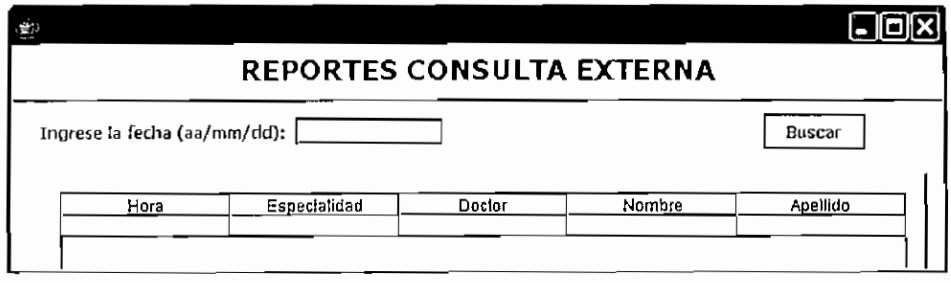



Figura 4C.17 Reportes Consulta Externa

Y también de los casos que se atendieron en Emergencias, dada una fecha para la búsqueda. A continuación se presenta un formulario en donde se presenta dicha información (figura 4C.18):

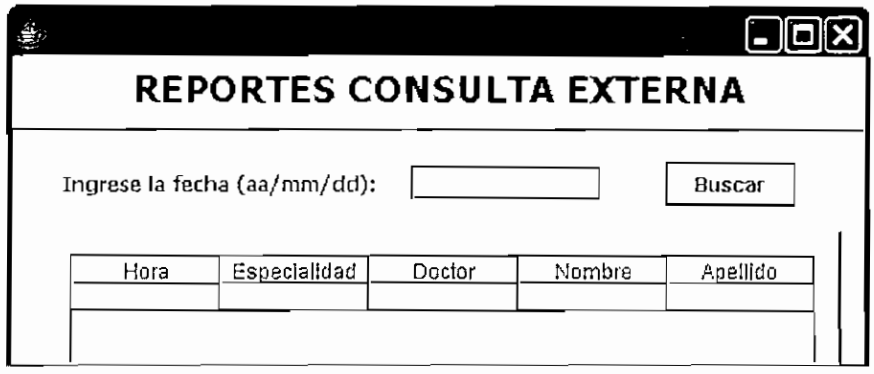



Figura 4C.18 Reportes Consulta Externa

Para llegar a esta opción, se dirige a través de la ruta de menú: **Reportes → Reportes Emergencia**

### Cambio de Sesión

En el sistema se puede cambiar de la sesión actual e ingresar con otro usuario, para esto se dirige en el menú: **Archivo → Cambio de Sesión** para lo cual aparece la pantalla tal cual al inicio del programa (figura 4C.5).

### Salida del sistema

En cualquier momento se puede cerrar la aplicación a través del menú: **Archivo → Salir**