Universidad Don Bosco
Facultad de Ingeniería
Escuela de Ingeniería Electrónica

Trabajo de graduación:

"Diseño de acceso inalámbrico al sistema de información de un hospital desde PDA"

Para optar al grado de:

Ingeniero en Telecomunicaciones

Presentado por:

Edgard Mauricio Dueñas Alvarenga
Carlos Ernesto Flores Ayala
José Rafael Zavala Trigueros

Septiembre 2007
Soyapango– El Salvador – Centro América

UNIVERSIDAD DON BOSCO

AUTORIDADES

Ing. Federico Miguel Huguet Rivera
Rector

Pbro. Víctor Bermúdez Yánez
Vicerrector Académico

Lic. Mario Olmos Argueta
Secretario General

Ing. Ernesto Godofredo Girón
Decano Facultad de Ingeniería.

Ing. Oscar Duran Vizcarra
Director Escuela de Electrónica

Ing. Juan Carlos Castro Chávez
Asesor del Trabajo de Graduación

Lic. Ana Daysi Montecino
Ing. Ingrid Lara
Ing. Marcos Tulio Portillo
Jurado Examinador

Universidad Don Bosco
Facultad de Ingeniería
Escuela de Ingeniería Electrónica

JURADO EVALUADOR DEL TRABAJO DE GRADUACIÓN

“Diseño de acceso inalámbrico al sistema de información de un hospital desde PDA”

_____
Ing. Juan Carlos Castro Chávez
Asesor del Trabajo de Graduación

_____
Lic. Ana Daysi Montecino
Jurado Evaluador

_____
Ing. Ingrid Lara
Jurado Evaluador

_____
Ing. Marcos Tulio Portillo
Jurado Evaluador

Agradecimientos

Cuando empezó esta aventura veía tan lejano su final dado lo complejo y amplio que se hacia a medida pasaba el tiempo y todas la dificultades que encontrábamos en el camino las cuales me hacían a veces dudar de mis capacidades.

Sin embargo lo logramos y digo lo logramos porque mi esfuerzo individual hubiera sido inútil, sin la suma de los esfuerzos de mis otros dos compañeros de aventura que se convirtieron en camaradas y amigos de por vida, no solo en el transcurso de la elaboración de la tesis sino, en la etapa de la vida en donde aprendí a ser ingeniero y me convertí en uno junto con ellos, por eso es que quiero empezar agradeciéndoles a mis colegas. Pero todo esto no hubiera sido posible sin el apoyo incondicional de mi madre Elizabeth que con tanto sacrificio dio toda su energía, amor, cariño y corazón, día tras día durante mas de treinta años para que yo llegara a este momento y conteniendo todo el amor y afecto que le tengo no encuentro una palabra que sea capas de expresar todo mi agradecimiento solo puedo decirle que es inmenso el amor que le tengo y que no cabe en mi pecho todo este sentimiento por lo que mis lagrimas al escribir estas líneas son parte de este amor tan intenso que siento por ella, gracias por estar y por existir para mi.

Agradezco también a Roxana que apareció como un oasis en medio del desierto que vino a llenar mi vida de alegría y fue como un rayito de sol cuando la oscuridad me estaba rodeando, con toda su alegría me lleno de entusiasmo y dio un suspiro para completar la recta final de este caminar que fue tan difícil de superar, y me enseño a soñar nuevamente.
A la Mari que con toda su entrega desinteresada y amor de madre me colmo de atenciones durante tanto tiempo. A mi familia que con todo su apoyo y cariño me enseñaron a querer salir adelante y convertirme en un profesional.
A todos mis amigos y personas que convivieron conmigo y de las cuales aprendí y me llevo una parte de cada uno de ellos, gracias e eso soy la persona que soy,

Y finalmente al mas importante a Dios que siempre me ayudo y lleno de bendiciones, jamás me sentí solo, siempre me sentí amparado por el y en los momentos mas difíciles, el fue quien me cargo y acobijo para que todo saliera bien, por mas complicaciones y trabas que por circunstancias de la vida aparecían siempre mediante el poder de mi padre Dios todo salía bien, mil gracias por quererme a pesar de equivocarme y además creer en mi.

Edgard Mauricio Dueñas Alvarenga

Al final de esta meta es necesario reflexionar el como y por que la he alcanzado, y ambos tiene similitudes, he llegado hasta aquí por las personas que de una u otra manera me dieron su apoyo y confianza, y es por ellas también el por que nunca pensé en retirarme y siempre tubé como única opción el alcanzarla.

Agradezco a Dios por darme la oportunidad de haber finalizado mis estudios y de haber puesto a personas tan especiales en mi camino, y por haberme llenado de esperanza cuando mas lo necesite.

A mis padres (Carlos y Marta): Por de de verdad aprecio los múltiples sacrificios que tuvieron que afrontar para que yo pueda ahora escribir estas líneas, de verdad gracias y ahora cuenten con mi apoyo incondicional para afrontar los desafíos venideros.

A mis hermanos (Sandra y Ricardo): Por su haberme apoyado y motivado en el transcurso de este proyecto de vida.

A mis familiares (Susana, Antonio, Franklin, Elsita) Infinitas gracias por haber confiado en mi y por todo ese apoyo que siempre me mostraron de una forma incondicional, de verdad muchas gracias, y espero nunca defraudar ese esfuerzo y confianza en mi depositados.

A mis amigos (Juan Carlos, Jonathan, Cristian, Roberto, Francisco, Elsy, Roxana, Leydi, Rosa, Alma, Carmen, Mónica, Rafael, Mauricio, Miguel, Montoya, Erick): Con los que sude la camiseta, y con los que aprendí, a ver las cosas desde otra perspectiva, gracias por su apoyo, y solidaridad y por todas esas muestras de apoyo y cariño.

A los Docentes: Por haber dado la guía de donde y el que aprender, en el momento, y la forma debida.

A todos aquellos que no mencione pero que sin su ayuda no podría estar finalizando esta meta.

“Si he visto más lejos ha sido porque he subido a hombros de gigantes.” (Newton)

A todos Gracias
Carlos Ernesto Flores Ayala

He concluido otra etapa mas de mi vida, me siento satisfecho de los logros obtenidos, no se en que momento discerní orientarme en el área de las telecomunicaciones, pero que buena decisión tome. Me es muy difícil poder agradecer a todas las personas que han intervenido directa, e indirectamente, en la culminación de tan anhelado logro, pero de alguna u otra manera debo de hacerlo.

Gracias doy a Dios todo poderoso, por muchas cosas, por la vida, la salud, y en lo que respecta a los agradecimientos, por la oportunidad que me ha brindado de concluir con mis estudios universitarios, a La Virgen Maria, por interceder siempre por mí y por ser luz en mi camino, a San Juan Bosco, padre y maestro de la juventud, por guiarme siempre de su mano y ser protector.

A mis padres, José Neftali y Maria Carmela, por haber confiado en la educación salesiana, por haberme permitido demostrarles que yo era, soy y seré capaz siempre de salir adelante, por haber tolerado todas las malas acciones de mi parte hacia ellos, por haberlos preocupado en determinados momentos de sus vidas, por haberme dado la vida sencillamente, por ser el mejor ejemplo de vida, por enseñarme no solo con palabras, si no también con hechos, porque nunca dudaron reprenderme cuando era necesario, por haberme dado la oportunidad de concluir con mis estudios universitarios, por darme la oportunidad de que mi futuro sea el mejor, gracias padres por ser las personas que son, espero se sientan orgullosos de lo que sembraron en mi. A mis hermanos (a), Neftaly Antonio, Jorge Alfredo y Ana Silvia, por ser parte de mi vida, por estar siempre a mi lado, por ayudarme a culminar este logro, por alentarme cuando lo necesite, por cubrirme cuando lo necesite también, recuerden que eso es esencial en una hermandad. A Flor de Maria Guzmán (mi novia), a ella, por ser la persona que me ha enseñado a ser humilde, respetuoso, responsable. Porque me ha tolerado por 13 años y a confiado en mi capacidad de hacer las cosas, por permitirme demostrarle mi amor y respeto hacia ella, por dejarme incorporarme en su núcleo familiar y por todo el amor que me ha brindado, el cual ha sido motor y aliciente en el transcurso de mi carrera. A mis demás familiares, abuelos, tíos, primos, sobrinos (casi ni tengo), que directa o indirectamente fueron parte de este logro, por estar siempre pendientes de mi y por preguntar sobre el avance de mi carrera, hoy les digo gracias de todo corazón. A mis compañeros de universidad y demás amigos, gracias por ser como son, por apoyarme, por demostrarme la verdadera amistad y estar en todos los momentos de mi vida, espero también se sientan orgullos de tener un amigo al cual llaman “El Abuelo”, y siempre estén a mi lado.

A Carlos Flores y Edgard Dueñas, por haberme permitido culminar junto a ellos este logro, por haber aguantado junto a mi las inclemencias que vivimos en el transcurso de la realización de nuestro trabajo de graduación, por las palabras de aliento que me brindaron cuando todo parecía no tener salida, por confiar en mis conocimientos, y por esperar a que egresara por segunda vez para poder unirme a ellos en esta ultima batalla.
Es un agrado decirles a todos que lo logre, de ahora en adelante soy el “Ing. José Rafael Zavala Trigueros”, gracias y espero ser ejemplo para los que están tratando de alcanzar lo mismo que hoy he logrado.

José Rafael Zavala Trigueros
(Alias El Abuelo, oyebob)
(Dedicado a mi abuelo Antonio
Cornelio Trigueros y mí
Abuela que nunca conocí
Maria Esperanza Monico)

Indice

Introducción

En la actualidad los procesos médicos están volviendo su mirada a las tecnologías de información, por ejemplo redes inalámbricas, telemetría, asistencia remota y muchas otras aplicaciones las cuales ya en el primer mundo tienen un buen nivel de depuración, sin embargo aún hay mucho que hacer, especialmente en países como el nuestro.

En los próximos capítulos, detallamos los aspectos tanto técnicos como administrativos a tomar en cuenta en una aplicación de este tipo. La importancia que tiene una excelente compatibilidad entre todos los equipos que se involucran en el cuidado médico de las personas es fundamental, es por eso que hemos dedicado un capitulo completo para abordar el tema y basado en estudios de países con más experiencia como España, Chile, Bélgica y Alemania.

Iniciamos tratando el marco que envuelven los procesos médicos en nuestro país y como la poca inversión en tecnología a hecho que nos quedemos rezagados y con procesos ineficientes en donde la tecnología debe jugar un papel más protagónico. Sin embargo en otros países sí se tienen muy desarrolladas distintas aplicaciones y redes de información.

Luego de generar un vistazo de los actuales procesos médicos, entramos de lleno al tema de la compatibilidad electromagnética en entornos hospitalarios y nos orientamos a desglosar los distintos aspectos que pueden intervenir en el equipo hospitalario. Posteriormente detallamos las diferentes tecnologías inalámbricas que tienen más uso en este momento, así como también las diferentes aplicaciones que se pueden desarrollar con estas tecnologías para posteriormente poder mostrar la incursión de computadoras de bolsillo en dichas aplicaciones y su compatibilidad con las redes inalámbricas.

Capitulo 1.

1. Tecnologías de la información en entornos hospitalarios.

1.1 Introducción.

Las TIC's (Tecnologías de la Información y Comunicaciones) se están convirtiendo en una herramienta que cada vez toma más y más importancia en los entornos hospitalarios, aún en países subdesarrollados como el nuestro. En nuestras visitas al Hospital Bloom (hospital que decidimos tomar como referencia debido a la capacidad para atender pacientes ya que es un centro hospitalario de tercer nivel por su misma capacidad de atención y complejidad) encontramos muchos proyectos que tendrían gran impacto en los pacientes y que se tienen proyectados para un futuro, lastimosamente la situación precaria en la que se encuentran la mayoría de nuestros hospitales impiden que se lleven a cabo proyectos como el que proponemos y que en otros países están muy depurados.

En este capitulo iniciamos con los avances tecnológicos en temas de información especialmente a los concernientes al cuido de los pacientes en nuestro país (basándonos principalmente en el Hospital Bloom), tratamos de describir algunos de los procesos a los que tuvimos acceso, ya que como sabemos es muy difícil tener un acceso completo a equipo e información confidencial, pero gracias a la ayuda de la universidad y la colaboración del departamento de informática del Hospital Bloom, conocimos de primera mano la situación referente a nuestro tema en dicho hospital.

Cabe destacar que a pesar de todas las dificultades que se tienen en nuestros entornos hospitalarios en general, se tiene la buena intención de querer modernizar los sistemas informáticos, ya que estos deben ir de la mano con los avances médicos y no se pueden divorciar, para beneficio de todos.

En nuestro país debido a la poca inversión en investigación y estudios no se tienen muchos datos de la incidencia que tienen los campos electromagnéticos en estos entornos, por lo que los ejemplos que citamos son de países en donde ya hay grandes avances en este tema, con recomendaciones técnicas que en países como el nuestro pueden ser utilizadas y que además nos han servido como material de consulta.

1.2 Tecnologías de la información en entornos hospitalarios en el Salvador.

El manejo de la información de un paciente es sumamente delicado, se tiene que administrar con mucha responsabilidad y privacidad. En las visitas que hemos realizado al Hospital Bloom se nos han descrito y explicado procesos de manejos de información de los pacientes, ya que estos pueden venir de consulta externa, hospitalización, urgencias y referidos de otros hospitales. El Hospital Bloom es catalogado como tercer nivel[1], por su capacidad y por contar con todas las especialidades con las que debe contar un hospital de tercer nivel.

[1] http://www.mspas.gob.sv/infraestru_servicios.asp

Los pacientes de hospitalización efectúan visitas programadas por los médicos encargados. Los pacientes de consulta externa inician su proceso en la entrevista con su médico, quien prescribe lo necesario para el tratamiento a seguir; tales solicitudes son llevadas al área de recepción del Hospital, donde se programan los estudios y se señala la hora y el día en que se realizaran, todo esto por medio de un sistema computarizado. Toda la información referente al proceso, actualmente es llevada en computadora por un sistema de citas que fue creado en el hospital por su equipo de informática.

Podemos resumir la creación de la ficha de un paciente en general de la siguiente forma[2]:

- Ingreso de Paciente*:* Es el primer paso, y se refiere a la llegada del paciente al hospital en donde este se identifica en recepción del hospital.
- Creación del Expediente*:* se constituye en su conjunto, por las personas que forman parte del perfil de pacientes; este requerirá los datos generales del paciente, será llenado un formulario a mano, el cual se archivará
- El expediente, será entregado al archivista, que revisará que la solicitud de expediente clínico este debidamente completada. El expediente se encontrará en el departamento de admisión y registro médico a la espera de que nuevos datos y exámenes sean ingresados en él en un futuro.

En la figura 1.1 observamos un diagrama de flujo simplificado y generalizado para la creación de un expediente médico. En donde el paso de la elaboración del expediente es hecho de forma manual y en algunos casos como en el Hospital Bloom se hace de forma digital también, lo que ayuda a hacer más eficientes los controles de citas.

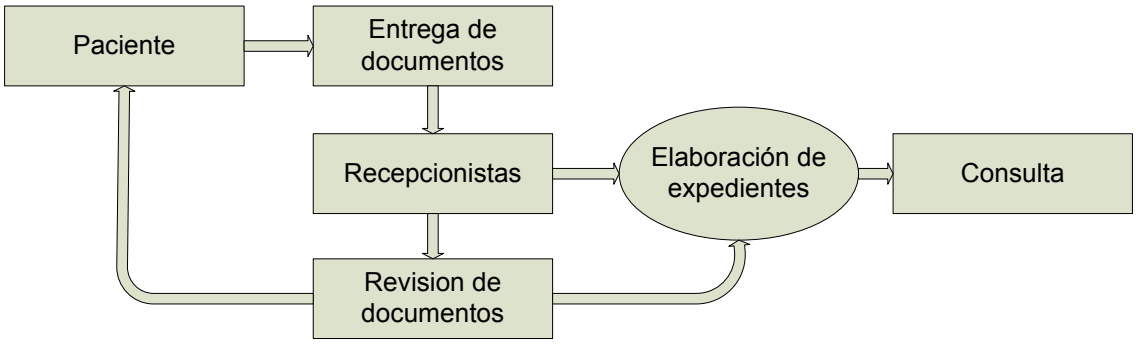


Figura 1.1 Recepción de información para creación del expediente de un paciente[3].

Los documentos básicos que conforman el expediente clínico para un niño tal como es el caso del Hospital Bloom serían los siguientes:

- Hoja de identificación.
- Registro de identificación del niño.
- Consulta médica 1ª vez-historia clínica.

[2] Información recopilada en entrevistas con personal de informática del Hospital Bloom.
[3] http://www.mspas.gob.sv/documentos.asp

- Consulta médica subsiguiente-historia clínica.
- Escala simplificada de evaluación del desarrollo.
- Grafica de crecimiento infantil peso/edad.
- Grafica de crecimiento infantil peso/talla-perímetro cefálico.
- Atención de crecimiento y desarrollo-hoja de consulta de 1ª vez.
- Atención de crecimiento y desarrollo-hoja de consulta subsecuente.
- Hoja de observaciones y cuidados de enfermería.
- Hoja de exámenes de laboratorio.
- Hoja de informes radiológicos.

Es de resaltar que en los procesos descritos anteriormente es muy poca la intervención de sistemas modernos de información, existe poco interés en el desarrollo y estudio de aplicaciones, además de una gran carencia de recursos tecnológicos en estos centros hospitalarios.

Las deficiencias que pudimos notar en los procesos básicos de registros de pacientes en nuestras visitas al Hospital fueron las siguientes:

- Al manejar datos tan variados, el posterior acceso de la información se vuelve lenta e ineficiente, se convierte en un sistema burocrático y tardío para el paciente y para el personal médico del hospital, además que se debe de tener un control de las personas que archivan esta información tan valiosa. Por lo que es necesario establecer un registro acerca de las entradas y salidas de cada expediente clínico, en el cual se haga constar información relevante del préstamo como número del expediente clínico, fecha de préstamo, solicitante y destinatario, fecha de devolución, servicio donde se utilizara, etc. Son controles que hacen al sistemas más lento. Además, impedir que estos datos sean leídos, copiados, ò alterados es un poco difícil de controlar ya que depende más de factores éticos correspondientes a cada persona. En caso de verificar que la información fue ò esta siendo manipulada, seria recomendable imponer sanciones ante dicha falta. Con todo lo anterior lo que se busca es proteger el derecho a la privacidad del paciente, la cual se ve muy vulnerable al haber una irregularidad en el área de archivo.

- Es necesario diferenciar entre el derecho de acceso a la información sobre salud y el derecho que se tiene al acceso de datos personales, ya que el primero se refiere a toda aquella información relacionada con enfermedades, tipos de tratamientos y exámenes, procedimientos quirúrgicos, etc. a la cual toda persona tiene derecho, caso contrario sucede con la segunda donde se deben de tener normalizado a quien se le permitirá conocer dicha información.

- Falta de una política de administración y depuración de archivos. Cada expediente se compone de una gran cantidad documentos de diferente tipo y tamaño, por lo que se vuelve más difícil la adecuada manipulación de estos.

Muchos de estos problemas se pueden solventar al digitalizar toda esta información pero para dar este paso aún falta mucho trabajo e inversión en tecnologías.

1.3 Tecnologías de la información en entornos hospitalarios a nivel mundial.

La instalación de redes inalámbricas en centros de salud y hospitales se ha convertido en un área importante de actividad por la cantidad de aplicaciones que se están desarrollando. Cada vez más, se considera su capacidad para facilitar el acceso, desde cualquier punto, a recursos de diagnóstico o conocimiento especializado, y están introduciendo aplicaciones más versátiles y flexibles en el diagnóstico médico y en el tratamiento y atención al paciente. En definitiva, la utilización de sistemas inalámbricos integrados para aplicaciones en entornos hospitalarios, supone un funcionamiento más eficiente, efectivo y competitivo del sistema hospitalario, al dotarle de una mayor flexibilidad y movilidad en la monitorización de los pacientes, de un seguimiento continuo de sus patologías y de una reducción de los costos de atención a los mismos. En los últimos años ha habido un notable incremento de la demanda de estos sistemas en varias partes del planeta. Junto con el crecimiento de estas aplicaciones, ha crecido también la preocupación sobre las posibles interferencias producidas por otros sistemas de radiocomunicaciones. Por ejemplo, en febrero de 1998, ocurrió un incidente en el Centro Médico Baylor de Dallas, Texas, en el que el 50% del sistema de telemetría se bloqueó por la interferencia causada por una estación de televisión local en pruebas de TV de alta definición[4]. Estos incidentes, entre otros, ponen de manifiesto la necesidad de una cuidadosa asignación de la banda de frecuencias para minimizar los posibles riesgos que estas interferencias puedan causar en la atención hospitalaria. La utilización de nuevos sistemas inalámbricos de telemetría médica en las bandas de frecuencias asignadas, deberían llevar asociados un proyecto técnico detallado de los posibles efectos o riesgos sobre emisiones radioeléctricas y la garantía de compatibilidad electromagnética entre el equipo utilizado y las redes desplegadas, a fin de evitar potenciales riesgos en la atención y tratamiento del paciente.

La gran difusión y la amplia disponibilidad de WLAN (Wireless Local Area Network, Red de Area Local Inalámbrica) para el público en general han dado lugar a un interés creciente por parte de las instituciones hospitalarias en las soluciones inalámbricas, tanto como parte de sus propias redes corporativas de comunicación, como soporte de aplicaciones y desarrollos específicos de telemedicina. La limitación de estas posibilidades, ha supuesto hasta hace poco importantes limitaciones en la atención hospitalaria, sus comunicaciones y su planificación.

Teóricamente, con las normas IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos) 802.11b y, más recientemente, con la IEEE 802.11g, ambas utilizando las bandas de 2,4 GHz, se consigue una cobertura superior a 100 m en espacio abierto. Con la IEEE 802.11b se puede conseguir una taza de transferencia de 11 Mbps, con la IEEE 802.11g se pueden alcanzar los 54 Mbps, e incluso superiores con la IEEE 802.11n futura.

Sin embargo, el concepto de espacio abierto en un hospital resulta una utopía, caracterizado en concreto por superficies metálicas, ascensores, zonas aisladas y

[4] "Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios". Colegio oficial de Ingenieros en Telecomunicaciones Madrid España 2005.

altamente equipadas, y todo esto combinado da lugar a una importante reducción de la cobertura y del rendimiento. Con IEEE 802.11g, entre aproximadamente 10 m y la primera pared se consigue la capacidad máxima, pero rápidamente esta capacidad disminuye, requiriendo la instalación de más antenas. Por lo tanto, una red WLAN amplia para un hospital, requiere un estudio detallado incluso sin consideraciones de interferencias, Roaming, seguridad y organización. La cobertura limitada y la necesidad de múltiples antenas hacen necesaria una planificación cuidadosa. Para las normas IEEE 802.11b e IEEE 802.11g hay en Europa 13 canales disponibles. La existencia de interferencias entre canales obliga a que las antenas de una sala utilicen canales suficientemente separados (por ejemplo, 1, 7 y 13). Las interferencias entre diferentes plantas se deben tener en cuenta en la planificación de la instalación.

1.3.1 Algunos ejemplos.

En el Hospital Universitario de Gante, Bélgica, en el Servicio de Traumatología, ha comenzado en marzo de 2004 un proyecto piloto destinado a evaluar el acceso inalámbrico desde la cama del paciente a la HCE (Historia Clínica Electrónica)[5]. En este hospital, como en muchos otros, se había instalado previamente una red DECT (Digital Enhanced Cordless Network, Red Inalámbrica Digital Mejorada) para permitir la telefonía inalámbrica. El piloto se inició reutilizando la red de antenas DECT existentes por medio de tarjetas PCMCIA–DECT (Personal Computer Memory Card Internacional Association, Asociación Internacional de tarjetas de Memoria de Computadoras Personales-DECT) en las PC´s (Personal Computers, Computadoras Personales) portátiles. Los puntos positivos están en la instalación de DECT ya existente, la cobertura adecuada y la seguridad del hardware permitiendo unas velocidades razonables. Como el ancho de banda para los datos en la red DECT es bastante limitado, la utilización de las partes gráficas de la HCE está limitada.

Pruebas realizadas durante varios meses revelaron problemas iniciales con la conexión y el Roaming. Han hecho falta cambios de organización y hardware para garantizar el funcionamiento correcto durante 24 horas (baterías extra, cargadores, procedimiento de recarga, etc.). Aunque la mayoría de los problemas se solucionaron, el Roaming no se pudo garantizar en todas las ocasiones, produciendo casos de falta de conectividad y el ancho de banda limitado de DECT impidió el acceso a partes gráficas de la HCE y a futuras expansiones.

A partir de esta experiencia, se ha instalado una red local basada en el estándar IEEE 802.11. Aunque la tecnología asociada a estas normas ha mejorado sustancialmente en los últimos dos años, todavía han aparecido ciertas diferencias entre fabricantes, tales como:

- El Roaming automático no siempre es tan rápido como sería de desear (conexión a 2 Mbps cuando estaba próxima a los 54 Mbps).
- Puntos de acceso temporalmente apagados cuando no detectan actividad.
- Problemas de tráfico en algunas aplicaciones.

Como aspectos positivos:

- Destacar que la conectividad nunca se pierde aunque disminuya.

[5] "Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios". Colegio oficial de Ingenieros en Telecomunicaciones Madrid España 2005.

- Están garantizadas velocidades elevadas.
- Se abre la posibilidad de la utilización de aplicaciones gráficas de manera intensiva.

La seguridad de una red WLAN es un problema importante y más en un centro hospitalario donde la naturaleza de los datos alcanza a la protección de datos inalámbricos. La norma de seguridad de WLAN WEP (Wired Equivalent Privacy, Equivalente Cableado de Privacidad) que cifrar mensajes con una clave estática, puede romperse en varias horas incluso si se toman medidas de seguridad adicionales. Actualmente, la mejor opción es implementar WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi) que utiliza algunas de las nuevas normas 802.11i junto con autentificación del tipo RADIUS (Remote Authentication Dial In User Service, Autenticación de Marcado Remoto del Servicio de Usuario). En este hospital, además se instala un firewall adicional entre WLAN y LAN (Local Area Network, Red de Area Local) para minimizar los riesgos.

En el area de Maternidad del Hospital Gregorio Marañón, de Madrid, se ha inaugurado una nueva red Wi-Fi, que permite a los profesionales disponer de la información sobre sus pacientes en cualquier lugar del centro de manera automática, ya que el sistema se actualiza constantemente aportando datos recientes sobre el estado o las incidencias que ocurren[6]. Se sustituye la imagen del médico o estudiante acudiendo a la cama del enfermo con un montón de papeles por otra más moderna del médico con una PC portátil con todos los datos del paciente. La utilización de las Table PC supone un paso más con respecto al uso de PDA (Personal Digital Assistant, Asistente Personal Digital) ya que aunque estas últimas son más cómodas de llevar, su lectura es más difícil y algunas pruebas no se pueden visualizar.

También se ha instalado una red WLAN en el Hospital Infantil Universitario Niño Jesús, de Madrid. En este caso, y gracias a un estudio realizado en el hospital, se ha llegado a la conclusión de que la transmisión de datos por redes inalámbricas no es perjudicial para la salud, es decir, que no hay ninguna relación causa-efecto entre la exposición a radiaciones de estas frecuencias y patologías conocidas, debido a que los niveles de señal que se utilizan están bastante por debajo de los considerados perjudiciales. Asimismo, se ha establecido que no hay interferencias entre la red WLAN y los servicios de comunicación clásicos, ni con instrumentos médicos propios del entorno. El hospital mallorquín Son Llàtzer se ha situado entre los más innovadores de Europa en cuanto a la utilización de las TIC's. En la actualidad, el 95% de los procesos del centro se hacen sin necesidad de utilizar ningún papel. Se ha dotado al personal de enfermería y a los médicos con dispositivos Table PC y PDA's para poder consultar la HCE de cada paciente en cualquier lugar y momento, y poder acceder al HIS (Sistema de Información Hospitalario) completamente informatizado. Para posibilitar la conexión en línea de estos aparatos se ha desplegado una red inalámbrica Wi-Fi. Los beneficios obtenidos de este proyecto, según los usuarios del mismo, fueron la rápida implementación del sistema, la movilidad que permite el sistema, el acceso inmediato a la información, la mejora del servicio y el hecho de que la curva de aprendizaje fuera totalmente nula. En el Hospital Carlos III, se realizó en el año 1998 un sistema de Telemedicina sobre GSM (Global System for Mobile Comunications, Sistema Global para las Comunicaciones Móviles) integrado con un sistema de información clínica incluyendo un servidor WWW (World

[6] "Informe sobre emisiones electromagnéticas de los sistemas de telefonía móvil y acceso fijo inalámbrico". Colegio Oficial de Ingenieros de Telecomunicación. Madrid España 2001

Wide Web) con acceso móvil. El sistema incluye conectividad a redes inalámbricas tipo GSM y DECT accesibles con terminales tipo comunicador o PDA's. El Hospital Municipal de Badalona presentó en 2001 una red inalámbrica de gestión hospitalaria para el uso de PDA's por el personal de enfermería, con el fin de registrar la toma de constantes de los enfermos ingresados, seleccionar el tipo de dieta y mostrar gráficas. Una aplicación similar se encuentra en la Fundación Hospital de Calahorra, en la Rioja, desde comienzos de 2002. Otras aplicaciones sanitarias de este tipo se encuentran en el C.H.U. Juan Canalejo de La Coruña y en el Hospital de la Santa Creu i Sant Pau de Barcelona para cuidados continuados en Diabetes Mellitus[7].

[7] "Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios". Colegio oficial de Ingenieros en Telecomunicaciones Madrid España 2005.

Capitulo 2.

2. Telemedicina y telemetría.

2.1. Introducción

La tecnología ha dado saltos agigantados en los últimos años, esto ha permitido integrar diferentes áreas de ella para mejorar la calidad de vida de las personas.
El despegue de Internet y el impulso de la Sociedad de la Información en todos los países industrializados, ha dado lugar a un nuevo entorno donde es posible, entre otros factores, una mayor interacción entre los sistemas hospitalarios y los ciudadanos.
La aplicación de las TIC's a la atención médica permite una mayor flexibilidad y movilidad que suponen una mejora en la calidad y una reducción de costos de la atención al paciente. Por otra parte, la utilización de sistemas inalámbricos integrados para aplicaciones clínicas en un recinto médico, supone un funcionamiento más eficiente, efectivo y competitivo del sistema hospitalario.

Como ya mencionamos son muchas las ventajas de implementar las TIC's en ambientes hospitalarios, pero el despliegue de estos sistemas de radiocomunicaciones en dichos entornos hacen necesaria una cuidadosa planificación de los mismos. Esta planificación es necesaria para evitar interferencias no sólo entre estos sistemas, sino entre éstos y el equipo médico y clínico existente en un hospital.
Por lo tanto, en estos ambientes se hace imprescindible una adecuada planificación y gestión de los sistemas radioeléctricos para evitar interferencias.

2.2 Telemedicina

Vamos a empezar definiendo lo que es telemedicina, que en pocas palabras es "medicina a distancia", definiciones más detalladas serían[8]:

- La investigación, monitorización y gestión de pacientes y personal usando sistemas que permiten el acceso inmediato al asesoramiento de expertos y a información de pacientes, sin importar dónde se encuentre el paciente o su información.
- El uso de tecnologías de información electrónica y comunicaciones para proporcionar y soportar cuidados médicos cuando la distancia separa a los participantes.

La prestación de servicios de cuidados médicos, cuando la distancia es un factor crítico, usando tecnologías de la información y comunicaciones es válida para aquellos casos en donde el intercambio de información, diagnóstico, tratamiento y prevención no es oficial pero da una idea para un futuro estudio y diagnóstico del médico.

En resumen podemos decir que cualquier actividad relacionada con cuidados médicos (incluyendo diagnóstico, consulta, tratamiento y monitorización) que normalmente involucra un profesional y un paciente (o un profesional y otro que está separado en el

[8] "Telemedicina: construyendo la sanidad del futuro". José Luís Monteagudo Peña.

espacio, y posiblemente en tiempo), y que se facilita a través del uso de tecnologías de la información y las comunicaciones, es telemedicina.

Por lo tanto, la telemedicina consiste en la provisión de servicios médicos a distancia usando medios electrónicos y de telecomunicaciones. Desde sus orígenes, la motivación principal para su uso ha sido la de facilitar el acceso a los servicios del cuidado de la salud desde lugares remotos y aislados. Otro motivo típico ha sido su utilización como soporte a los equipos médicos en situaciones de emergencias médicas y de desastres. Sin embargo, cada vez más se considera su capacidad para facilitar el acceso desde cualquier punto a recursos de diagnóstico o al conocimiento especializado. La experiencia muestra que la telemedicina presenta un potencial muy apreciado para educación y formación evitando costos de tiempo y desplazamientos a los profesionales médicos.

Tradicionalmente, las limitaciones en las líneas telefónicas únicamente permitían intercambios de imágenes, de datos y de audio, por lo que las aplicaciones de Telemedicina estuvieron reducidas, inicialmente, a la videoconferencia y a la utilización de redes distribuidas para el acceso y el almacenamiento de datos. Posteriormente, se incorporó la posibilidad de acceso móvil a servicios, independientemente de la localización del paciente. El desarrollo de las tecnologías de comunicaciones personales se está extendiendo también, y como no podía ser de otra forma, también a los sistemas de salud pública y privados. Hay también, una serie de dificultades que incluyen la aceptación por parte de los pacientes y del personal médico, la privacidad, la seguridad y la infraestructura de soporte, que son puntos claves para la buena acogida a cualquier nueva tecnología.

2.3 Telemetría

Los dispositivos inalámbricos se pueden adaptar a monitores de parámetros fisiológicos transfiriendo los datos y permitiendo el seguimiento en un área limitada. La tecnología inalámbrica se puede integrar directamente con los sensores en un único aparato electrónico para facilitar la continuidad de la monitorización.

La telemetría es la medida remota de parámetros biológicos (ritmo cardíaco, presión sanguínea, temperatura), por medio de una línea telefónica o usando frecuencias de radio o infrarrojos, del espectro radioeléctrico de acuerdo a la tabla 2.1.

Sistemas inalámbricos utilizados en telemetrìa		
Estandar	**Frecuencias de operación**	**Tasa máxima de transferencia**
802,11	2,4 GHZ	2 Mbps
802,11a	5 GHZ	54 Mbps
802,11b	2,4 GHZ	11 Mbps
802,11g	2,4 GHZ	54 Mbps
HiperLAN/2	5 GHZ	54 Mbps
Home RF	2,4 GHZ	2 Mbps
Bluetooth	2,4 GHZ	721 Kbps
802,15 WPAN Low Rate	2,4 GHZ	250 Kbps
802,15 WPAN High Rate	2,4 GHZ	55 Mbps
IrDA	≥300 GHZ	2 Mbps

Tabla 2.1 Sistemas inalámbricos utilizados en telemetría[9].

La expansión de los dispositivos con posibilidad de comunicación inalámbrica permite que ya se encuentren disponibles a precios reducidos circuitos integrados con radios para estas aplicaciones. Los circuitos disponibles cada vez son más pequeños, más ligeros y más baratos.

Una aplicación de este tipo necesita una adaptación específica en cada aplicación. En una red inalámbrica típica, el paciente es portador de un pequeño transmisor de baja potencia con una antena. La unidad transmisora lee los datos que proceden de los sensores colocados en el cuerpo del paciente y los transmite al sistema conectado al receptor central, que se encuentra normalmente a corta distancia, y dispone de una o varias antenas receptoras. El sistema de antenas puede estar instalado en las paredes o el techo de una sala del centro sanitario.

Algunos equipos antiguos estaban diseñados para trabajar a frecuencias fijas, pero los modernos permiten el cambio ágil de frecuencia durante la instalación en el lugar requerido utilizando varios canales (generalmente contiguos) para permitir un acceso al espectro con anchos de banda mayores.

La instalación de estos sistemas tiene en cuenta tres consideraciones:

- El acceso al espectro de radiofrecuencia.
- Las licencias de radiofrecuencia.
- El cumplimiento de las normativas por parte de los equipos.

Los sistemas de biotelemetría no deben operar en los mismos canales ni en las mismas áreas en que lo hacen otros sistemas de comunicaciones, como por ejemplo las emisoras de radiodifusión o de televisión, móviles (de banda estrecha a una o dos frecuencias “punto a punto” o “punto a multipunto” y/o servicios rurales de banda ancha “punto a punto” o “punto a multipunto”), servicio fijo, radiolocalización o radioaficionados, para no dar lugar a interferencias y estar protegido frente a ellas.
Compartir el espectro con ciertos servicios que operan con potencias elevadas implica coordinación con los servicios que funcionan en las mismas bandas de frecuencias. En estos casos, los equipos de biotelemetría necesitan operar con licencia.

La implementación de un sistema de telemetría médica supone un análisis detallado de las opciones de que se dispone. En la tabla 2.2 se comparan las prestaciones de los sistemas que operan en las bandas de frecuencias tradicionales (distintas de las ISM), los que operan en las bandas ISM (Industrial Scientific Médical, Industrial, Científica y Médica) inferiores de 2.4 GHz y los que operan en las bandas de 2,4 GHz.

Características	Telemetria tradicional	ISM (< 2,4 GHZ)	ISM de 2,4 GHz

[9] “La situación de las tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("Wi-Fi")”. Grupo de Nuevas Actividades Profesionales. Colegio Oficial de Ingenieros de Telecomunicación. Octubre 2004.

Características	Telemetria tradicional	ISM (< 2,4 GHZ)	ISM de 2,4 GHz
Frecuencias	TV en VHF, TV en UHF, Redes móviles privadas	13,552–13,567 MHz, 26,957-27,283 MHz, 40,660-40,700 MHz, 402-405 MHz, 433,050-434,790 MHz	2.403–2.500 MHz
Protección	No; usuario secundario	Protección legal frente a transmisiones intencionadas no médicas. No Protegida de interferencia de canal adyacente ni de productos de la competencia.	Utilización de espectro disperso para reducir interferencias y aumentar la inmunidad RFI
Espectro disponible	Adecuado para aplicaciones rurales, saturado en zonas urbanas	Disponible hasta 14 MHz pero no todas las frecuencias están disponibles en todas la zonas	83,5 MHz compartidos con los usuarios de LANs
Utilización mundial	No	No	Si
Utilización del espectro	Dedicado. Fijo con canales de 25 KHz	Sin restricciones, en cuatro subcanales de 1,5 MHz	Requiere espectro disperso
Comunicación bidireccional	No	Permitida, pero no utilizada normalmente	
Soporta utilización no médica	No	No	Si
Basado en norma	No	No	Si IEEE 802,1X
Escalabilidad	Baja	Baja/Moderada	Alta
Incorporable en la infraestructura existente	No; necesita un sistema de antenas moderadas	No; necesita un sistema de antenas moderadas	Si con un diseño de la red adecuado
Costo de la infraestructura	Alto	Alto/Moderado	Bajo
Admite PDAs y voz	No	No, prohibido	Si
Herramientas de gestión	No	No	Si

Tabla 2.2 comparación las prestaciones de los sistemas que operan en las bandas de frecuencias tradicionales (distintas de las ISM)[10].

2.4 Comunicaciones entre equipos y servicios hospitalarios

2.4.1 Servicios para aplicaciones médicas.

Desde un punto de vista general, podemos distinguir tres grandes grupos de aplicaciones telemáticas multimedia para el cuidado de la salud:

[10] http://www.mdsr.ecri.org/summary/detail.aspx?doc_id=8117

- Sistemas para infraestructuras corporativas, que dan conectividad electrónica y soportes avanzados con fines generales y administrativos, aunque se utilicen también datos médicos
- Aplicaciones de servicios de información para profesionales y pacientes, acceso a bases de datos y de conocimiento, incluyendo servicios tipo http (Hipertex Transfer Protocol, Protocolo de Transmisión de Hipertexto) sobre TCP/IP (Transfer Control Protocol, Protocolo de Control y Transmisión).
- Aplicaciones orientadas a dar soporte de comunicación en las tareas médicas, clínicas y quirúrgicas.

Las tres definiciones anteriores son las que representan quizás más genuinamente la capacidad de las comunicaciones para mejorar el servicio a los pacientes y usuarios en general, en nuestro país aún nos encontramos atrás de los países desarrollados en donde ya se tienen muchas experiencias en el campo de las TIC's en hospitales.

Entre los servicios hospitalarios, hay que destacar que las aplicaciones inalámbricas de sistemas informáticos de gestión hospitalaria y enfermería han encontrado una buena acogida en los países del primer mundo. Esto es debido a que procesos tales como gestión de camas, dietas, inventarios, o medicación y farmacia, son más fáciles de definir y protocolizar en este tipo de aplicaciones inalámbricas, que los sistemas antecesores para toma de decisiones clínicas o los informativos correspondientes a un sistema tradicional de un hospital, y de registros electrónicos del historial clínico de un paciente para una asistencia médica mas inmediata. En países subdesarrollados como el nuestro, en donde procesos administrativos están demasiado atrasados tecnológicamente, la situación empeora ya que los sistemas son obsoletos y muy pocos eficientes.

Algunos de los objetivos de las aplicaciones que mencionamos antes son:

- Transmisión de videos o imágenes para el diagnostico y asistencia de un especialista que no esta cerca del lugar, resultando así una consulta remota rápida, en donde el especialista puede revisar mas detenidamente las imágenes o video después.
- Cuidados del paciente de forma directa, en donde el médico diagnostica y aconseja a un paciente desde una clínica remota, compartiendo audio, imágenes video, historiales clínicos, plan de medicación etc.
- Permitir que el médico disponga de datos de manera instantánea.
- Monitoreo de pacientes vía remota, en donde un dispositivo especial reúne información de alguno de los signos vitales de un paciente para que se interprete por un médico de forma inmediata, estos podrían ser: la presión sanguínea, glucosa, electrocardiograma o el peso.
- Supervisión y ayuda a internos que comienzan a hacer sus prácticas para tener a un especialista con más experiencia supervisándolo en diagnósticos o consejos interactivos para sus pacientes y así tener una segunda opinión médica.

2.4.2 Equipo médico.

La asistencia remota es un proceso sumamente delicado debido a que esta en juego la vida de las personas, por lo que tanto los sistemas encargados de las aplicaciones como el equipo deben ser muy especializados y altamente depurados para evitar errores o problemas en el diagnostico del médico y la compatibilidad electromagnética con el resto

del equipo médico por lo que deben cumplir diferentes normativas y recomendaciones internacionales.

Podemos definir a un equipo médico como cualquier aparato, instrumento, aplicación, material y otro articulo que se utilice, solo en combinación de otros, (incluidos software necesario para su funcionamiento) con la finalidad de diagnostico, prevención, monitorización, tratamiento de un paciente etc.

Para nuestros fines vamos a clasificar al equipo médico en tres grupos según la clasificación internacional ISM, los cuales se catalogan de la siguiente manera:

- Equipos ISM en los que es intencionadamente generada y/o usada energía electromagnética conducida; la cual es necesaria para el funcionamiento interno del propio equipo.
- Equipos ISM en los que la energía radioeléctrica es intencionadamente generados y/o usados en forma de energía electromagnética radiada para el tratamiento.
- Equipo electromédico, los cuales son equipos médicos con componentes eléctricos y/o electrónicos.

Entre otros, se encuentra el siguiente equipo médico destinado para:

- La aceleración de los análisis químicos utilizando 2450 MHz.
- El tratamiento local del cáncer por radiaciones de frecuencias inferiores a 400 MHz (hipertermia[11]).
- La fijación de tejidos.
- La formación de imágenes por resonancia magnética con frecuencias de 10 a 100 MHz en salas especialmente apantalladas.
- Equipos electromédicos. (Equipos con componentes tanto eléctricos con electrónicos).

Debido a que en la medicina hay muchas disciplinas, hay equipos médicos que realizan muchas funciones y están diseñados para cumplir dichas tareas. Algunas de estas funciones involucran, por ejemplo, la medición de niveles muy bajos de las señales de monitorización de un paciente, que pueden llegar a ser comparables a los niveles de ruido electromagnético. El fabricante debe revelar los niveles en los cuales el equipo satisface los requisitos de funcionamiento y especificar las características del entorno de uso electromagnético, en el cual el equipo funcionará según se ha previsto.

La tabla 2.3 muestra los posibles entornos electromagnéticos en los que se ven envueltos los equipos médicos.

Entorno	Localizaciones	Caracteristicas generales
Típico para el cuidado de la salud	Hospital, clínica, consulta	Parcialmente controlado, cubierto por estándares de norma.
Residencial	Consulta clínica pequeña	No controlado esta presente un responsable del cuido de la salud

[11] Elevación de la temperatura del cuerpo diferente a la fiebre.

Entorno	Localizaciones	Caracteristicas generales
Residencial	Hogar	No controlado esta presente un responsable del cuido de la salud
Transporte móvil	Vehículo, avión, helicóptero, ambulancia	No controlado amplias variaciones entornos severos de RF y campos electromagnéticos
Especial	Quirófano sala de urgencias	Análisis caso a caso

Tabla 2.3 Posibles entornos electromagnéticos en los que se ven envueltos los equipos médicos[12].

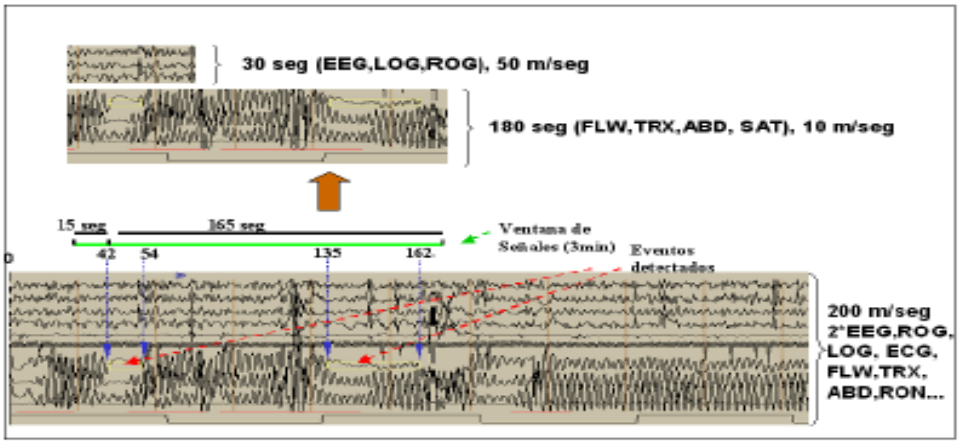
En cualquier aplicación médica es sumamente necesaria la precisión y fiabilidad del equipo, al tratarse de vidas humanas, por lo que es necesario trabajar a bajos niveles de potencia en estos entornos.

En la tabla 2.4 se presentan algunos de los parámetros y los tipos de señales que se pueden registrar en una aplicación de telemetría.

Señal Biològica	Rango de voltaje	Numero de sensores	Ancho de banda (Hertz)
ECG	0,5–4 mV	5-9	0,01–250
Sonido cardíaco	Muy bajo	2-4	5–2000
Ritmo cardíaco	0,5–4 mV	2	0,4–5
EEG	2–200 µV	20	0,5–70
EMG	0,1–5 mV	2+	0–10.000
Ritmo respiratorio	Pequeño	1	0,1–10
Temperatura corporal	0–100 mV	1+	0–1

Tabla 2.5 Parámetros presente en equipos médicos[13].

La figura 2.1 muestra algunas imágenes que se pueden ver en diferentes equipos médicos



[12] http://bvs.isciii.es/mono/pdf/UCIS_02.pdf
[13] http://www.mdsr.ecri.org/summary/detail.aspx?doc_id=8117

Figura 2.1 Imágenes Médicas[14].

Las EMI (interferencias electromagnéticas), pueden ser un problema considerable para cualquier dispositivo electrónico, pero en los dispositivos médicos, las consecuencias pueden ser fatales.

En el Reino Unido, La *Médical Device Agency* y en Canadá el *Health Canada's Médical Devices Bureau* han realizado registros de este tipo de incidentes. Los problemas con este origen registrados por la *Food and Drug Administration* (FDA) de los EEUU, desde 1979 incluyen fallos debidos a EMI conducidas y radiadas, alteraciones producidas por líneas de alta tensión y por descargas electrostáticas. Todos estos casos destacan la necesidad de incrementar las precauciones adoptadas por parte de usuarios, ingenieros, fabricantes, investigadores y organismos reguladores.

Así mismo, el *Health Canada's Médical Devices Bureau* recibió entre los años1984 y 2000, treinta y seis informes de fallos de funcionamiento de equipos médicos atribuidos a Interferencias Electromagnéticas.

En la tabla 2.6 se muestran algunas de las incidencias médicas registradas y su fuente de origen.

Dispositivo médico	Fuente de origen de la incidencia en el dispositivo médico
Monitores de apnea	Radiodifusión en FM
Monitores de gas de anestesia	Electrobisturíes
Electrocardiograma	Telefonía móvil celular analógica y digital
Bombas de infusión y de jeringa	Telefonía móvil celular analógica y digital y equipos de rayos-X portátiles
Sillas de ruedas electrónicas	Equipos de comunicaciones de policía, bomberos y radioaficionados
Análisis hematológicos	Buscapersonas
Indicación de temperatura y presión sanguínea	Electrobisturíes
Monitores de incubadoras	Radioaficionados, telefonía móvil celular
Marcapasos	Comunicaciones de ambulancias, walkytalkies,detector de metales
Monitor de telemetría cardíaco	Comunicaciones en 160 - 174 MHz
Respirador	Equipos de rayos-X portátiles, walky-talkies y radiodifusión en FM
Equipos de diálisis	Telefonía móvil celular
Desfibriladores	Telefonía móvil celular
Monitor de telemetría	Paging
Ayudas a la audición	Walky-talkies, telefonía móvil celular
Equipos de laparoscopia	Electrobisturíes

Tabla 2.6 Incidencias Médicas[15].

[14] http://bvs.isciii.es/mono/pdf/UCIS_02.pdf

[15] http://212.170.242.14/pesalud/Main?ISUM_ID=Groups&ISUM_SCR=serviceScr&ISUM_CIPH=NO4nynRwy0N-IpMEtu9egsdqfukqoiIKAtwb3IrFAo4_

2.5 Protección de la información.

Con respecto a la información de un paciente, su historial clínico tiene una gran importancia porque son instrumentos necesarios para garantizar una correcta asistencia médica por lo que están vinculados de una manera muy profunda al derecho de la vida y la protección de la salud. La acumulación de esta información y la correcta manipulación de ella son elementos necesarios para el seguimiento de la salud de las personas.

Así mismo, los datos médicos de un paciente son algo que afecta su ambiente personal e íntimo, por lo que probablemente una persona desee tener toda la información médica manejada con gran confidencialidad. Su conocimiento por terceros puede atentar gravemente a la intimidad personal y familiar, provocando en muchas situaciones el atropellamiento de sus derechos.

La gestión de la asistencia y de los servicios médicos tanto en atención primaria, como en atención especializada, en la urgencia o en la atención hospitalaria, exige necesariamente una acumulación masiva de información personal.

Como ya hemos mencionado antes, las tecnologías de la información y las comunicaciones son un instrumento muy útil y positivo para mejorar la calidad asistencial de los pacientes, pero proyectos como el que planteamos, requieren de una masiva concentración de información sobre pacientes, a las cuales, personal médico, con distintos niveles de privilegio, tendrán acceso por lo que esto podría convertirse en una potencial amenaza a la confidencialidad del paciente.

Capitulo 3.

3. Compatibilidad electromagnética.

3.1Introducción.

En relación a la compatibilidad de los equipos médicos con las aplicaciones inalámbricas tendremos que tomar en cuenta los siguientes aspectos:

- Evitar interferencias entre los diferentes sistemas de comunicación.
- Entre sistemas de comunicación inalámbrica y el equipo médico presente en el lugar.
- Entre sistemas de comunicación inalámbrica y las aplicaciones relacionadas a la gestión y administración de la información de pacientes.

Dentro de la definición de servicios en entornos hospitalarios abordamos la posibilidad de comunicación cableada e inalámbrica, pero haremos énfasis en las ventajas de la comunicación inalámbrica debido a:

- Monitorización (telemedicina) y medición de signos vitales (telemetría), lo que hará mas fácil la forma en que el personal médico acceda a este tipo de información.
- Disponer de una estructura de red más económica.
- Disponer de datos sin necesidad de presencia con el paciente.

Algunos de los actuales sistemas de comunicación utilizan las bandas de frecuencia ISM de 2403-2500 MHz y 5725-5875 MHz, que son bandas de comunicación bidireccional asignadas a dispositivos de comunicación de corto alcance, telemedicina, telemando, etc. Dentro de estas bandas de frecuencias, se encuentra la banda de 2400 – 2483,5 MHz asignada a las WLAN's para la conexión de computadoras y dispositivos periféricos para aplicaciones en interior de edificios y aplicaciones de baja potencia para transmisión de datos en recintos cerrados y exteriores de corto alcance.

El desarrollo de las TIC's se ha visto involucrada en el ambiente hospitalario, esto junto con el desarrollo de las redes móviles, sistemas de tercera generación UMTS (Universal Mobile Telecommunications System, Sistema de Telecomunicación Móvil Universal), protocolos de seguridad WAP y redes personales inalámbricas, las cuales facilitaran la movilidad del personal médico y el acceso a la información pertinente de pacientes en cualquier parte de un centro hospitalario y con sistemas e interfaces amigables.
En la figura 3.1 se puede observar las diferentes tecnologías que dan soporte a aplicaciones hospitalarias.

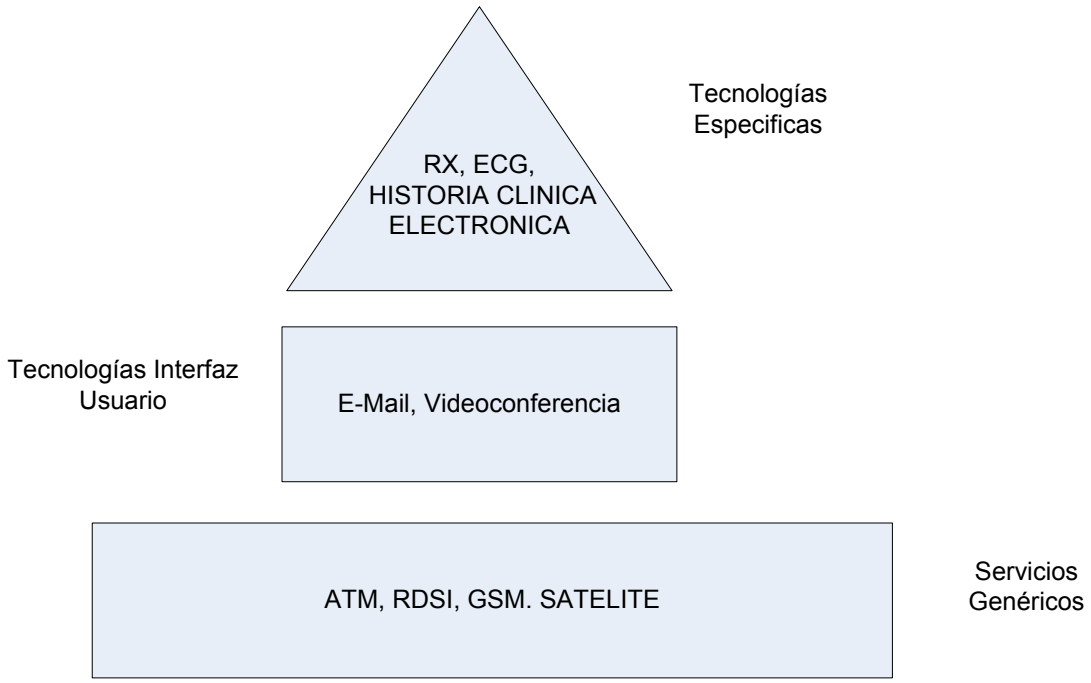


Figura 3.1 Soporte a aplicaciones hospitalarias[16].

3.2 Bandas de frecuencias de uso libre y regulado.

Un medio de vital importancia para el desarrollo del sector de las telecomunicaciones es el constituido por las radiocomunicaciones, a las que podremos definir como aquellas comunicaciones que precisan del uso de frecuencias radioeléctricas.
Con el fin de facilitar la cooperación internacional en materia de telecomunicaciones, fue creada la ITU (International Telecommunications Union, Unión Internacional de Telecomunicaciones), la cual reconoce en toda su plenitud, el derecho soberano de cada estado a reglamentar sus telecomunicaciones y teniendo en cuenta la importancia creciente de las radiocomunicaciones para salvaguarda de la paz, el desarrollo económico y social, por medio del buen funcionamiento de las radiocomunicaciones.
Con el objeto de normar las actividades, del sector Telecomunicaciones, especialmente mediante la regulación de la explotación del espectro radioeléctrico, fue elaborada la Ley de Telecomunicaciones, en la cual se establece que el "Espectro Radioeléctrico es propiedad del Estado". Así como la creación de la SIGET (Superintendencia General de Electricidad y Telecomunicaciones), en la cual se determina que la SIGET es la entidad competente para aplicar las normas contenidas en tratados internacionales sobre electricidad y telecomunicaciones vigentes en El Salvador[17].

Con el fin de lograr una eficiente utilización y coordinación del espectro radioeléctrico es preciso disponer de un marco reglamentario que recoja tanto la normativa internacional como nacional en materia de radiocomunicaciones, el cual se ha convenido en llamar CNAF (Cuadro Nacional de Atribución de Frecuencias).

[16] "Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios". Colegio oficial de Ingenieros en Telecomunicaciones Madrid España 2005.
[17] Texto extraído del documento "Cuadro nacional de atribución de frecuencias (CNAF) de la Republica de El Salvador".

Actualmente se conocen usos de las frecuencias en el país los cuales mencionaremos a continuación[18]:

- Libre (L): El espectro de uso libre lo constituye el conjunto de bandas de frecuencias que pueden ser utilizadas por el público en general para operar estaciones radioeléctricas que incluyan transmisores bajo determinadas condiciones establecidas por la SIGET en el CNAF, las bandas de uso libre pueden ser compartidas con bandas de uso Oficial y de uso Regulado, en estas circunstancias, las de uso libre deberán dar protección a las de uso oficial y regulado. Por lo que no se dará protección contra interferencias perjudiciales a las emisiones de uso Libre cuando las bandas de frecuencias sean compartidas.
- Oficial (O): El espectro de uso oficial se constituye por el conjunto de bandas de frecuencias destinadas para uso exclusivo de las instituciones gubernamentales, las bandas de frecuencias que deban ser reservadas para aplicaciones futuras, así como las que deban ser protegidas en virtud de Tratados, Acuerdos o Convenios internacionales. Las frecuencias oficiales serán consignadas como tales en el CNAF y a excepción de las asignadas a las diferentes instituciones gubernamentales se registrarán a nombre de la SIGET; su uso requerirá de autorización.
- Regulado (R): El espectro de uso Regulado se constituye por el conjunto de bandas de frecuencias que no han sido contempladas en esta Ley como de uso Libre o de uso Oficial; su uso requerirá de concesión.

En la realización de este documento se hablara mucho de la banda ISM que pertenece una banda de espectro de uso libre en el país.

3.3 Servicios de comunicaciones dentro de la banda ISM.

A continuación se enuncian algunos de los servicios que podrían ser utilizados dentro de la banda ISM y que podrían ser no susceptibles en entornos hospitalarios. Muchos de estos servicios existen en países europeos como en países del continente americano, y algunos de estos servicios están presentes en nuestro país.

- Dispositivos de baja frecuencia conocidos como de bucle inductivo.
- Dispositivos de corto alcance para aplicaciones de baja potencia no específicas.
- Banda ciudadana CB-27.
- Walkie-Talkies.
- Sistemas de radiocomunicaciones de telemando, teleseñalizacion y usos afines de baja potencia.
- Telemando y telemedicina.
- Telemando, telemedicina y telealarmas.
- Radio enlaces fijos y radio enlaces móviles de televisión.
- Redes de área local inalámbrica.
- Enlaces de video de corto alcance.
- RDFI (Dispositivos de Radiofrecuencia para aplicaciones de Identificación).
- Dispositivos genéricos de corto alcance.
- Dispositivos de baja potencia arriba de 10 GHz.

[18] Texto extraído del documento “Cuadro nacional de atribución de frecuencias (CNAF) de la Republica de El Salvador”.

3.4 Servicios de comunicaciones fuera de la banda ISM.

A continuación se enuncian algunos de los servicios que podrían ser utilizados fuera de la banda ISM, estos servicios serian susceptibles al ser usados en entornos hospitalarios, muchos de los cuales se encuentran operando en nuestro país.

- GSM y GPRS (General Radio Packet Service, Servicio General de Paquetes de Radio).
- UMTS.
- DECT.
- TETRA (Terrestrial Trunked Radio, Radio Truncado Terrestre).
- TRAC.
- Radiodifusión.
- Televisión.
- Militares y Estado.
- GPS (Global Position System, Sistema de Posición Global).

3.5 Equipo médico, bandas de frecuencias de trabajo y señales biomédicas.

Un dispositivo médico es cualquier aparato, instrumento, aplicación, material u otro artículo que se utilice, solo o en combinación de un Software, con la finalidad de:

- Diagnostico, prevención, monitorización, tratamiento o alivio de una enfermedad.
- Diagnostico, monitorización, tratamiento, alivio o compensación de cualquier daño o limitación.
- Investigación, sustitución o modificación de la anatomía o de un proceso fisiológico.
- Control de concepción.
- Todo lo que no consigue su finalidad dentro o sobre el cuerpo por medios farmacológicos, inmunológicos o metabólicos pero que puede ser parte de estos medios.

Los dispositivos, equipos o sistemas médicos lo podremos separar en tres grupos:

- El primer grupo son los dispositivos que usan energía de radiofrecuencia solo internamente.
- El segundo grupo lo conforman los dispositivos que usan energía de radiofrecuencia externamente.
- El tercer grupo son los dispositivos médicos que pueden estar o no asociados a dispositivos transmisores o receptores.

Ahora describiremos con detalle los equipos de uso médico y que trabajan en la banda de frecuencia ISM:

- Equipos ISM del grupo 1*:* equipos ISM en los que es intencionalmente generada y/o usada energía electromagnética conducida, la cual es necesaria para el funcionamiento interno del propio equipo.
- Equipos ISM del grupo 2*:* equipos ISM, en los que la energía radioeléctrica es intencionalmente generada y/o usada en forma de energía electromagnética radiada para el tratamiento.

- Equipos Electromédicos*:* equipos médicos con componentes eléctricos y electrónicos.

En relación al entorno del ambiente electromagnético en cuestión del cuidado de la salud puede verificarse la interacción de algunos entornos inalámbricos con algunas aplicaciones relacionadas al cuidado de la salud. Algunos parámetros y tipos de señales que se pueden registrar en una aplicación de telemetría referenciados a algunas aplicaciones inalámbricas.

3.6 Emisiones Radioeléctricas.

En 1974, la IRPA (Asociación Internacional para la Protección contra la Radiación) formó un grupo de trabajo para Radiaciones No-Ionizantes, con la finalidad de examinar los problemas suscitados en el campo de la protección contra varios tipos de RNI (Radiaciones No-Ionizantes). En el Congreso de la IRPA en París en 1977, este grupo de trabajo se convirtió en el INIRC (Comité Internacional para las Radiaciones No-Ionizantes).

En cooperación con la División de Salud Ambiental de la OMS (Organización Mundial de la Salud), la IRPA/INIRC desarrolló un número de documentos sobre criterios de salud en relación a las RNI, como parte del Programa de Criterios de Salud Ambiental de la OMS, auspiciado por el UNEP (Programa de Naciones Unidas para el Ambiente). En el VIII Congreso Internacional de la IRPA en Montreal en mayo de 1992, fue establecida una nueva organización científica independiente, la ICNIRP (Comisión Internacional para la Protección contra las Radiaciones No-Ionizantes) como sucesora de la IRPA/INIRC. Las funciones de la Comisión son investigar los posibles peligros asociados con las diferentes formas de RNI, desarrollar recomendaciones internacionales sobre límites de exposición para las RNI y tratar todos los aspectos sobre protección.

En abril de 1998, la ICNIRP publicó las Recomendaciones sobre límites de la exposición a campos variables en el tiempo hasta 300 GHz. Esta guía revisa y sustituye las anteriores de 1984, 1987, 1991 y 1993, y se incorporó a la Recomendación del Consejo Europeo 1999/519/CE.
La Tabla 3.1 muestra los limites básicos de exposición especificados en las recomendaciones de la ICNIRP-98.

Tipo de exposicion	Freecuencias	Densidad espectral de potencia (S) (W/m2)	SAR media en todo el cuerpo (W/Kg)	SAR localizada (cabeza y tronco) (W/Kg)	SAR localizada (extremidades) (W/Kg)
Ocupacional	10 MHz-10 GHz	--	0.4	10	20
Publico en general	10 MHz-10 GHz	--	0.08	2	4

Tabla 3.1 Limites básicos de la ICNIRP-98[19].

[19] "Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios". Colegio oficial de Ingenieros en Telecomunicaciones Madrid España 2005.

3.7 Análisis de interferencia y compatibilidad electromagnética.

La habilidad de los sistemas eléctricos y electrónicos para operar en un ambiente electromagnético sin efectos adversos, sin introducir perturbaciones intolerables en ese ambiente y soportar las producidas por otros equipos, se conoce como EMC (compatibilidad electromagnética). El estudio de la problemática de generación, propagación, influencia sobre otros circuitos y medidas de corrección de interferencias electromagnéticas se denomina EMI (Interferencia Electromagnética).

Además de la EMC en otros equipos, debe prestarse especial atención al tema de las EMI entre equipos de radiocomunicaciones, entendiendo ésta como la degradación de la recepción de la señal útil causada por una perturbación radioeléctrica. Desde el punto de vista de la compatibilidad electromagnética son dos los factores a tener en cuenta:

- El nivel de perturbación de las interferencias del generador.
- La susceptibilidad del receptor.

El término susceptibilidad y su opuesto inmunidad, se emplean para indicar la mayor o menor propensión de un dispositivo o equipo a ser afectado por interferencias radioeléctricas, es decir, el nivel de susceptibilidad de un equipo es la propiedad que tiene éste para funcionar correctamente en un ambiente electromagnéticamente complejo. Así pues, resulta prácticamente imposible hablar de susceptibilidad, inmunidad o medidas de protección en términos generales, sin referirse a equipos o dispositivos en concreto, ya que cada uno de ellos tendrá un comportamiento distinto al de otros tipos de interferencias electromagnéticas.

Los problemas debidos a las interferencias radioeléctricas pueden ocurrir entre sistemas independientes dentro de un amplio espectro de frecuencias (50 Hz a 30 GHz) tales como emisores de radio/TV, radares, aviones, barcos, líneas de distribución de energía eléctrica, equipos de radiodifusión, etc. Para solucionar estos problemas, el control en la asignación de frecuencias reduce la posibilidad de que estos sistemas interfieran. Otros métodos para reducir las interferencias son el reparto del tiempo de emisión, la localización geográfica y la orientación de las antenas de los mismos. La evaluación del riesgo de interferencias radioeléctricas en un centro hospitalario involucra una serie de consideraciones:

- La posibilidad de aumentar las prestaciones de las redes de comunicaciones internas de gestión.
- La posibilidad de instalar equipos radioeléctricos (estaciones base GSM, emisoras de radiodifusión) en el exterior del centro o sus proximidades.
- La posibilidad de extender las redes de comunicaciones de aplicaciones hospitalarias a un área mayor de la prevista inicialmente.

Las normas y recomendaciones sobre interferencias radioeléctricas suelen distinguir entre los distintos tipos de receptores afectados y distintas categorías o clases de efectos. Las clases de receptores son:

- Dispositivos, entendiendo como tales los elementos o componentes más simples que intervienen en un sistema.
- Equipos, que son conjuntos funcionales destinados a desempeñar alguna función concreta.

- Sistemas, o conjunto de equipos destinados a realizar tareas o procesos más complejos.

Y las clases de efectos son:

- Clase O: No se produce mal funcionamiento del equipo o dispositivo. La perturbación no influye.
- Clase A: La perturbación produce efectos aceptables, pero no altera el funcionamiento del equipo o dispositivo.
- Clase B: La perturbación altera temporalmente el funcionamiento del equipo o dispositivo, pero éste no sufre efectos irreversibles, pudiendo funcionar de nuevo sin intervención técnica.
- Clase C: La perturbación altera el funcionamiento del equipo o dispositivo, haciendo necesaria la intervención técnica para volver a funcionar.
- Clase D: La perturbación produce daños irreversibles en el equipo o dispositivo, quedando irrecuperable.

La creciente disponibilidad de equipos eléctricos/electrónicos en medicina, plantea problemas de seguridad nuevos, para los que la propia técnica ofrece soluciones. La comprensión de éstas es esencial en el diseño, fabricación, instalación, utilización y mantenimiento de la instrumentación médica.

3.8 Incidencias médicas.

Las interferencias electromagnéticas, EMI, pueden ser un problema considerable para cualquier dispositivo electrónico, pero en los dispositivos médicos, las consecuencias pueden ser fatales. En el Reino Unido, la Médical Device Agency y en Canadá el Health Canada's Médical Devices Bureau[20] han realizado registros de este tipo de incidentes. Los problemas con este origen registrados por la FDA (Food and Drug Administration, Administración de Drogas y Alimentos) de los EEUU, desde 1979 incluyen fallos debidos a EMI conducidas y radiadas, alteraciones producidas por líneas de alta tensión y por descargas electrostáticas. Todos estos casos destacan la necesidad de incrementar las precauciones adoptadas por parte de usuarios, ingenieros, fabricantes, investigadores y organismos reguladores. Así mismo, el Health Canada's Médical Devices Bureau recibió entre los años 1984 y 2000, treinta y seis informes de fallos de funcionamiento de productos sanitarios atribuidos a Interferencias Electromagnéticas[21]. Aunque el número de fallos registrados debidos a EMI es relativamente bajo en comparación con todos los fallos registrados, la gran difusión de estos informes y la gravedad de los problemas descritos, demuestra que las consideraciones sobre EMC en el diseño de equipos, la normativa, las verificaciones y las precauciones tomadas por los usuarios, son esenciales para la seguridad y la fiabilidad de los dispositivos médicos electrónicos.

La tabla 2.6 del capitulo 2 muestra algunas incidencias médicas registradas por equipos médicos y su origen.

[20] http://www.mohca.org/
[21] http://www.mohca.org/

3.9 Seguridad electromagnética para pacientes y para la aplicación.

El incremento de la utilización de las tecnologías inalámbricas en las aplicaciones hospitalarias, además de las inherentes ventajas que conlleva, requiere una adecuada planificación para tener en cuenta las interferencias radioeléctricas y electromagnéticas. Por tanto, se hace necesario garantizar la seguridad y la compatibilidad electromagnéticas en las aplicaciones de Telemedicina y servicios hospitalarios por medio de:

- Disminución del riesgo de interacciones adversas.
- Identificación y minimización de estas interacciones.

La definición de un procedimiento para la implementación de una aplicación de telemedicina supondrá una mejora en:

- Reducción de los errores médicos, mejora en la eficiencia y de la calidad de la atención al paciente.
- Aumentar el número de dispositivos médicos utilizados en la aplicación.
- Reducción de los errores de los dispositivos.
- Disminución del temor a lo desconocido.

Por último, en el despliegue de estas redes debe tenerse en cuenta el incremento del uso de redes de comunicaciones en las proximidades de los centros hospitalarios y/o los dispositivos médicos, es importante determinar las zonas con niveles altos de exposición, así como la contribución relativa de antenas auxiliares que se puedan instalar en las proximidades (incluso sin licencia o no instaladas permanentemente).

3.10 Medidas tomadas en diferentes países.

El registro de los problemas originados por interacción entre equipos de comunicaciones y dispositivos médicos y la preocupación por garantizar la operación segura en centros hospitalarios, es una cuestión considerada en distintos países desde hace tiempo. Las primeras fuente de emisiones radioeléctricas eran las instalaciones de radiodifusión y desde los años 90, cuando empezó el despliegue a gran escala de la telefonía móvil celular, las estaciones base pasaron a ser la primera preocupación social y también de los profesionales en la área de la salud.

En los últimos tiempos, con el despliegue generalizado de redes inalámbricas en muchos centros hospitalarios, empieza a ser tema de interés para los responsables de servicios informáticos y departamentos de bioingeniería en los citados centros.

Sin embargo, estas instalaciones inalámbricas sólo se han empezando a desplegar intensivamente en los últimos años. No es el caso de las redes de telefonía móvil celular, con respecto a las cuales ya se han tomado medidas de precaución o restrictivas de uso en varios países como se presenta a continuación.

En el Reino Unido, en cada hospital se decide individualmente. El problema se considera de baja prioridad, en comparación con otras causas de fallos, tales como el uso inapropiado del equipo médico o los errores de los operadores. Por ejemplo, en el Hospital de St. James en Leeds, el uso de teléfonos móviles está prohibido en todo el

centro, excepto para propósitos clínicos esenciales en cuyo caso se recomienda que no se utilice a distancias inferiores a 2 m de los dispositivos médicos.

En la tabla 3.2 se muestran algunas medidas tomadas en diferentes países:

País	Medida
Australia	Separación de 2 metros
Francia	Prohibición total
Alemania	Recomendación de prohibición total
Holanda	Prohibición de algunas zonas y separación de 1.5 metros en el resto
EEUU	Prohibición de algunas zonas
Reino Unido	Recomendación de prohibición de algunas zonas Necesidad de regulación y responsabilidad legal en relación con la instalación de microceldas y picoceldas

Tabla 3.2 Medidas tomadas en diferentes países[22].

3.11 Prevención de riesgos.

La prevención de degradación de prestaciones en los dispositivos o productos hospitalarios requiere el esfuerzo tanto de fabricantes como de usuarios, así como de los organismos de normalización.

Los fabricantes deben asegurar el mantenimiento de las especificaciones de los dispositivos en el entorno de uso. El empleo de técnicas de atenuación adecuadas durante el diseño, junto con la verificación del cumplimiento de la normativa existente sobre interferencias electromagnéticas, ayuda a prevenir los problemas. Los fabricantes también deben proporcionar a los usuarios una guía clara de funcionamiento y de reconocimiento y prevención de estos problemas.

El problema de las posibles interferencias producidas por EMC deben tener en consideración en la etapa de construcción e instalación de instrumentación así como durante a selección de nuevos equipos eléctricos y electrónicos, teniendo en cuenta las siguientes consideraciones:

- Identificación de posibles riesgos en el escenario de la aplicación.
- Control de los riesgos.

Los riesgos relacionados con el uso de dispositivos médicos en ciertos entornos electromagnéticos deben considerarse detalladamente en un proceso de análisis de riesgos. La finalidad es minimizar el riesgo asociado al uso en las proximidades de emisores radioeléctricos, asegurar que el usuario utiliza el dispositivo de forma segura y

[22] "Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios". Colegio oficial de Ingenieros en Telecomunicaciones Madrid España 2005.

eficiente, así como también facilitar la introducción de nuevos dispositivos. El control del riesgo debe ayudar a la identificación, comprensión, control y prevención de fallos que puedan derivar en riesgos y debe ser una aplicación sistemática de políticas, procedimientos y prácticas de análisis, evaluación y control. Este análisis comprenderá la identificación y descripción de riesgos y cómo se pueden presentar, sus consecuencias esperadas y la estimación de su probabilidad relativa así como la severidad del daño y sus consecuencias. Las incidencias producidas por sistemas radioeléctricos en dispositivos médicos se presentan con baja probabilidad pero las consecuencias suelen ser graves y con gran difusión, lo que hace recomendable la redacción de procedimientos de instalación y utilización segura en los entornos sanitarios. Las situaciones peligrosas e infrecuentes son a menudo difíciles de identificar siendo a veces necesario obtener la información de los usuarios o de las pruebas a las que se someten en condiciones reales o simuladas.

En el análisis de riesgos debería de estudiarse el uso de dispositivos, con consideraciones tales como:

- Usuarios del dispositivo: paciente, miembro de la familia, médico, enfermera, cuidador, etc.
- Utilización típica y atípica del dispositivo.
- Características del dispositivo.
- Características del entorno en el que se van a utilizar dispositivos médicos (hospital, consulta, quirófano) y entornos en los que es previsible que los dispositivos se vean afectados.
- Interacción entre usuarios, dispositivos y entorno de uso.

Sobre el estudio de la utilización del dispositivo, es preciso identificar e investigar usos y/o entornos de dispositivos que presenten alguna probabilidad de riesgo, así como investigar sobre riesgos conocidos o sospechados que se pueden traducir en diagnósticos erróneos (producidos por fallos en la identificación del paciente, de la enfermedad o en la exactitud del parámetro fisiológico evaluado), interpretación errónea de la información procedente de los dispositivos de monitorización, o en tratamientos incorrectos (terapias no efectivas o dañinas). Los usuarios también deben recibir indicaciones sobre identificación y eliminación de problemas de compatibilidad electromagnética, y deben dar a conocer la existencia de estos incidentes cuando tengan lugar, para alertar a la comunidad médica y poder tomar medidas adecuadas para evitar su repetición.

La prohibición de la utilización de terminales móviles en las proximidades de dispositivos médicos puede ser adecuada en una fase inicial de la aplicación, pero las tecnologías inalámbricas no deben estar excluidas de ésta permitiendo una mayor calidad de la atención al paciente. Con un planteamiento adecuado, será posible identificar, controlar y advertir sobre problemas significativos de interferencias electromagnéticas antes de que ocurran, teniendo en cuenta que el riesgo de EMI depende de varios factores que incluyen la susceptibilidad de los productos sanitarios, la frecuencia en la que funcionan los transmisores, así como su potencia emitida, su tipo de modulación y la proximidad al dispositivo médico.

Capitulo 4.

4. Tecnologías Inalámbricas

4.1 Introducción

La necesidad de comunicación actual a obligado a buscar formas de acceso a la información, cada vez mas accesibles y rápidas, en tal caso se han desarrollado las redes de datos inalámbricas, que como su nombre lo dice ofrecen acceso información por medio de un medio sin alambres, este medio es el aire, estas tecnologías ofrecen acceso a la información sin necesidad de encontrarse en un lugar fijo o inclusive encontrándose en movimiento, esta es la gran virtud de estas tecnologías.

El desarrollo de las tecnologías de modulación y compresión que han impulsado en los últimos años plataformas como la tecnología celular, han favorecido en gran medida a la técnica de transmisión de las redes de datos.

En este campo existen diferentes estándares de redes inalámbricas diseñadas para aplicaciones especificas y que se encuentran desarrolladas de una manera que permita optimizar los criterios de ancho de banda, cobertura, y movilidad de acuerdo a la aplicación, en tal sentido se pueden mencionar tecnologías como Bluetooth, que esta optimizada a ofrecer una taza media de datos con poco consumo de potencia de los equipos y utilizada para redes de pequeño alcance.

Estas nuevas tecnologías están creando nuevas aplicaciones que por tener las características de movilidad, dan un grado de flexibilidad al usuario en el acceso a la información incrementando así la productividad y diversificando sus campos de acción.

4.2 Evolución de las tecnologías inalámbricas

El origen de las WLAN se remonta a los resultados obtenidos de una investigación realizada en 1979 por ingenieros de IBM de Suiza, dicha investigación se basaba en un experimento en el cual trasmitían datos mediante rayos infrarrojos dentro de una fábrica para crear una red local. Estos resultados publicados por el IEEE, se pueden considerar como el punto de partida de la tecnología inalámbrica en redes de área local.

En febrero de 1980 se formó en el IEEE un comité de redes locales con la intención de estandarizar un sistema de 1 o 2 Mbps, que básicamente era Ethernet .El numero 802 es el numero correlativo que le toco al comité.

El primer estándar de las tecnologías de acceso inalámbrico de datos, denominadas Wi-Fi (Wireless Fidelity, Fidelidad Inalámbrica) nace en 1997 cuando la IEEE creo el estándar 802.11 el cual hacia uso de la frecuencia de 2.4Ghz y era capaz de manejar anchos de banda de 1 y hasta 2 Mbps, este protocolo mostró, lo que era capaz de realizarse con tecnologías inalámbricas, a pesar de no haber tenido el éxito que se esperaba, en parte por que el sistema era poco experimentado y los problemas de cobertura dados por los tipos de modulación utilizados.

Estos inconvenientes trataron de solventarse y es así como en 1999 surge el estándar 802.11b el cual buscaba mejorar los problemas obtenidos con la norma inicial, esta vez se

ofrecían anchos de banda mas elevados en el orden de los 5 Mbps a 11 Mbps y trabajaba sobre la frecuencia de 2.4 GHz, paralelo a este esfuerzo se presento un estándar que trabajaba en la frecuencia de 5 GHz y ofrecía velocidades de 54 Mbps.

Los problemas de compatibilidad entre ambas normas impidió que los equipos para la norma A se desarrollaran y por ello se hizo necesario crear un estándar compatible con norma B y es así como surge el estándar 802.11g, esto mejoro las prestaciones de los equipos, al mostrar la compatibilidad con ambos estándares a tal grado que los dispositivos de mayor presencia en la actualidad utilizan compatibilidad con la norma B y G.

La constante necesidad de mayor ancho de banda producida por las nuevas aplicaciones que pueden montarse sobre una red de datos obligo a crear nuevos estándares, por lo que IEEE ya trabaja en un nuevo estándar denominado 802.11n el cual pretende alcanzar velocidades de 600 Mbps, y con los nuevos protocolos para mejorar el desempeño de las aplicaciones sensibles al retardo, este panorama se muestra mas atractivo para la implementación de servicios basados en recursos multimedia, utilizando la interfase aire.

Actualmente la norma N esta aun en discusión sin embargo ya existe un adelanto de esa norma y equipos que logran manejar velocidades de 300Mbps con este plus de la norma. La norma N pretende utilizar las frecuencias de 2.4 GHz y 5 GHz simultáneamente, aparte de mostrar compatibilidad total con los equipos de norma B y G.

4.3 Normalización IEEE.

IEEE 802 es un comité y grupo de estudio de estándares perteneciente al IEEE, que actúa sobre Redes de Datos, concretamente y según su propia definición sobre redes LAN y redes MAN (redes de área metropolitana).

El grupo de trabajo enfoco esfuerzos en la creación de estándares para redes personales (de algunos metros de rango) y en redes más amplias como las metropolitanas.

Algunos de los estándares creados por este grupo de trabajo son los mostrados por la tabla 4.1.

Estándar	Aplicación
IEEE 802.1	Protocolos superiores de redes de área local
IEEE 802.2	Control de enlace lógico
IEEE 802.3	Ethernet
IEEE 802.4	Token Bus (abandonado)
IEEE 802.5	Token Ring
IEEE 802.6	Red de área metropolitana (abandonado)
IEEE 802.7	Grupo de Asesoría Técnica sobre banda ancha (abandonado)
IEEE 802.8	Grupo de Asesoría Técnica sobre fibra óptica (abandonado)
IEEE 802.9	RAL de servicios integrados (abandonado)
IEEE 802.10	Seguridad interoperable en RAL(abandonado)
IEEE 802.11	Red local inalámbrica, también conocido como Wi-Fi
IEEE 802.12	Prioridad de demanda
IEEE 802.13	(no usado) (véase trece, la superstición llega a cualquier

Estándar	Aplicación
	sitio)
IEEE 802.14	Cable módems, es decir módems para televisión por cable. (abandonado)
IEEE 802.15	Red de área personal inalámbrica, que viene a ser Bluetooth
IEEE 802.16	Acceso inalámbrico de Banda Ancha, también llamada WiMAX, para acceso inalámbrico desde casa.
IEEE 802.17	Anillos de paquetes con recuperación, se supone que esto es aplicable a cualquier tamaño de red, y está bastante orientado a anillos de fibra óptica.
IEEE 802.18	Grupo de Asesoría Técnica sobre Normativas de Radio
IEEE 802.19	Grupo de Asesoría Técnica sobre Coexistencia.
IEEE 802.20	Acceso inalámbrico de Banda ancha móvil, que viene a ser como el 16 pero en movimiento.
IEEE 802.21	Interoperabilidad independiente del medio
IEEE 802.22	Red inalámbrica de área regional.

Tabla 4.1 Normalización de estándares IEEE[23].

Entre estos estándares resaltan los inalámbricos 802.11, 802.15 y el 802.15 que son Wi-Fi, Bluetooth y WiMax (Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para el Acceso por Microondas) respectivamente.

Estos son los principales estándares para redes de acceso inalámbricos utilizados en la actualidad y en el caso de WiMax el que se cree será el futuro de estas tecnologías a mediano plazo, y que se convertirá en el acceso inalámbrico metropolitano.

4.3.1 802.11 legacy

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 Mbps que se transmiten por señales IR (señales infrarrojas) en la banda ISM a 2.4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

4.3.2 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de

[23] http://es.wikipedia.org/wiki/IEEE_802

2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP (User Datagram Protocol, Protocolo Datagrama de Usuario).

4.3.3 802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbps, o cerca de 24.7 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. .

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

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

4.3.4 802.11a

En 1997 el IEEE crea el Estándar 802.11 con velocidades de transmisión de 2 Mbps. En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b. En 2001 hizo su aparición en el mercado los productos del estándar 802.11a. La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 sub-portadoras OFDM (Orthogonal Frequency Division Multiplexing, División de Multiplexacion de Frecuencia Ortogonal) con una velocidad máxima de 54 Mbps, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbps. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbps en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No existe interoperabilidad con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas como lo muestra la tabla 4.2:

Transmisión	Valor máximo de Ancho de banda	Valor mínimo de Ancho de Banda
Externa	30 Mts / 54 Mbps	300 Mts / 6 Mbps
Interna	12 Mts / 54 Mbps	90 Mts / 6 Mbps

Tabla 4.2 Valores de anchos de banda[24].

4.3.5 802.11d

Resuelve aspectos reglamentarios de países que no disponen aun de normativa en vigor para la operación de LAN's 802.11. La ampliación 802.11d garantiza la interoperabilidad de WLAN's en tales países.

4.3.6 802.11e

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

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

4.3.7 802.11f

Es el IAPP (Inter Access Point Protocol). Mejora el mecanismo de traspaso en 802.11 entre puntos de acceso y segmentos de conmutación mientras los usuarios se desplazan de unos a otros.

4.3.8 802.11h

Añade un mejor control de la potencia de transmisión y de la selección de canal de radio a 802.11a. Esta norma surge principalmente como respuesta a los requisitos de los organismos reguladores europeos.

4.3.9 802.11i

Proporciona seguridad mejorada, incluye el uso de protocolo de autenticación 802.1X, un sistema mejorado de distribución de clave y un cifrado mas sólido mediante el estándar AES (Advanced Encription Standard, Estándar Avanzado de Cifrado).

4.3.10 802.11j

Resuelve la adición del canal de 49 GHz al de 5 GHz para 802.11a en Japón.

4.3.11 802.11n

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. la velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea

[24] http://es.wikipedia.org/wiki/IEEE_802.11#802.11a

mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto. No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo esté implantado).

4.4 Tecnologías.

La evolución en las técnicas de transmisión han dado pie a la creación de las redes inalámbricas, en tal sentido se han desarrollado diversas tecnologías que aun en la actualidad siguen en desarrollo y su evolución dicta las nuevas formas de comunicación.

En la creación de los estándares de las redes inalámbricas se manejan varias tecnologías utilizadas en la transmisión de datos en la interface aérea, entre estas tecnologías tenemos:

- Infrarrojo
- Banda Angosta
- Espectro Extendido.
- Bluetooth.
- Wi-Fi.

4.4.1 Infrarrojo (IrDA)

Los inicios de esta tecnología datan de 1979 cuando un grupo de especialistas de IBM en Suiza publican en la IEEE los resultados de sus experimentos, en los cuales se transmitían datos utilizando señales infrarrojas.

En 1993 se crea un grupo de desarrollo denominado IrDA (Infrared Data Association, Asociación de Datos Infrarrojos), este grupo esta formado por HP, IBM y Sharp entre otros 153 miembros en la industria de la fabricación de hardware, su principal objetivo es estandarizar la transmisión de datos por medio de rayos infrarrojos.

Los estándares de IrDA definen comunicaciones bidireccionales punto a punto empleando un haz de luz infrarroja que requiere línea de vista, un ángulo no mayor de 30 grados y una distancia que no excede un metro para obtener tasas de transmisión de datos entre 9.6Kbps y 16Mbps dependiendo de las características del entorno. La banda de frecuencia va desde 300 GHz hasta los 200 THz, justo debajo del espectro de la luz visible.

No obstante, es oportuno aclarar que estos estándares están divididos en dos segmentos diferentes para satisfacer las necesidades del mercado:

- IrDA-Data: Empleado básicamente para transferencias bidireccionales de información en forma inalámbrica y con altas tasas de transmisión entre dispositivos portátiles.

- IrDA-Control: Fue establecido para cursar comunicaciones de control entre dispositivos periféricos como teclados, ratones, joysticks o controles remotos. La distancia máxima se amplia hasta garantizar un mínimo de 5 metros con tasas de transmisión alrededor de 75 Kbps.

El IrDA reside en las capas bajas del modelo OSI, por lo que solo se regula capa física o envió de datos en la interfase aire haciendo uso de técnicas de modulación sobre los rayos infrarrojos.
Las velocidades de transmisión son relativamente bajas y su máximo inconveniente reside en el alcance y en la necesidad de tener línea vista, por que lo que esta técnica es utilizada solo para dispositivos nómadas[25], ya que intrínsicamente esta técnica, es poco utilizada en equipos en donde la movilidad es critica.
El nicho de mercado para esta tecnología son los controles remotos, teclados inalámbricos, teléfonos celulares, PDA´s etc.

4.4.2 Banda Angosta (NARROW BAND)

Los sistemas de Banda angosta para la transmisión de datos son el resultado de la evolución en las técnicas de radiodifusión que evolucionaron desde en invento de la radio por Marconi en 1896, y con la adición de nuevas técnicas de modulación y codificación, es posible contar con sistemas de banda angosta.

Un sistema de radio de banda angosta transmite y recibe información en una radiofrecuencia específica. La banda amplia mantiene la frecuencia de la señal de radio tan angostamente posible para pasar la información. El cruzamiento no deseado entre canales es evitado al coordinar cuidadosamente diferentes usuarios en diferente canal de frecuencia. En un sistema de radio la privacidad y la no-interferencia se incrementan por el uso de frecuencias separadas de radio. El radio receptor filtra todas aquellas frecuencias que no son de su competencia. La desventaja de esta tecnología es el uso amplio de frecuencias, uno para cada usuario, lo cual es impráctico si se tienen muchos.

Estos sistemas de Banda angosta son denominados comúnmente como de micro ondas por la gama de frecuencias utilizada. Esta técnica es utilizada en las redes de datos para unir redes LAN distantes creando así lo que se denomina backhaul´s[26].
Estos sistemas son sofisticados y costosos, con la limitante que es necesario la autorización y compra de licencias para la transmisión ya que hace uso de frecuencias licenciadas[27] en la mayoría de los casos.

Por sus características estos sistemas son utilizados solo en dispositivos fijos ya que la técnica de modulación y la estrechez de las ondas utilizadas exigen que los equipos se encuentren alineados para llevar a cabo la comunicación.

[25] Nómadas: entiéndase por dispositivos que cambian de ubicación pero no están en movimiento constante.
[26] Backhaul, es el término con el que se denomina la red de radioenlaces que une otras redes LAN distantes, esta red generalmente es de mayor ancho de banda que las redes a unir y es el corazón de las redes de datos, inalámbricas.
[27] Grupo de Licencias de uso restringido según el cuadro de asignación de frecuencias de la ITU. Es necesario la extensión y compra de permisos para hacer uso de ellas, y están regidas según la legislación del país.

4.4.3 Banda Ancha (SPREAD SPECTRUM)

Esta técnica de comunicación fue desarrollada por organismos militares, ya que su principal misión es esparcir los datos en un espectro amplio para evitar así las interferencias, y los robos de información. Este sistema fue ideado en plena segunda guerra mundial, como un mecanismo para controlar misiles guiados por radiodifusión, se utilizo una técnica en la que no se ocupaba una sola frecuencia en el control, sino que esta frecuencia cambiaba constantemente para que no pudiera ser interferida. La patente del sistema fue adjudicada el 11 de agosto de 1942 a Hedy Kiesler Markey una actriz cuyo esposo era pianista y allegado a Hitler, y se baso en los cambio de tonalidad del piano para crear su idea. Los primeros prototipos de transmisores que utilizaban esta técnica fueron desarrollados en 1957 por la compañía Estadounidense Silvania Electronics Systems Division, y su uso fue exclusivamente militar por los altos costos que representaba. Hasta principios de los años 90 donde los bajos costos de fabricación de hardware así, como los avances en la miniaturización de los dispositivos y los logros en materia de procesamiento digital de señales hizo posible su implementación en forma comercial. Para lo cual la IEEE estandarizo esta técnica y la incluyo en sus estándares IEEE 802.11 mas comúnmente conocidos con el término de Wi-Fi.

Esta técnica esparce la señales radiales en un espectro amplio inclusive mucho mayor que el máximo ancho de banda requerido para transmitir la señal, esta técnica definitivamente no parece hacer uso eficiente del espectro, sin embargo su bondad radica en que puede coexistir con sistemas de banda estrecha ya que para ellos solo se comporta como una pequeña inserción de ruido, en lo que se refiere al receptor de espectro ensanchado, él no ve las señales de banda estrecha, ya que está escuchando un ancho de banda mucho más amplio gracias a una secuencia de código preestablecido. Por estas características este sistema se muestra apto para sistemas de acceso punto multipunto en los que múltiples usuarios pueden acceder a un único receptor sin presentar interferencias entre si y manteniendo las comunicaciones codificadas hacia los otros usuarios, mediante un código de transmisión preestablecido.

Existen al menos 5 técnicas distintas que hacen uso del Espectro ensanchado.

4.4.3.1 Sistema de secuencia directa. (DSSS /Direct Sequence Spread Spectrum).

Esta técnica se realiza modulando la señal de datos mediante una función pseudo-aleatoria, que convierte la señal radiada en una especie de ruido, el cual es transmitido, y el tamaño del espectro utilizado esta relacionado directamente con la tasa de bits transmitidos.
Para la recuperación de la señal el receptor crea una señal igual a la utilizada en la transmisión y por medio de técnicas de detección similar a la utilizada en la recepción de radios convencionales, se extrae la señal enviada.

Esta técnica hace uso de mayor potencia de transmisión que otras técnicas de SS[28] por otra parte, es posible alcanzar velocidades de 8 Mbps en la transmisión mediante esta técnica.

[28] SS Spread Spectrum, Espectro Ensanchado.

4.4.3.2 Sistema de Salto de Frecuencia (FHSS /Frequency Hopping Spread Spectrum).

Esta técnica de SS consiste en cambiar de forma pseudos-aleatoria la frecuencia de transmisión, saltando de frecuencia en frecuencia en un ancho de banda determinado, en función del tiempo, El receptor así busca la señal transmitida en la misma secuencia en la que fue enviada, y esta es modulada nuevamente, como una señal convencional.

El sistema necesita que ambos equipos, transmisor como receptor sean FHSS y que a la ves conozcan el código seudo aleatorio.

En la figura 4.1 se muestra el diagrama de un transmisor de FHSS

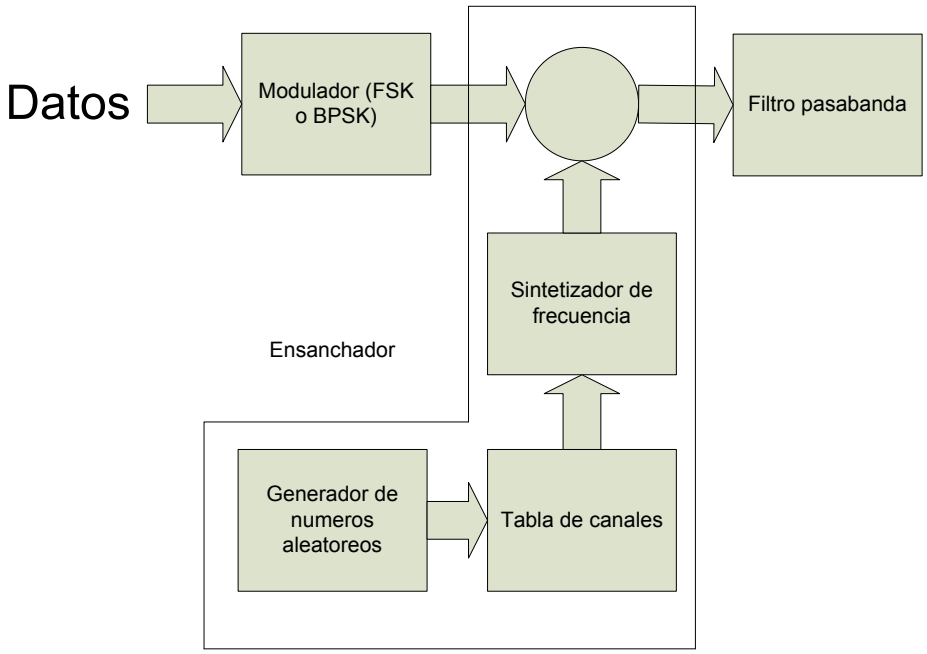


Figura 4.1 Transmisor de FHSS[29].

Se tienen dos partes fundamentales, una constituida por un modulador convencional que hace uso de técnicas de modulación digital convencionales como FSK y otra es una sección que se encarga de ensanchar la señal a transmitir.

Primero se genera una secuencia digital pseudos-aleatoria, luego esta señal es convertida a una señal analógica que controla un PLL que genera la señal analógica que se utilizara para el envió, esta señal es utilizada como portadora temporal y mezclada con los datos modulados , luego esta señal es pasada por un filtro pasa banda que solo deja pasar la señal de banda angosta resultante del proceso, cuando un segundo bloque de información es transmitido el generador seudo aleatorio genera un valor nuevo de frecuencia por lo que la transmisión de estos fragmentos nunca se realiza en la misma frecuencia en forma consecutiva.

[29] http://www3.fi.mdp.edu.ar/electronica/articulos/EspectroEsparcidoFHSS.doc

Por otra parte el receptor debe poseer un diagrama en bloques como el mostrado en la figura 4.2

De igual forma en el receptor se obtiene la señal de FHSS esta es modulada nuevamente haciendo uso de una frecuencia que se genera de forma pseudos-aleatoria y en secuencia con la señal que la genero, esta secuencia genera una señal analógica que maneja un PLL y que es utilizada para modular nuevamente la señal de FHSS luego esta es modulada de el FSK que la transporto y se obtienen los datos que se enviaron.

Para recibir el siguiente fragmento de datos se vuelve a generar la secuencia seudo aleatoria y se repite el proceso.

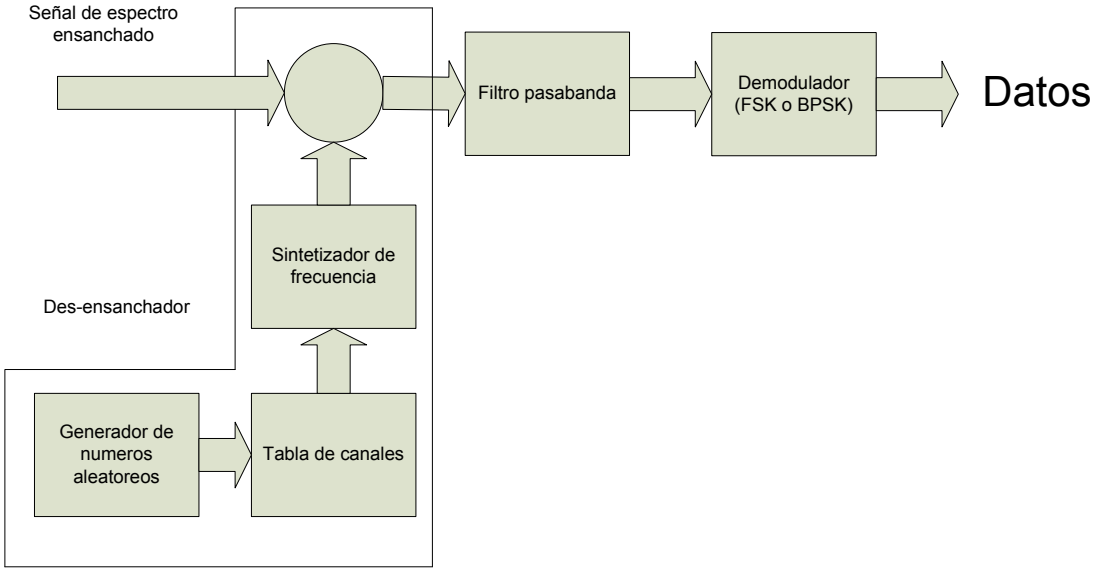


Figura 4.2 Receptor FHSS[30].

Esta comparada con la de DSSS utiliza menos energía para la transmisión y puede alcanzar anchos de banda teóricos de hasta 2 Mbps. Esta técnica es muy utilizada en estándares de redes de acceso mediano y ampliamente difundida en el estándar de Bluetooth

4.4.3.3 Sistemas de salto temporal (FFHSS/ Fast Frecuancy Doping Spread Spectrum).

Esta técnica es parecida al FHSS con la diferencia que la frecuencia utilizada para la transmisión varia de forma aleatoria al igual que el periodo que se le utiliza. Esta combinación hace más robusto el sistema en el sentido de la seguridad y añade un grado de complejidad para su intervención. Esta técnica de SS es ampliamente utilizada en la tecnología celular en y es una variación de TDMA (Time division Multipexer Access, Acceso Múltiple por División de Tiempo)

[30] http://www3.fi.mdp.edu.ar/electronica/articulos/EspectroEsparcidoFHSS.doc

4.4.3.4 Sistemas de frecuencia modulada pulsada (o *Chirping*).

Se trata de una técnica de modulación en espectro ensanchado menos común que las anteriores, en la que se emplea un pulso que barre todas las frecuencias, llamado chirp, para expandir la señal espectral. Esta técnica utiliza todas las portadoras disponibles en el espectro asignado y lo hace de manera ordenada, algunas variaciones de esta técnica, se logran al utilizar cada portadora un periodo de tiempo pseudos-aleatorio.

4.4.3.5 Sistemas Híbridos.

Existen sistemas híbridos que hacen uso de SS donde los principales componentes son FHSS y el DSSS, estos sistemas tratan de tomar los mejor de cada una de las técnicas para hacer un uso mas eficiente del ancho de banda, potencia, y aumentar la cantidad de información a transmitir.

4.4.4 Bluetooth

El nombre procede del rey danés y noruego Harald Blåtand cuya traducción al inglés sería *Harold Bluetooth* (Diente Azul, aunque en lengua danesa significa 'de tez oscura') conocido por unificar las tribus noruegas, suecas y danesas.
De la misma manera, Bluetooth intenta unir diferentes tecnologías como las de las computadoras, los teléfonos móviles y el resto de dispositivos periféricos. El símbolo de Bluetooth es la unión de las runas nórdicas H y B.
Es la norma que define un estándar global de comunicación inalámbrica que posibilitada la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

La tecnología *Bluetooth* comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Motorola, Toshiba, IBM e Intel, entre otros. Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente lo hagan también empresas de sectores tan variados como automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etc., con lo que en poco tiempo se nos presentará un panorama de total conectividad de nuestros aparatos tanto en casa como en el trabajo.

4.4.4.1 Antecedentes

En 1994, Ericsson inició un estudio para investigar la viabilidad de una nueva interfaz de bajo costo y consumo para la interconexión vía radio (eliminando así cables) entre dispositivos como teléfonos móviles y otros accesorios. El estudio partía de un largo proyecto que investigaba unos multicomunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado *MC link*. Conforme este

proyecto avanzaba se fue haciendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud que se basaba en un chip de radio.

4.4.4.2 El SIG de Bluetooth

El SIG (*Special Interest Group*) de Bluetooth es un grupo de compañías que trabajan juntas para desarrollar, promover, definir y publicar las especificaciones de esta tecnología inalámbrica a corta distancia para la conexión entre dispositivos móviles, así como gestionar los programas de calidad para que los usuarios disfruten de más prestaciones.
Este grupo se fundó en febrero de 1999 por estos promotores:

- Ericsson Mobile Communications AB.
- Intel Corporation.
- IBM Corporation.
- Toshiba Corporation.
- Nokia Mobile Phones.

En mayo del mismo año, se invitó a otras compañías para participar en el grupo, publicando la versión 1.0 de las especificaciones Bluetooth en julio de 1999. En diciembre, el núcleo inicial de promotores admitió a otras cuatro grandes compañías:

- Microsoft.
- Lucent.
- 3COM.
- Motorola.

Al ser partícipes del SIG, las compañías pueden dotar de Bluetooth a sus productos con la garantía que ofrece el pertenecer al grupo y conocer las especificaciones técnicas de la tecnología, además de poder utilizar libremente la banda radio de Bluetooth (2.4 GHz) mientras que las compañías externas no pueden aplicar la tecnología al no tener su patente.

El SIG creció hasta llegar a más de 1800 miembros en abril de 2000. En octubre de 2006, Nokia anunció el lanzamiento de Wibree como sustituto de Bluetooth, dedicándose al mismo segmento de dispositivos y aplicaciones pero con un menor consumo de energía.

4.4.4.3 La tecnología

Los dispositivos Bluetooth están catalogados en tres diferentes clases por la potencia que estos utilizan:

- Dispositivos Clase 3, tienen una potencia de transmisión de 1 mW y un rango de alcance de 0.1 a 10 metros.
- Dispositivos Clase 2, tienen una potencia de transmisión de 1 a 2.5 mW y un rango de alcance de 10 metros.
- Dispositivos Clase 1, tienen una potencia de transmisión arriba de 100 mW y un rango de alcance mayor de los 100 metros.

La arqITUectura de Bluetooth esta formada por la interface aérea, la banda de frecuencia libre y el administrador de enlace. Bluetooth usa una rango de frecuencia de 2.45 GHz. El

ancho de banda máximo teóricamente es de 1 Mbps, el cual levemente baja un bit por la FEC (Forward Error Correction, Corrección de Error Felantera).

El administrador de enlace es una parte esencial de la arqITUectura Bluetooth. Este utiliza un protocolo de administrador de enlace LMP (Link Manager Protocol, Protocolo de Administrador de Enlace) para configurar, autenticar y autorizar.

4.4.4.4 Seguridad en Bluetooth

Para asegurar la protección de la información se ha definido un nivel básico de cifrado, que se ha incluido en el diseño del chip de radio para proveer de seguridad en equipos que carezcan de capacidad de procesamiento, las principales medidas de seguridad son:

- Una rutina de pregunta-respuesta, para autenticación.
- Una corriente cifrada de datos, para cifrado.
- Generación de una clave de sesión (que puede ser cambiada durante la conexión).

Tres entidades son utilizadas en los algoritmos de seguridad: la dirección de la unidad Bluetooth, que es una entidad pública; una clave de usuario privada, como una entidad secreta; y un número aleatorio, que es diferente por cada nueva transacción.
Como se ha descrito anteriormente, la dirección Bluetooth se puede obtener a través de un procedimiento de consulta. La clave privada se deriva durante la inicialización y no es revelada posteriormente. El número aleatorio se genera en un proceso pseudos aleatorio en cada unidad Bluetooth.

Observemos con mayor detalle las medidas de seguridad de Bluetooth. Primero, debemos examinar la seguridad Bluetooth en general y como han sido tomadas en cuenta los diferentes detalles. Luego seguiremos acercándonos a algunos detalles específicos en la generación de la clave de sesión, cifrada y autenticación. Finalmente, veremos los aspectos de Ad hoc de la seguridad de Bluetooth. En cada dispositivo Bluetooth existen cuatro formas usadas para mantener la seguridad a nivel de enlace.
La dirección del dispositivo Bluetooth (BD_ADDR), la cual es una dirección de 48 bits que es única por cada dispositivo y es definida por la IEEE. La clave privada de autenticación, la cual es un número aleatorio de 128 bits y es usada para propósitos de autenticación. La clave privada de cifrado, la cual tiene una longitud entre 8 y 128 bits y es usada para el cifrado. Por ultimo, un numero aleatorio, el cual transforma frecuentemente los 128 bits aleatorios o pseudos aleatorios hechos por el dispositivo mismo.

En el perfil de acceso genérico, la seguridad en Bluetooth esta dividida en tres modos:

- Modo de Seguridad 1 No Seguro.
- Modo de Seguridad 2 El Nivel de servicio impone la seguridad.
- Modo de Seguridad 3 El nivel de enlace impone la seguridad.

La diferencia entre los modos de seguridad 2 y 3 es que en el Modo de Seguridad 3 los dispositivos Bluetooth inicializan los procedimientos de seguridad antes que el canal sea establecido También existen diferentes niveles de seguridad para dispositivos y servicios.

Para dispositivos existen 2 niveles, dispositivos fiables y dispositivos no fiables. Los dispositivos fiables obviamente tienen acceso sin restricciones a todos los servicios. Para servicios**,** existen 3 niveles de seguridad que son definidos así: servicios que requieren

autorización y autenticación, servicios que requieren solo autenticación y servicios que están abiertos para todos los dispositivos.

4.4.4.5 Versiones

- Bluetooth v.1.1
- Bluetooth v.1.2
- Bluetooth v.2.0

La versión 1.2, a diferencia de la 1.1, provee una solución inalámbrica complementaria para co-existir Bluetooth y Wi-Fi en el espectro de los 2.4 GHz, sin interferencia entre ellos. La versión 1.2 usa la técnica AFH (Adaptive Frequency Hopping, Salto de Frecuencia Adaptativa), que ejecuta una transmisión más eficiente y una cifrado más segura. Para mejorar las experiencias de los usuarios, la V1.2 ofrece una calidad de voz (Voice Quality - Enhanced Voice Procesing) con menor ruido ambiental, y provee una más rápida configuración de la comunicación con los otros dispositivos Bluetooth dentro del rango del alcance, como pueden ser PDA's, HIDs (Human Interface Devices, Dispositivos de interfae Humana), computadoras portátiles, computadoras de escritorio, Headsets, impresoras y celulares. La versión 2.0, creada para ser una especificación separada, principalmente incorpora la técnica EDR (Enhanced Data Rate, Tasad e Datos Mejorada) que le permite mejorar las velocidades de transmisión en hasta 3 Mbps a la vez que intenta solucionar algunos errores de la especificación 1.2.

4.4.4.6 Usos y aplicaciones

- Conexión sin cables entre los celulares y equipos de manos libres y kit para autos.
- Red inalámbrica en espacios reducidos donde no sea tan importante un gran ancho de banda.
- Comunicación sin cables entre la PC y dispositivos de entrada y salida. Mayormente impresora, teclado y Mouse.
- Transferencia de archivos entre dispositivos.
- Reemplazo de la tradicional comunicación por cable entre equipos GPS y equipamiento médico.
- Controles remotos (tradicionalmente dominado por el infrarrojo)
- Enviar pequeñas publicidades entre anunciantes y dispositivos con Bluetooth. Un negocio podría enviar publicidad a celulares / teléfonos móviles con Bluetooth activado al pasar cerca.
- Las consolas Sony Playstation 3 y Nintendo Wii traen Bluetooth para utilizar controles inalámbricos.

4.4.4.7 Clases de dispositivo

La clasificación de los dispositivos Bluetooth como "Clase 1", "Clase 2" o "Clase 3" es únicamente una referencia de la potencia de transmisión del dispositivo, siendo totalmente compatibles los dispositivos de una clase con los de la otra.

Los dispositivos de Clase 1 se definen como con un alcance de 100 metros, mientras que los de Clase 2 llega a los 20/30 metros, y los de Clase 3 a un metro aproximadamente. Si un dispositivo de clase 1 desea conectarse con uno de clase 2, deberán colocarse la distancia del alcance del de clase 2, ya que por más que el otro sea clase 1, debe ponerse a la distancia donde llega el de clase 2.

Cabe aquí aclarar que las distancias que indican las especificaciones son medidas tomando punto a punto dos dispositivos de la misma clase, instalados a campo abierto, sin ninguna interferencia. La realidad es que en instalaciones normales en interiores de edificios, la distancia oscila entre 5 y 25 metros, según las condiciones ambientales.

Además, existen ciertos dispositivos en los que la señal se amplifica hasta un nivel en teoría por encima del máximo permitido por la tecnología. Así, es fácil encontrar a la venta adaptadores USB Bluetooth con un alcance de 150 metros, que son considerados de Clase 1. Por otro lado, mediante técnicas como Bluetoone o Bluesniping se logra, mediante antenas más potentes y/o direccionales, obtener alcances de entre uno y dos kilómetros.

4.4.5 Wi-Fi

Existen varias tecnologías de transmisión inalámbrica pero la más conocida es la Wi-Fi, publicada bajo el estándar 802.11, ésta ha variado a lo largo de los tiempos pues como todo en el mundo tecnológico, se han producido varios cambios o actualizaciones, como por ejemplo: 802.11a, 802.11b, 802.11g las cuales trabajan a diferentes velocidades:

- 802.11 = 1 Mbps.
- 802.11a = 54 Mbps (Ésta trabaja a una frecuencia en el rango de los 5 GHz).
- 802.11b = 11 Mbps (Trabaja a 2.4 GHz. Conserva compatibilidad con el estándar nativo 802.11 de 1 Mbps)
- 802.11g = 54 Mbps (Trabaja a 2.4 GHz. Puede alcanzar los 108 Mbps con dispositivos del mismo fabricante, siempre que se den las condiciones óptimas y sólo si el fabricante hizo la adaptación).

IEEE 802.11 o Wi-Fi es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arqITUectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local. La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos.

El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2.4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11 legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2.4 GHz. También se realizó una especificación sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g.

El siguiente paso se dará con la norma 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen un primer borrador del estándar N con un máximo de 300 Mbps (80-100 estables). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a

especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b. Los estándares 802.11b y 802.11g utilizan bandas de 2.4 GHz que no necesitan de permisos para su uso. El estándar 802.11a utiliza la banda de 5 GHz. El estándar 802.11n hará uso de ambas bandas, 2,4 GHz y 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2.4 GHz.

4.4.5.1 Conceptos generales

- Estaciones: computadoras o dispositivos con interfaz inalámbrica.
- Medio: se pueden definir dos la radiofrecuencia y los infrarrojos
- AP (Punto de acceso): tiene las funciones de un puente (conecta dos redes con niveles de enlaces parecidos o distintos), y realiza por tanto las conversiones de trama pertinente.
- Sistema de distribución: importantes ya que proporcionan movilidad entre AP, para tramas entre distintos puntos de acceso o con los terminales, ayudan ya que es el mecánico que controla donde esta la estación para enviarle las tramas.
- BSS (Conjunto de servicio básico): Grupo de estaciones que se intercomunican entre ellas. Se define dos tipos:
- Independientes: cuando las estaciones, se intercomunican directamente.
- Infraestructura: Cuando se comunican todas a través de un punto de acceso.
- ESS (Conjunto de servicio Extendido): Es la unión de varios BSS.
- BSA (Área de Servicio Básico): es la zona donde se comunican las estaciones de una misma BSS, se definen dependiendo del medio.
- Movilidad: este es un concepto importante en las redes 802.11, ya que lo que indica es la capacidad de cambiar la ubicación de los terminales, variando la BSS. La transición será correcta si se realiza dentro del mismo ESS en otro caso no se podrá realizar.
- Límites de la red: Los límites de las redes 802.11 son difusos ya que pueden solaparse diferentes BSS.

Capitulo 5

5. Tecnologías de PDA's

5.1 Introducción

El desarrollo de la electrónica ha llevado en los últimos años a la optimización de recursos y a reducir los tamaños de los dispositivos, con características de procesamiento cada vez superiores. Esto ha ayudado a la masificación de la tecnología, y a la creación de productos cada vez más portátiles y económicos.
El concepto de una agenda electrónica, es una concepción nueva que la tecnología ya ha hecho posible en neutros tiempos. Estos equipos están logrando que la tecnología se vea de otra forma y que el acceso a la información se realice de una manera rápida y oportuna, dando características de movilidad, y portabilidad.

5.2 Historia

La idea de la PDA nace en la literatura de 1956 de Isaac Asimov, su trabajo "Pocket Terminal" and "Pocketsec" donde definía las características básicas de una PDA y ponía de manifiesto algunas utilidades que esta tecnología podría tener, la idea encontró suelo fértil y se publicaron diferentes trabajos en la década que no pasaron de ser trabajos de ciencia ficción, trabajos como el de George Margolin's en 1974 que planteaba una calculadora de entrada y salida alfanumérica que permitía aparte de realizar las funciones básicas de una calculadora científica, almacenar y procesar datos alfanuméricos, donde se podían almacenar directorios telefónicos, y pequeñas notas.
HP desarrollo esta idea y logro crear el primer prototipo que se aprecia en la figura 5.1, en 1973 la HP-45 este fue el primer equipo que incluya características de alarmas, reloj, y agendas a aparte de las características de la calculadora convencional. Los detalles de este prototipo se publicaron en el libro A Guide to HP Handheld Calculators and Computers en donde se documentaron las fallas del prototipo, relacionadas a los cristales osciladores y a la poca electrónica de la época.

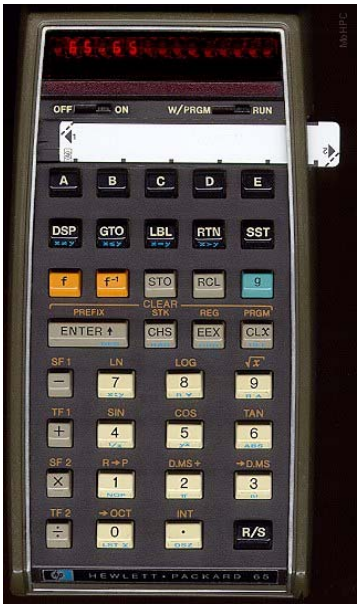


Figura 5.1 HP-45 primer prototipo de PDA desarrollada por HP.

En 1974 se mejoraron los problemas del prototipo y se lanzo al mercado el primer organizador electrónico, HP-65 que era una calculadora programable, el cual tenia una cinta magnética removible donde podían almacenarse los datos del usuario.

En 1975 Satyanarayan Gangaram Pitroda quien es considerado un pionero de las PDA´s desarrollo y construyo una Pre PDA que incluía archivación de notas, mensajes de alarmas, este equipo salio al mercado con el nombre de “Electronic Diary” y se inscribió con la patente #3,999,050. Pitroda viajo a Chicago y Illinois, y mostró su idea a colegas en la industria de le electrónica, llegando a oídos de Bob Noyce, que trabajaba en el desarrollo de PBX y en la creación de nuevos microprocesadores para una compañía que luego se conocería bajo el nombre de Intel. La idea se llevo a fabricantes como Casio, HP, Radio Shack, Sharp, y Texas Instruments, la idea fue mas fértil en el mercado Japones donde se desarrollo la fabricación masiva de esta y dio como resultado diferentes productos como la Casio Computer Quartz. CQ1 que se muestra en la figura 5.2.

Figura 5.2 Casio Computers Quartz CQ1

Este equipo no tuvo la aceptación esperada en el mercado y pocas unidades fueron vendidas, sin embargo la idea siguió en los desarrolladores. En 1976 en Silicon Valley Xerox desarrolla su primera computadora portátil mostrada en la figura 5.3, la cual incluía una pequeña pantalla basada en tubo de rayos catódicos, y un teclado. El conjunto era capaz de almacenar datos y de nivel mediano de procesamiento, orientado a la investigación, incluía también algún software como diccionarios y traductores de ingles a otros idiomas como el griego.

Figura 5.3 Prototipo de Xerox

El desarrollo continuo generando mas ofertas en el mercado y la idea se expandió a cada vez mas fabricantes que buscaban introducir mas procesamientos y funciones al equipo. SHARP desarrollo la PC 1211 como se muestra en la figura 5.4, la cual ya se denominaba computador de bolsillo ya que incluía varias funcionalidades de las computadoras de la época. Traductor, diccionario, agenda, alarmas, calculadora, almacenamiento de la información.

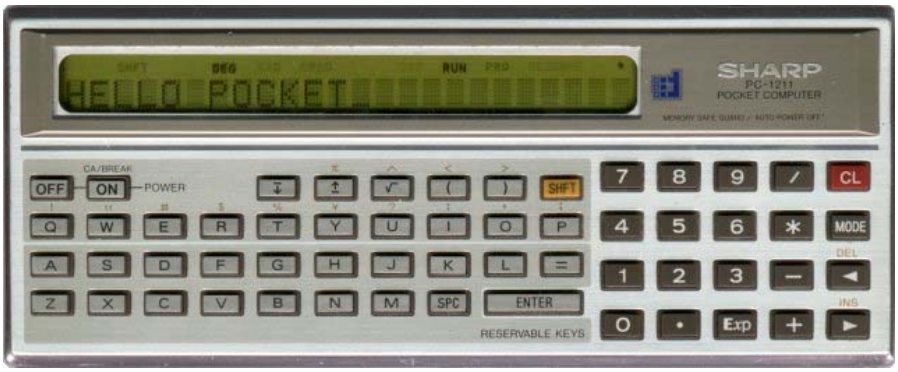


Figura 5.4 Sharp PC 1211

CASIO no se quedo atrás y creo la DATA BANK (banco de datos) que se muestra en la figura 5.5 que incluyo la detección de escritura natural, concepto que permitió la masificación de estos equipos y que agrego una nueva característica a los equipos que debían salir al mercado, consolidando cada vez mas las características que actualmente se conocen de una PDA.

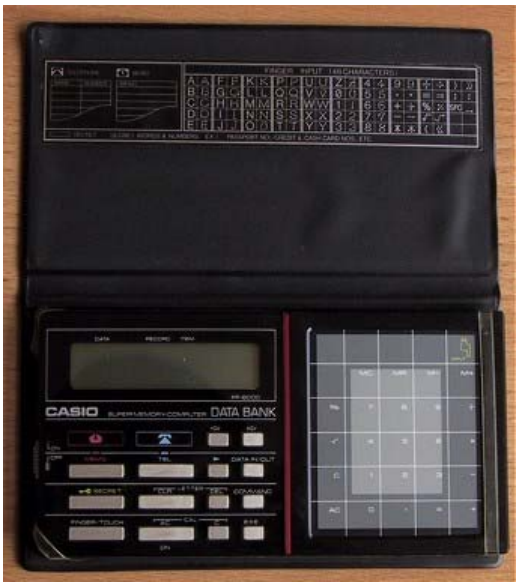


Figura 5.5 CASIO PF 8000

Desarrollos como los logrados por Atari en sus consolas de video juegos portátiles que luego fueron mejoradas por Nintendo en su versión portátil de GameBoy, mostraron las mejoras en el tema de pantallas de cristal líquido y dieron un atractivo extra a los equipos. En 1990 otros fabricantes como AT&T y Apple desarrollaron pantallas sensibles al tacto, esta tecnología maduro y se incluyo en los nuevos dispositivos. En 1994 Apple en colaboración con Sun Microsystem generan un equipo que incluía, la pantalla sensible al tacto así como funciones de reconocimiento de voz, este equipo era el Newton PAD. La propaganda lanzada para este equipo fue masiva y fue el primero en denominarse PDA. IBM realizo una alianza estratégica con la compañía BellSouth y como resultado se creo la primera PDA con funciones de comunicación que ya incluía el uso de correo electrónico, recepción de FAX y realización de llamadas, esto fue posible por la inclusión de un modem dial up.

En 1996 Sharp y Apple crean el consorcio PALM y lanzan la serie de equipos PILOT como en la figura 5.6, la cual fue un éxito en el mercado este equipo incluía todas las funciones de calculadora, agenda, alarmas, calendario, pantalla sensible al tacto, reconocimiento de escritura natural, y aplicaciones como diccionario y traductor. Este éxito potencio a la compañía Palm y la ubico en un sitio privilegiado en el marcado, convirtiendo a la marca Palm en un sinónimo de PDA.

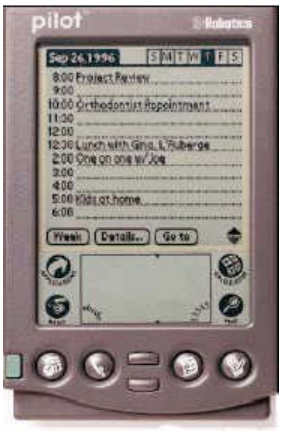


Figura 5.6 Modelo PILOT del consorcio Sharp-Apple.

Actualmente la carrera del desarrollo crece agrandando mas funcionalidades a las PDA e incluyendo características avanzadas de comunicación, desde la adición de telefonía celular hasta la posibilidad de hacer uso de redes de datos WLAN, y de agregar funcionalidades como GPS, lector de barras, cámaras digitales, etc.

5.3 Software

Gran parte del desarrollo y desimanación de esta tecnología se debe a los avances logrados en materia de software, en donde las nuevas técnicas de programación en conjunto con microprocesadores más rápidos y económicos han logrado crear los equipos que hoy vemos en el mercado. En la industria de las PDA existe una gama de fabricantes que han logrado desarrollar de forma casi independiente la tecnología de PDA y este rubro carece de estándares, universales en la fabricación y procesamiento, lo que ha permitido crear estándares de facto, lo que hace incompatibles entre si a estos sistemas.

El desarrollo y la aceptación de los sistemas operativos se han visto favorecida por la cantidad de aplicaciones existentes para cada sistema operativo. Actualmente existen una amplia gama de aplicaciones que van desde simples organizadores, procesadores de texto, hojas de calculo y aplicaciones de archivos multimedia, hasta programas para astronomía, medicina e ingeniería. En la figura 5.7 se muestra la cantidad de aplicaciones existentes para los sistemas operativos comúnmente utilizados en dispositivos portátiles.

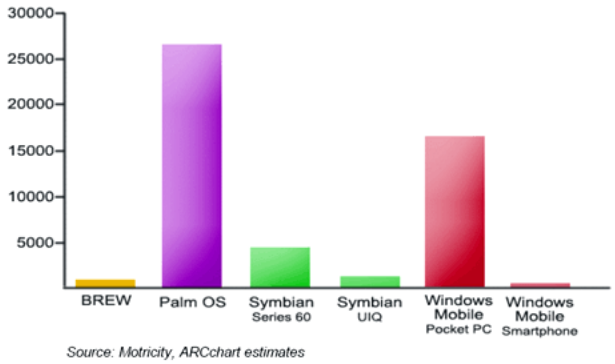


Figura 5.7 Aplicaciones existentes para cada SO para el año 2006.

Podemos observar que los sistemas con mas presencia, y desarrollo son básicamente dos, el Palm OS que esta desarrollado para correr en dispositivos Palm y el Windows Mobile, que esta desarrollado para funcionar en Pocket PC. Pocket PC, es un termino utilizado para denominar a un dispositivo PDA cuyo núcleo o lógica de funcionamiento esta basada en la plataforma API Win32. API Win32 , es una interface de programación de aplicaciones (Application Programming Interface), que funciona mediante un conjunto de librerías que especifican las relaciones entre los programas y el núcleo principal del sistema operativo; esta versión de API esta pensada para sistemas de 32 bits, y es similar a la usada por los sistemas Windows para computadores de escritorio.

El API Win32 tienen básicamente las siguientes funciones:

- Depuración y manejo de errores
- E/S de dispositivos
- Procesos e hilos
- Comunicación entre procesos
- Manejo de la memoria
- Monitoreo del desempeño
- Manejo de energía
- Almacenamiento
- Información del sistema
- GDI (interfaz gráfica)
- Interfase de usuario.

Esta plataforma fue desarrollada por la empresa Microsoft y es utilizada en sistemas operativos denominados multitarea, que están diseñados para ejecutar múltiples rutinas a la vez mediante el uso de múltiples unidades de procesamiento que interactúan por medio de llamadas, comúnmente denominadas interrupciones que pueden ser provocadas por el cambio en las interfaces de usuario (tales como pulsaciones de teclado o movimiento de un Mouse) o bien por programas montados sobre la rutina principal.

Los sistemas multitarea pueden ser de varios tipos:

- Nula: El sistema operativo carece de multitarea. Aún así puede lograrse a veces algo parecido a una multitarea implementándola en espacio de usuario, o usando trucos como los TSR de MS-DOS. Un ejemplo típico de un sistema no multitarea es MS-DOS y sus clones.

- Cooperativa: Los procesos de usuario son quienes ceden la CPU al sistema operativo a intervalos regulares. Muy problemática, puesto que si el proceso de usuario se interrumpe y no cede la CPU al sistema operativo, todo el sistema estará trabado, es decir, sin poder hacer nada. Da lugar también a latencias muy irregulares, y la imposibilidad de tener en cuenta este esquema en sistemas operativos de tiempo real. Un ejemplo sería Windows hasta la versión 95.
- Preferente: El sistema operativo es el encargado de administrar el procesador, repartiendo el tiempo de uso de este entre los procesos que estén esperando para utilizarlo. Cada proceso utiliza el procesador durante cortos períodos de tiempo, pero el resultado final es prácticamente igual que si estuviesen ejecutándose al mismo tiempo. Ejemplos de sistemas de este tipo serían Unix y sus clones (FreeBSD, Linux...), VMS y derivados, AmigaOS, Windows NT.
- Real: Sólo se da en sistemas multiprocesador. Es aquella en la que varios procesos se ejecutan realmente al mismo tiempo, en distintos microprocesadores. Suele ser también preferente. Ejemplos de sistemas operativos con esa capacidad: variantes Unix, Linux, Windows NT, etc.

5.3.1 Windows Mobile

Windows Mobile (en el transcurso del documento será mencionado como WinM) es diseñado y distribuido por la empresa Microsoft, la creadora del sistema operativo Windows para computadoras convencionales. WinM es un sistema desarrollado sobre una plataforma API Win32 que es la plataforma en la cual esta basada el sistema operativo Windows, este desarrollo esta pensado para que las aplicaciones y el ambiente de la PDA sean similares al utilizado en las computadoras con la plataforma Windows. Microsoft desarrollo una nueva versión de sistema operativo orientada a dispositivos portátiles, con opciones de conectividad y microprocesadores de 32 bits, este SO se denomino Windows CE, el cual a pesar de su parecido en la interfase grafica con Windows XP y Windows NT, no es una consecución de estos ni una versión comprimida de estos, sino mas bien un SO nuevo basado en nuevas formas de procesamiento y diseñado para dispositivos de 32 bits. La primera versión de Windows CE fue lanzada en el año 2001 en su primera versión Pocket PC, esta versión tuvo poca aceptación, debido a la falta de compatibilidad con otros dispositivos y a la poca o nula conectividad ofrecida, y se convirtió en una versión de prueba e investigación. Nuevas mejoras en el tema de compatibilidad con la plataforma Windows para PC, que es el SO mas utilizado y conocido por los usuarios de computadoras en el mundo ayudaron a su diseminación, en conjunto con la estrategia de mercado de distribuir el sistema operativo en las PDA de diferentes fabricantes como DELL, Acer, y HP este ultimo un pionero en la industria de las PDA ubicaron al sistema operativo como una alternativa a considerar.

El lanzamiento de las denominadas Pocket PC 2002 que utilizaban la versión Windows CE 3.0 desarrollada exclusivamente para equipos con pantallas 240 × 320 píxeles (QVGA; pantallas sensibles a la presión), y con opciones de conectividad mediante puertos como el IrDA, conexiones seriales cableadas. Comercialmente a este sistema operativo se le denomino Windows Mobile 2002 y se desarrollo una versión para Pocket PC y para Smart Phone. Los avances en materia de hardware tales como resolución de las pantallas y velocidades de procesamiento dieron lugar a las mejoras de los SO, y en tal sentido se desarrollo la tercera versión es Windows Mobile 2003, esta fue lanzada el 23 de junio, 2003, y era el primer lanzamiento bajo el nombre Windows Mobile.

Para Windows Mobile 2003 se crearon tres diferentes versiones:

- Windows Mobile 2003 Pocket PC Edition: esta versión fue creada para PDA´s con características de procesamiento avanzadas para la época, para equipos de resoluciones medias; esta distribución fue difundida por HP, DELL y Acer.
- Windows Mobile 2003 Pocket PC Phone Edition: Esta versión fue creada para PDA con prestaciones de telefónica celular, y en tal sentido ofrece aplicaciones para equipos que tendrán un procesamiento dividido en funciones de teléfono y PDA. Fue difundido esencialmente por HTC´s Himalaya, en los dispositivos Qtek, XDA, MDA y VPA
- Windows Mobile 2003 Smartphone Edition: esta versión es utilizada en teléfonos celulares inteligentes que poseen algunas características de PDA's tales como agendas y pequeños procesadores de palabras y hojas de cálculo. Esta versión corre en equipos con limitaciones como la carencia de pantallas sensibles a la presión, resoluciones bajas, limitadas características de procesamiento y almacenamiento de memoria.

Por presión de los fabricantes en el tema de conectividad y resolución de los nuevos dispositivos, se creo una segunda versión de Windows Mobile 2003 que incluía entre otras prestaciones, la inclusión del navegador Internet Explorer Mobile y soporte para redes Wi-Fi, que sus sucesores no tenían.

Windows Mobile 5.0, salió al mercado el 9 de mayo del 2005. Utiliza Windows CE 5.0 y tecnología .NET para su desarrollo, entre las características básicas de esta versión están:

- Una nueva versión de Office llamada "Office Mobile".
- Powerpoint Mobile.
- Excel Mobile añade la capacidad de ver representaciones gráficas.
- Word Mobile incluirá la capacidad de insertar tablas y gráficos.
- Windows Media 10 Mobile reproductor de archivos multimedios (videos en formatos AVI, MPEG y audio MP3, MID, WAV).
- Conectividad Bluetooth.
- Interfaz de administración GPS.
- ActiveSync 4.2, prometiendo 10-15% de aumento de la velocidad en la sincronización de datos.
- Cliente para PPTP y L2TP/IPsec VPNs.
- Soporte para utilización de memoria flash SD.

El desarrollo de estos sistemas puede observarse en la tabla 5.1:

Sistema Operativo	Características	Interface Grafica
Windows C.E.	Para sistemas PDA Kernel Ad-hoc Basado en componentes Multitarea tipo tiempo real	No aplica

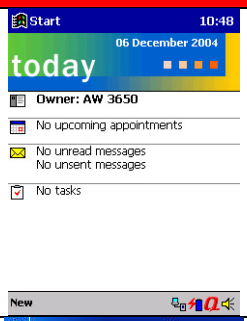
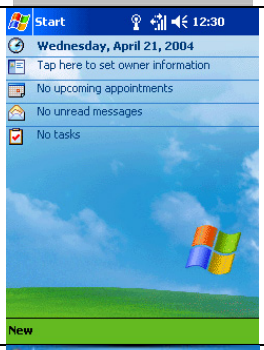
Sistema Operativo	Características	Interface Grafica
Pocket PC 2000	1. Codename: Rapier 2. Basado en Win CE 3 3. Pocas aplicaciones 4. No tuvo mucha aceptación.	
Pocket PC 2002	1. Codename: Merlin 2. Basado en Win CE 3 3. Enfocado a QVGA (240 × 320 pixeles) 4. Sin soporte QWERTY[31]	
Windows Mobile 2003	1. Codename: Ozone 2. Tres ediciones 3. Soporta WiFi 4. Soporta Compact Framework 5. WMP9	
Windows Mobile 5	1. Codename: Magneto 2. Basado en Win CE 5 3. Compact Framework 4. Office Mobile 5. Messaging queue 6. Soporte QWERTY 7. Error reporting 8. Persistent storage	

Tabla 5.1 Algunos sistemas operativos.

5.3.2 PALM OS

El sistema operativo Palm fue desarrollado originalmente por Jeff Hawkins para el Pilot PDA de US Robotics. La versión 1.0 se vendía con los primeros Pilot 1000 y 5000 y la versión 2.0 se introducía con el Palm Pilot Personal y Profesional. Cuando salieron los

[31] Tipo de teclado de software y hardware mediante la conexión Irda.

Palm de la serie III se introdujo la versión 3.0 del Sistema operativo. Posteriormente salieron las versiones 3.1, 3.3 y 3.5, que añadían apoyo para color, puertos de expansión múltiples, nuevos procesadores y otras prestaciones. La versión 4.0 salió con la serie m500, y más tarde salió la actualización para aparatos anteriores. Esto añadía una interfaz estándar para el acceso del sistema de archivos externo (como tarjetas SD) y mejoraba las bibliotecas de telefonía, seguridad y mejoras de IU.

La versión 5.0 (Garnet) fue la primera versión que soportó los dispositivos ARM (microprocesador RISC diseñado originalmente por Acorn Ltd., a veces llamado Advanced RISC Machine). Anunciado como paso importante por apoyar a los procesadores ARM, las aplicaciones Palm se ejecutan en un entorno emulado denominado el Entorno de Compatibilidad de Aplicaciones Palm (PACE en inglés), disminuyendo velocidad pero permitiendo gran compatibilidad con programas antiguos. El software nuevo puede aprovechar los procesadores de ARM con ARMlets, pequeñas unidades de código ARM. Era también aproximadamente entonces cuando Palm empezaba a separar sus divisiones de hardware y de sistemas operativos, y finalmente se convierten en dos compañías PalmSource, Inc. (sistemas operativos) y PalmOne, Inc. (hardware). Las siguientes versiones de Palm OS 5 han tenido un API estándar para alta resolución y áreas de entrada dinámicas, junto con un cierto número de mejoras menores.

Palm OS 4.1.2, 5.1 y posteriores, incluyen Graffiti 2, debido a la pérdida de un pleito de violación con Xerox. Graffiti se basa en Jot de CIC. PalmSource, Inc. presentó Palm OS Cobalt (también denominado Palm OS 6) a los licenciatarios el 29 de diciembre de 2003. Esto completaría la migración a aparatos con ARM, y permitiría apoyar a las aplicaciones nativas ARM junto con apoyo multimedia mejorado. Actualmente NO existen equipos que usen el Palm OS 6 o Cobalt. No está muy claro el futuro de esta versión de Palm OS, derivado de la compra de PalmSource por la compañía japonesa ACCESS, LTD. Aparentemente, en algún momento será posible tener nuevos equipos PDA con Palm OS cuyo núcleo (Kernel) sea un Linux completamente funcional.

Capitulo 6

6. Análisis y diseño del sistema.

6.1 Introducción.

A continuación veremos a detalle la aplicación, después de analizar las entrevistas, documentos e información, y revisar entre la variedad de protocolos, sistemas, y equipo para tomar una decisión mas acertada acerca de la implementación de la aplicación.

Lo primero a analizar es el flujo de la información del Hospital Bloom, en donde el problema a solventar es el llenado de la información general del paciente, la generación de una receta y los cuadros estadísticos utilizados en el centro hospitalario.

El siguiente tema será el acceso inalámbrico, eligiendo WIFI como la opción sobre otros protocolos inalámbricos. También se tratará el lenguaje PHP como el elegido para el desarrollo de la aplicación, debido a la versatilidad de este lenguaje y a que las PDA tienen un navegador Web que nos garantiza las interoperabilidad entre ambas hardware y sistemas operativos. Además explicaremos que tipo de servidor http se ha utilizado.

Abordaremos además el tema de la base de datos, su nivel de complejidad, las limitantes de la aplicación de la solución y para finalizar hablaremos sobre seguridad de red y de software aire, así como también el de integridad de la información

6.2 Análisis y modelado del proceso a estudiar.

6.2.1 Modelado del proceso, flujo de la información.

El manejo de información del paciente es uno de los puntos más delicados dentro de un ambiente hospitalario, debido a que de su manipulación, dependen muchas tomas de decisiones en torno a los procesos a seguir con el paciente, como tal, requiere mucha privacidad, responsabilidad y cuidado trabajar con ellos.

En la siguiente sección se muestra un análisis de flujo de datos relacionados al área de emergencias dentro del hospital para niños Benjamín Bloom, tomando en cuenta que cada uno de los servicios y especialidades dentro del hospital genera una cantidad alta de formularios, limitaremos el flujo de datos a algunos procesos generales al momento de asistir a dicho hospital.

En la figura 6.1 describiremos dicho flujo de datos.

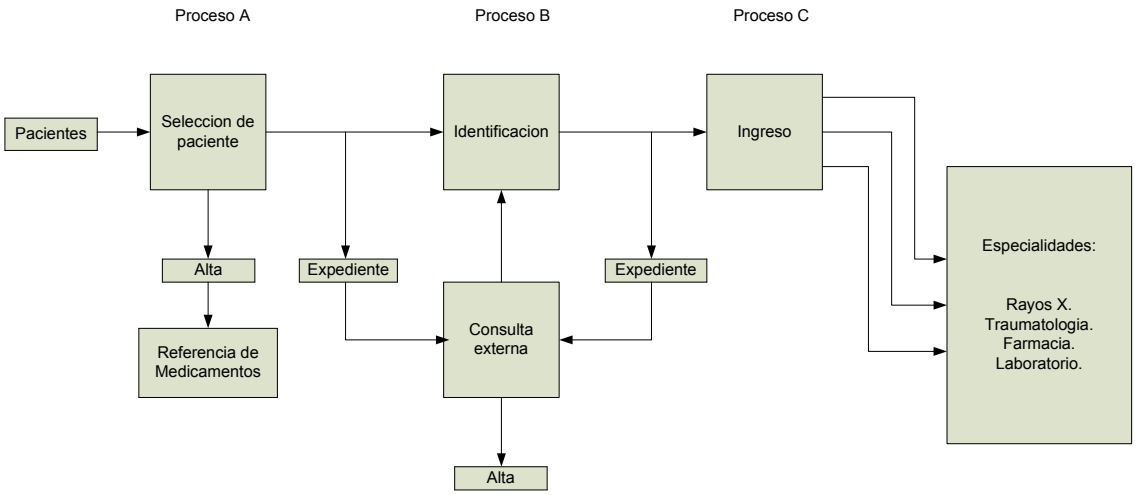


Figura 6.1 Flujo de datos para el área de emergencias.

Dividimos el modelado de la información y el flujo de datos en tres procesos que a continuación explicamos para el área de emergencias en el hospital Benjamín Bloom:

- Proceso A: el paciente llega al hospital por el padecimiento de una enfermedad, por medio de una selección de paciente los médicos en turno tienen la disposición de poder dar de alta al paciente con referencia de medicamentos si así lo requiere, o por otro lado pueden referir internamente al paciente para una identificación por medio de un médico especialista.
- Proceso B: una vez avalada la identificación del paciente se procede a la verificación del expediente clínico (si ya lo hubiese) o se le extiende en el momento para poder determinar si es necesaria la remisión a un especialista para su posterior ingreso, si no lo fuese así se le podrá dar de alta siempre o se le remeterá a una consulta externa por medio de otro centro de atención de menor nivel.
- Proceso C: una vez aprobado el ingreso por el médico se procede a la verificación de la especialidad donde será ingresado el paciente.

En cada uno de los procesos antes mencionados se generan formularios para el procesamiento e identificación de los datos de cada paciente.

6.3 Método de acceso Wi-Fi.

En base a la información recopilada en los capítulos anteriores, hemos tomado en consideración todas las normativas y recomendaciones giradas por organizaciones internacionales, para poder cumplir la normativa de compatibilidad electromagnética entre la aplicación y el equipo médico que intervenga.

Para nuestra aplicación hemos decidido utilizar como protocolo de acceso inalámbrico la tecnología 802.11 conocida como Wi-Fi basándonos en sus características técnicas, tipo de aplicación a operar y la facilidad de implementación como lo muestra la tabla 6.1.

Estandar	802.11b/g	Bluetooth	IRDA
Organismo	IEEE	Bluetooth SIG	IBM,HP,SHARP

Estandar	802.11b/g	Bluetooth	IRDA
Finalización	1999	2002	1993
Bandas de frecuencias	2.4 GHz	2.4 GHz	300 GHz a 200 THz
Velocidad máxima	11 Mbps/54 Mbps	721 Kbps	9.6 Kbps/16 Mbps
transferencia media	5.5 Mbps	36 Mbps	-
Interfaz aire	SSDS/FH/OFDM	DSSS/FHSS	-
Rango de alcance	100 metros	10 metros	5 metros

Tabla 6.1 Selección de protocolo de acceso.

Entre los puntos determinantes para utilizar Wi-Fi tenemos:

- Mayor ancho de banda, que incluye bandas de reserva para protección frente a interferencias producidas por canales adyacentes.
- Permite transmisión de voz y/o vídeo.
- Los dispositivos de telemetría médica compatibles con IEEE 802.1X pueden comunicarse con otros dispositivos inalambricamente o cableados utilizando puntos de acceso. La limitación del número de dispositivos conectados, la determina la infraestructura del punto de acceso.
- La banda ISM está disponible y es accesible en todo en mundo para aplicaciones inalámbricas, con la implicación que supone de economía de escala y mejora de prestaciones.
- Las características de propagación de las frecuencias en la banda de 2.4 GHz hacen que sea la banda óptima para utilización en el interior de edificios, donde su estructura atenúa la señal entre pisos.
- El cumplimiento de la especificación IEEE 802.1X permite el transporte de los dispositivos sin necesidad de resintonización
- Aunque la gestión del espectro es necesaria, no hace falta una gestión de las frecuencias, incluso para aplicaciones multi-hospitalarias.
- La utilización de herramientas de gestión de redes permite monitorizar el tráfico en la red para determinar la carga y los factores de utilización cuando la carga de la red excede un umbral.
- La escalabilidad permite soluciones flexibles a un coste óptimo según las necesidades de la red.
- La norma IEEE 802.11 especifica un mecanismo de seguridad que proporciona acceso a comunicaciones seguras punto a punto.
- A diferencia de los sistemas tradicionales de telemetría, el paciente sometido a monitorización no está sujeto a un receptor particular.

6.4 Lenguajes de programación (PHP).

El lenguaje de programación que fue seleccionado para la aplicación fue PHP (Hypertext Pre-processor), debido a su excelente compatibilidad entre los sistemas operativos de las PDA`s, ya que ambas utilizan navegadores Web que son compatibles con dicho lenguaje, y es un lenguaje muy flexible comparado con otros que son mas complejos y con alcances mucho más limitados.

En la tabla 6.2 mostramos algunas de las características de los diferentes lenguajes de programación que pudimos haber utilizado, y como PHP es el que cubre todas las necesidades de la aplicación.

Compatibilidad Software/Sistema operativo		
Lenguaje de programación	**PALM OS**	**Pocket PC Windows Mobile**
C++	No	Si
Visual Basic	No	Si
Palm Development	Si	No
HTML	Si	Si
PHP	Si	Si

Tabla 6.2 Características de algunos lenguajes de programación[32].

PHP es un lenguaje de programación usado frecuentemente para la creación de contenido para sitios Web tal como lo es nuestra aplicación. En estos sitios se pueden programar las páginas html y los códigos fuente que son los que se conectarán a las distintas bases de datos. PHP tiene distintos significados que han cambiado a medida ha ido evolucionando por ejemplo "PHP Hypertext Pre-processor" (inicialmente PHP Tools, o, Personal Home Page Tools), y se trata de un lenguaje interpretado, usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios Web. Últimamente también para la creación nuevas aplicaciones con mejoras grandes a nivel gráfico que dan una mejor experiencia de usuario.

6.4.1 Características y funcionamiento.

Su interpretación y ejecución se da en el servidor Web, en el cual se encuentra almacenado el script (Instrucciones internas de una aplicación), y el cliente sólo recibe el resultado de la ejecución. Cuando el cliente hace una petición al servidor para que se le envíe una página Web, generada por un script PHP, el servidor ejecuta el intérprete de PHP, el cual procesa el script solicitado que generará el contenido de manera dinámica, pudiendo modificar el contenido a enviar, y regresa el resultado al servidor, el cual se encarga de regresárselo al cliente. Además es posible utilizar PHP para generar archivos PDF, Flash, así como imágenes en diferentes formatos, entre otras cosas. Permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, Postgres, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird y SQLite; lo cual permite la creación de Aplicaciones Web muy robustas.

PHP también tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos tales como UNIX (y de ese tipo, como Linux), Windows y Mac OS X, y puede interactuar con los servidores de Web más populares, ya que existe en versión CGI (Common Gateway Interface, pasarela de Interfaz Común), además es una importante tecnología de la World Wide Web que permite a un explorador Web solicitar datos de un programa ejecutado en un servidor Web. CGI especifica un estándar para transferir datos (entre el cliente y el programa), y para nuestra aplicación los sistemas operativos PALM OS y Windows Mobile.

[32] http://es.wikipedia.org/wiki/PHP

6.4.2 Historia

PHP fue originalmente diseñado en Perl, seguido por la escritura de un grupo de CGI binarios, escritos en el lenguaje C por el programador danés-canadiense Rasmus Lerdorf en el año 1994 para mostrar su currículum vitae y guardar ciertos datos, como la cantidad de tráfico que su página Web recibía. El 8 de junio de 1995 fue publicado "Personal Home Page Tools[33]" después de que Lerdorf lo combinara con su propio Form Interpreter para crear PHP/FI.

6.4.3 PHP 3.2.4.3

Dos programadores israelíes del Technion, Zeev Suraski y Andi Gutmans, reescribieron el analizador sintáctico (parser en inglés) en el año 1997 y crearon la base del PHP 3, cambiando el nombre del lenguaje a la forma actual. Inmediatamente comenzaron experimentaciones públicas de PHP 3 y fue publicado oficialmente en junio del 1998. Para 1999, Suraski y Gutmans reescribieron el código de PHP, produciendo lo que hoy se conoce como Zend Engine o motor Zend, un portmanteau de los nombres de ambos, Zeev y Andi. También fundaron Zend Technologies en Ramat Gan, Israel.

6.4.4 PHP 4

En mayo de 2000 PHP 4 fue lanzado bajo el poder del motor Zend Engine 1.0. La última versión de PHP 4, disponible en febrero de 2007 es la 4.4.5. El soporte a PHP 4 continúa activo lanzando parches de seguridad para aquellas aplicaciones que lo requieren.

6.4.5 PHP5

El 13 de julio de 2004, fue lanzado PHP 5, utilizando el motor Zend Engine II (o Zend Engine 2). La versión más reciente de PHP es la 5.2.3, que incluye todas las ventajas que provee el nuevo Zend Engine 2 como:

- Soporte sólido para Programación Orientada a Objetos (OOP) con PHP Data Objects.
- Mejoras de rendimiento.
- Mejor soporte para MySQL con extensión completamente reescrita.
- Mejor soporte a XML (XPath, DOM).
- Soporte nativo para SQLite.
- Iteradores de datos.
- Excepciones de errores
- Esta es la última versión a Mayo 2007.

6.4.6 PHP 6

Está previsto el lanzamiento en breve la versión 6 de PHP, cuando se lance esta nueva versión, quedarán tres ramas activas en desarrollo (PHP 4, 5 y 6).
Las diferencias que encontraremos frente a PHP 5 son:

- Soportará Unicote.
- Limpieza de funcionalidades obsoletas como register,globals, safe_mode.
- PECL.
- Mejoras en orientación a objetos.

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

6.4.7 Usos de PHP

Los principales usos del PHP son los siguientes:

- Programación de páginas Web dinámicas, habitualmente en combinación con el motor de base datos MySQL, aunque cuenta con soporte nativo para otros motores, incluyendo el estándar ODBC, lo que amplía en gran medida sus posibilidades de conexión.
- Programación en consola, al estilo de Perl o Shell scripting.
- Creación de aplicaciones gráficas independientes del navegador, por medio de la combinación de PHP y GTK (GTK es un grupo importante de bibliotecas o rutinas para desarrollar interfaces gráficas de usuario “GUI” para principalmente los entornos gráficos GNOME, XFCE y ROX de sistemas Linux),lo que permite desarrollar aplicaciones de escritorio en los sistemas operativos en los que está soportado.

6.4.8 Ventajas de PHP

Dentro de las ventajas que ofrece PHP podemos encontrar:

- Es un lenguaje multiplataforma.
- Capacidad de conexión con la mayoría de los manejadores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL.
- Leer y manipular datos desde diversas fuentes, incluyendo datos que pueden ingresar los usuarios desde formularios HTML.
- Capacidad de expandir su potencial utilizando la enorme cantidad de módulos (llamados ext's o extensiones).
- Posee una amplia documentación en su página oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Permite las técnicas de Programación Orientada a Objetos.
- Permite crear los formularios para la Web.
- Biblioteca nativa de funciones sumamente amplia e incluida.
- No requiere definición de tipos de variables ni manejo detallado del bajo nivel.

En la tabla 6.3 mostramos un resumen de la historia de PHP así como su evolución en cada versión, esto con fin de apreciar las fortalezas y ventajas que ofrece dicho lenguaje de programación.

Versión	Fecha	Cambios más importanes

Versión	Fecha	Cambios más importanes
PHP 1.0	8 de Junio de 1995	Oficialmente llamado "Herramientas personales de trabajo (PHP Tools)". Es el primer uso del nombre "PHP".
PHP Version 2 (PHP/FI)	16 de Abril de 1996	Considerado por el creador como la "más rapida y simple herramienta" para la creación de páginas Webs dinámicas.
PHP 3.0	6 de Junio de 1998	Desarrollo movido de una persona a muchos desarrolladores. Zeev Suraski y Andi Gutmans reescriben la base para esta versión.
PHP 4.0	22 de Mayo de 2000	Se agregan avanzadas de dos etapas analizar/ejecutar la etiqueta-análisis sistema llamado entorno motor Zend.
PHP 4.1	10 de Diciembre de 2001	Introducidas las variables superglobals ($_GET, $_SESSION, etc.)
PHP 4.2	22 de Abril de 2002	Se deshabilitan register_globals por defecto
PHP 4.3	27 de Diciembre de 2002	Introducido la CLI, en adición a la CGI

Versión	Fecha	Cambios más importanes
PHP 4.4	11 de Julio de 2005	Sin cambio.
PHP 5.0	13 de Julio de 2004	Motor Zend II con un nuevo modelo de objetos.
PHP 5.1	25 de Noviembre de 2005	Sin cambio.
PHP 5.2	2 de Noviembre de 2006	Habilitado el filtro de extensiones por defecto

Tabla 6.3 Resumen leguaje de programación PHP.

6.5 Servidor HTTP

Hemos decido utilizar como servidor HTTP Apache 2.0 para levantar los servicios Web de nuestra aplicación, existe un paquete que contiene esta herramienta y algunas otras más. Este paquete es conocido como XAMPP y la versión que estamos utilizamos es la XAMPP para Windows 1.5.4a, que es una distribución Apache que contiene además MySQL, PHP y Perl. XAMPP es sencillo de instalar y usar, basta con descargar el paquete y comenzamos a utilizarlo. No necesita ninguna configuración solamente tener el cuidado de que otra aplicación no ocupe el puerto 8080 que corresponde a http en el servidor.

En la figura 6.2 vemos el panel de control de XAMPP.

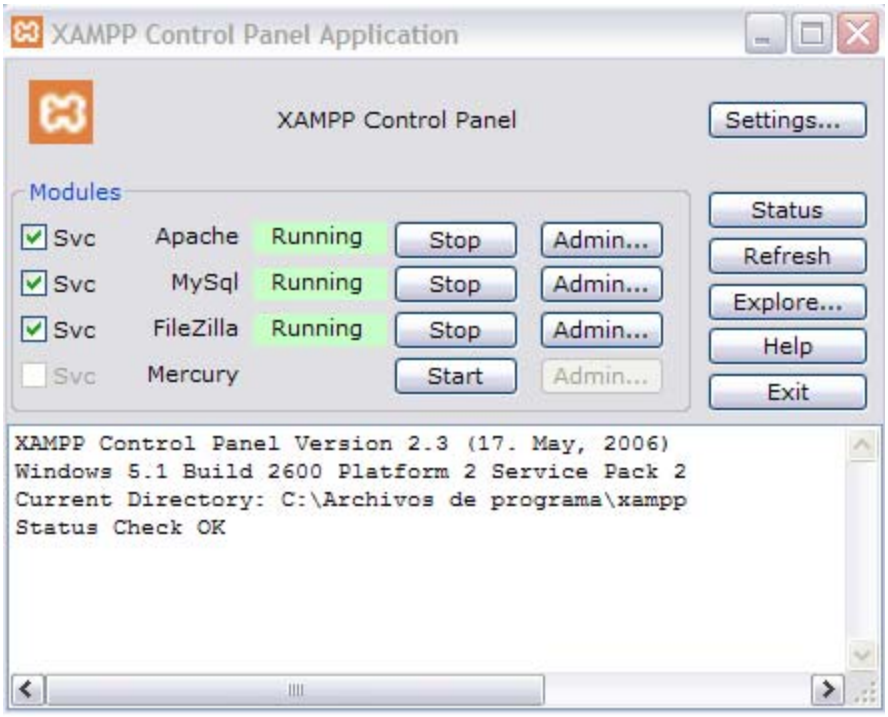


Figura 6.2 Panel de control del paquete XAMPP.

El servidor HTTP Apache es un software libre servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Windows, Macintosh y otras, que implementa el protocolo HTTP y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3 (El NCSA HTTPd era un Servidor Web desarrollado originalmente en el National Center for Supercomputing Applications por Robert McCool y una lista de colaboradores., pero más tarde fue reescrito por completo). Su nombre se debe a que originalmente Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, *a* patchy server (un servidor "parcheado"). El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración, algo que en el paquete XAMPP ya fue solventado. Estamos utilizando Apache 2.0 que es la versión más actualizada de este servidor y entre las mejoras tenemos:

Cambios en el proceso de configuración y compilación.

- Apache usa ahora autoconf y libtool en el proceso de compilación. Este sistema es parecido aunque no igual al sistema APACI de Apache 1.3.
- Además de la selección de módulos habitual que puede hacer al compilar, en Apache 2.0 la mayor parte del procesamiento de las peticiones son llevadas a cabo por módulos de multiprocesamiento (MPMs).

Cambios en el proceso de configuración inicial del servidor.

- Muchas directivas que pertenecían al núcleo del servidor en Apache 1.3 se encuentran ahora en distintos módulos de multiprocesamiento. Si desea que el nuevo servidor de comporte de la forma más parecida posible a como lo hacía Apache 1.3, debe usar el módulo de multiprocesamiento prefork. Otros módulos de multiprocesamiento tienen diferentes directivas para controlar la creación de procesos y el procesamiento de peticiones.
- El módulo proxy ha sido remodelado para ponerlo al día con la especificación HTTP/1.1. Entre los cambios más importantes está el que ahora el control de acceso al proxy está dentro de un bloque <Proxy> en lugar de en un bloque <Directory proxy:>.
- El procesamiento de PATH_INFO (la información que aparece detrás de un nombre de archivo válido) ha cambiado en algunos módulos. Los módulos que fueron previamente implementados como un manejador pero que ahora son implementados como un filtro puede que no acepten peticiones que incluyan PATH_INFO. Filtros como INCLUDES o PHP están implementados sobre el manejador principal, y por tanto rechazarán peticiones con PATH_INFO. Puede usar la directiva AcceptPathInfo para forzar al manejador principal a aceptar peticiones con PATH_INFO y por tanto restaurar la posibilidad de usar PATH_INFO en cualquier lado del servidor.
- Otro uso de la directiva Port en Apache 1.3 era fijar el número de puerto que se usaba para URLs autoreferenciadas. La directiva equivalente en Apache 2.0 es la nueva directiva ServerName, este cambio se ha introducido para permitir la especificación del nombre de servidor y del número de puerto para URLs autorreferenciadas en una sola directiva.
- La directiva ServerType ha dejado de existir. El método usado para servir peticiones está ahora determinado por la selección del módulo de multiprocesamiento. Actualmente no hay diseñado un módulo de multiprocesamiento que pueda ser ejecutado por inetd.
- Los módulos mod_log_agent y mod_log_referer que contenían las directivas AgentLog, RefererLog y RefererIgnore han desaparecido. Los registros de "agente" y de "referir" están disponibles todavía usando la directiva CustomLog del módulo mod_log_config.
- Las directivas AddModule y ClearModuleList no están presentes en la nueva versión de Apache. Estas directivas se usaban para asegurar que los módulos pudieran activarse en el orden correcto. La nueva API de Apache 2.0 permite a los módulos especificar explícitamente su orden de activación, eliminando la necesidad de las antiguas directivas.
- La directiva FancyIndexing se ha eliminado. La funcionalidad que cubría está ahora disponible a través de la opción FancyIndexing de la directiva IndexOptions.
- La técnica de negociación de contenido MultiViews ofrecida por mod_negotiation es ahora más estricta en su algoritmo de selección de archivos y solo seleccionará archivos negociables. El antiguo comportamiento puede restaurarse usando la directiva MultiviewsMatch.

6.6 Interfaz de la aplicación

Parte importante de la seguridad del sistema es la validación y permisos que tiene un usuario ya que esta es la llave de entrada a la aplicación. En la figura 6.3 describimos el proceso de validación de usuario que hemos utilizado en la aplicación.

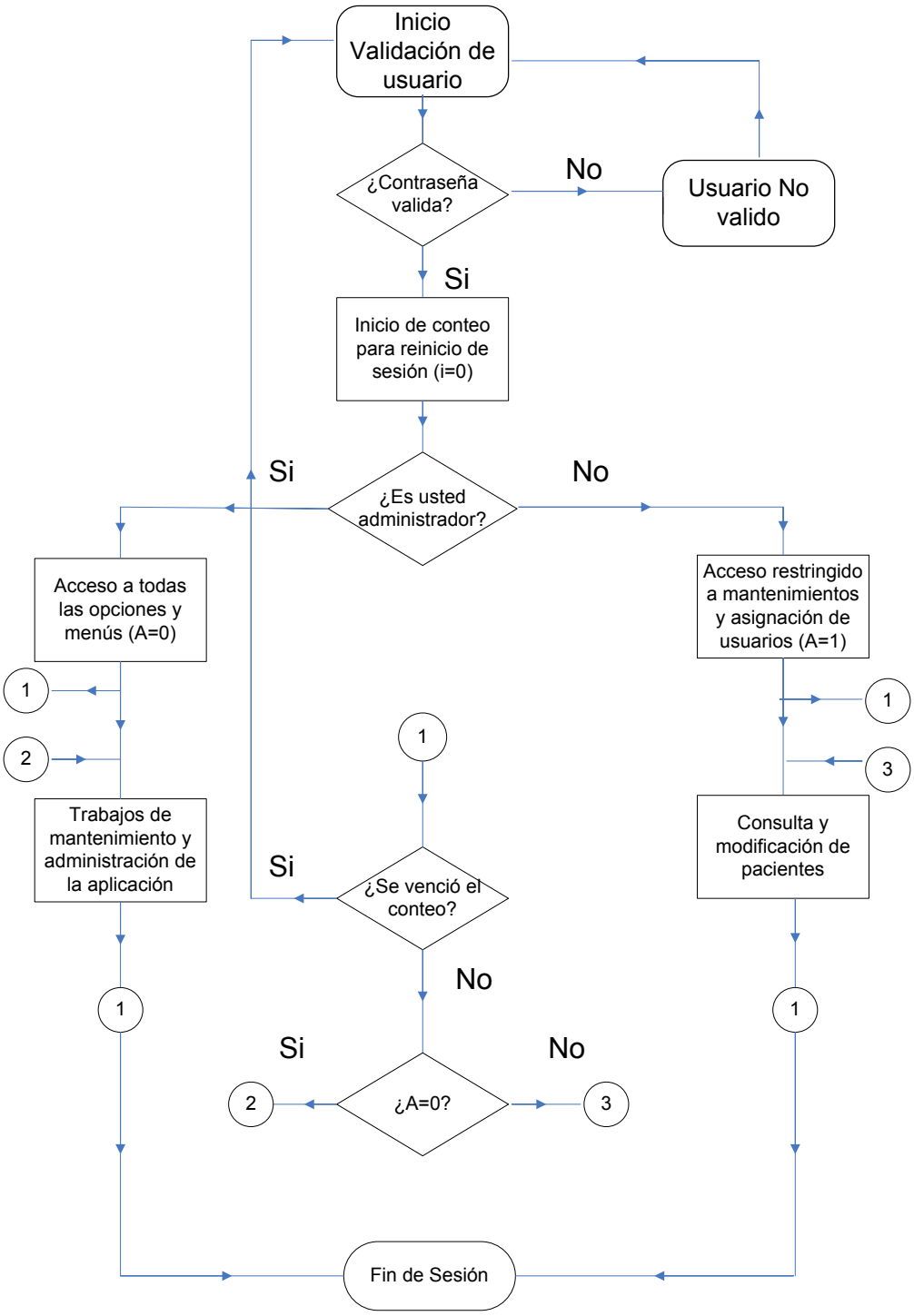


Figura 6.3 Flujo de registro y validación del usuario mediante contraseña.

Como primer paso el médico ingresa su usuario y contraseña proporcionado con anterioridad por el administrador del sistema, la aplicación entra en una condición en donde se evalúa si es administrador o es médico, dependiendo de su perfil así será su nivel de acceso y diferentes opciones a las que puede tener acceso. Si la contraseña no

es válida (no esta ingresada en las bases de datos por el administrador del sistema mediante el mantenimiento del sistema) no lo deja pasar de ese punto.

Al iniciar la sesión se ha programado un contador que le cede cierto tiempo al usuario para realizar la operación que tiene pensada hacer antes de volverse a validar, esto en el caso que un médico deje la PDA al alcance de otra persona, por ejemplo después de 2 minutos le pedirá nuevamente su usuario y contraseña para seguir realizando mas operaciones en el sistema. El administrador tendrá derecho a todas las opciones del sistema desde las de consulta, hasta la administración y mantenimiento de nuevos usuarios. Por lo que la responsabilidad de éste es grande.

6.6.1 Aplicación

En la figura 6.4 se puede apreciar la pantalla inicial del sistema en donde se nos pide el usuario y contraseña que será administrado y proporcionado a cada médico por un encargado de la aplicación.

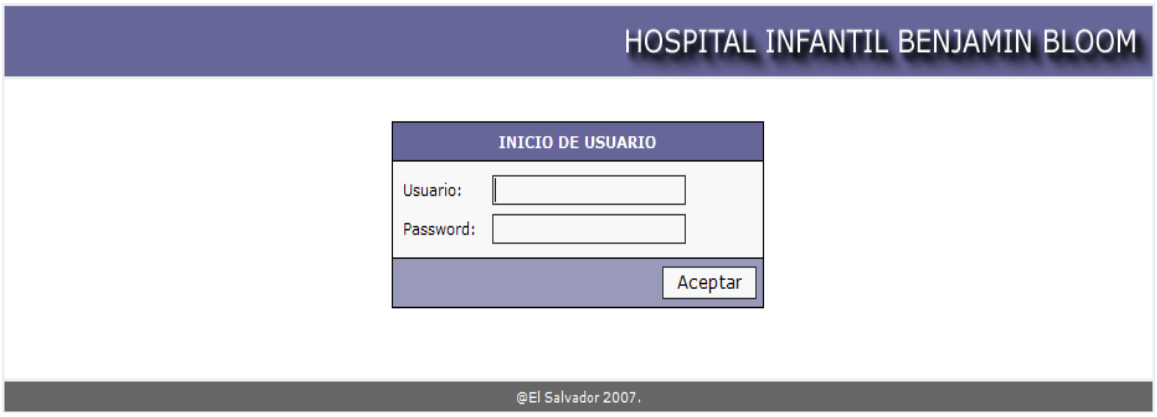


Figura 6.4 Pantalla inicial del sistema.

En la figura 6.5 apreciamos la pantalla para la introducción de un nuevo usuario, a esta configuración solo tendrá acceso el administrador. Los datos que se llenan son usuario y su correspondiente contraseña además de su perfil, los cuales pueden ser dos como administrador o como médico.

Figura 6.5 Pantalla de ingreso de nuevo usuario.

Esta opción esta descrita en la figura 6.6 dependiendo del perfil del usuario así serán sus privilegios dentro de la aplicación

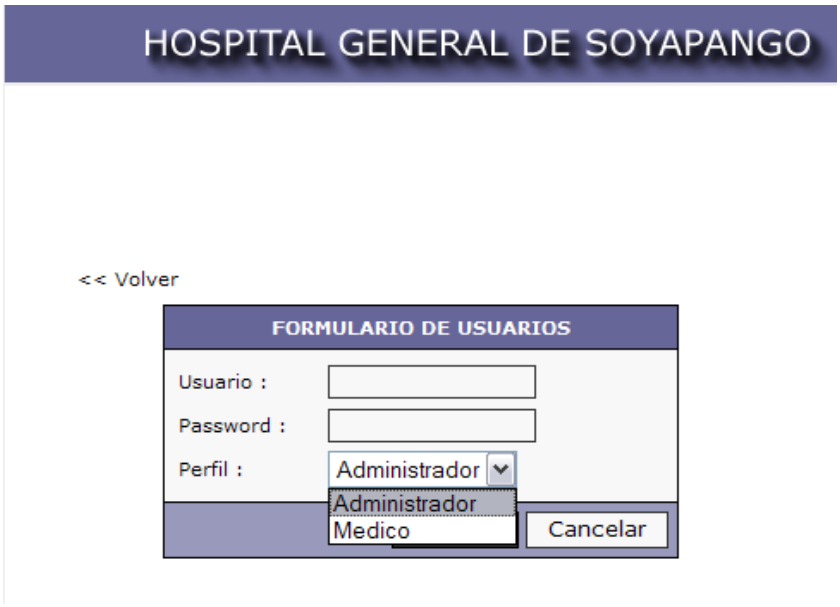


Figura 6.6 Pantalla de privilegio de usuario.

A continuación en la figura 6.7 mostramos todos los accesos y movimientos que se pueden hacer mediante la aplicación como administrador. Podemos tener acceso a configuración de pacientes, usuarios, agregar médicos, agregar nuevas opciones en la casilla parentesco, en fin mantenimientos a otros criterios que constituyen la información de un paciente como el área de la que provienen, municipio, departamento, país.

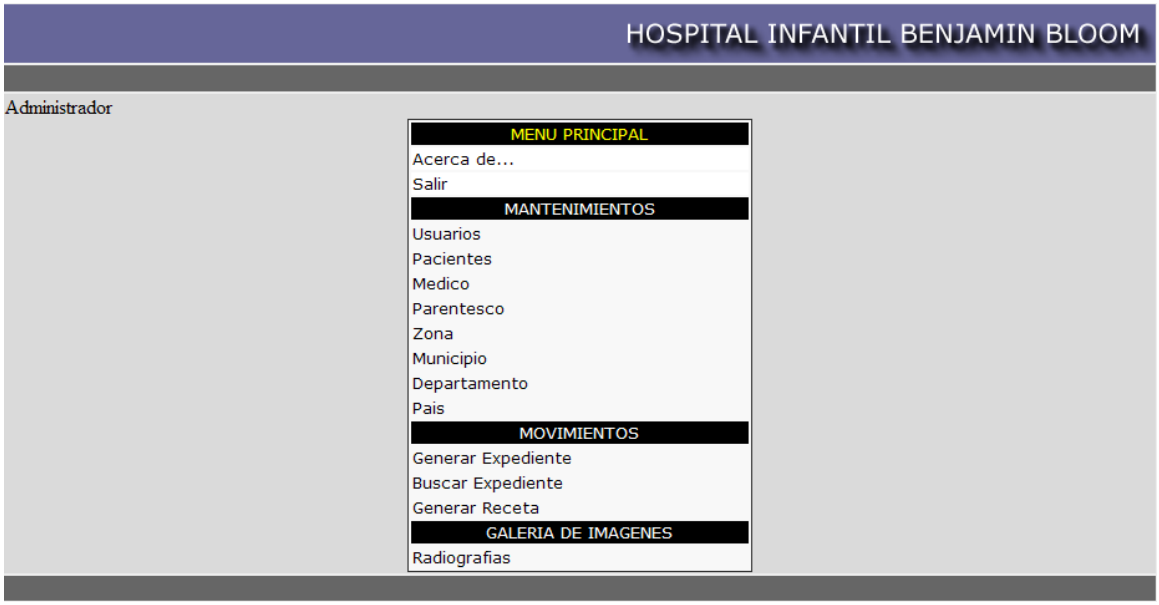


Figura 6.7 Mantenimiento de los servicios de la aplicación.

En la figura 6.8 tenemos las opciones a las que un médico puede acceder como lo son la generación y consulta de un expediente y la generación de una receta, no tiene acceso a ninguna opción de configuración.

Figura 6.8 Opciones del perfil de un médico.

En la figura 6.9 tenemos el formulario de la información general de un paciente para ser ingresada en las bases de datos, pantalla que será utilizada principalmente por el médico.

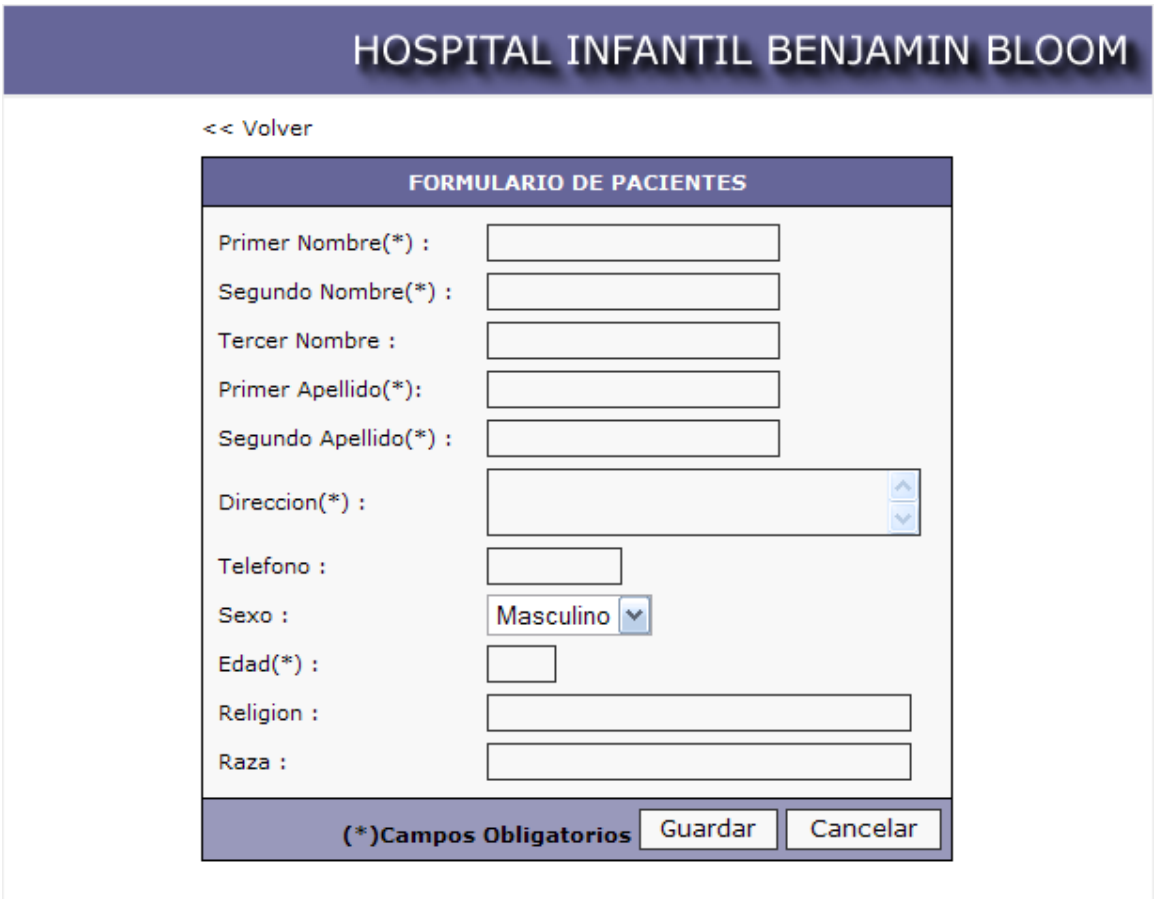


Figura 6.9 Formulario de ingreso de información general de un paciente.

A continuación tenemos la pantalla de confirmación de ingreso de un registro en la figura 6.10.

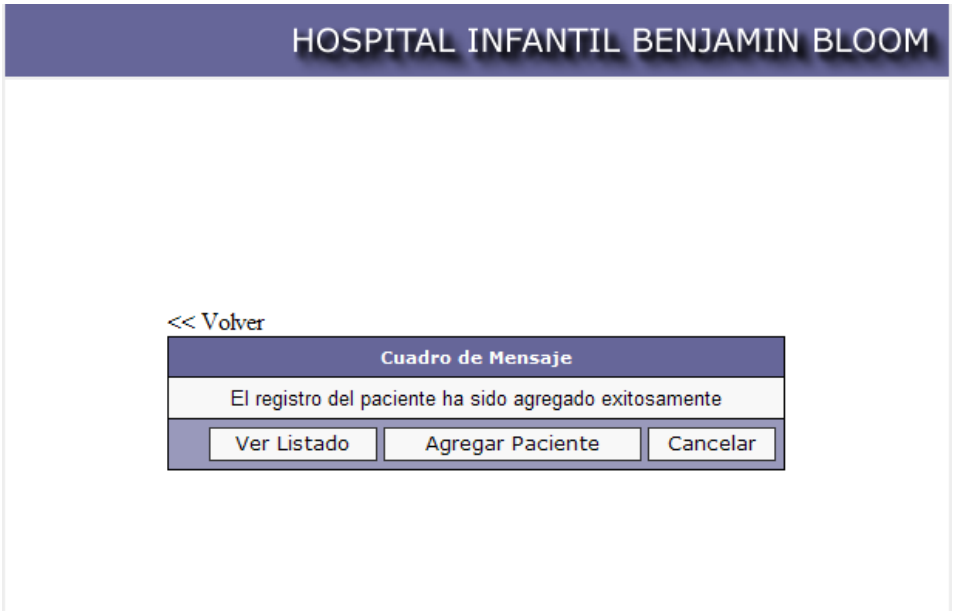


Figura 6.10 Confirmación del ingreso de un registro.

En la figura 6.11 vemos una lista de los usuarios creados por el administrador de la aplicación junto a su perfil.

Figura 6.11 Lista de todos los usuarios creados en la aplicación.

Se tendrá la necesidad de buscar la información general de un expediente de algún paciente de forma rápida y eficiente o algún usuario, por lo que la aplicación consta de una hoja de búsqueda por nombre, ella nos permite recopilar la información general de un paciente o usuario y tener acceso ya sea a modificarla o crear nueva información.

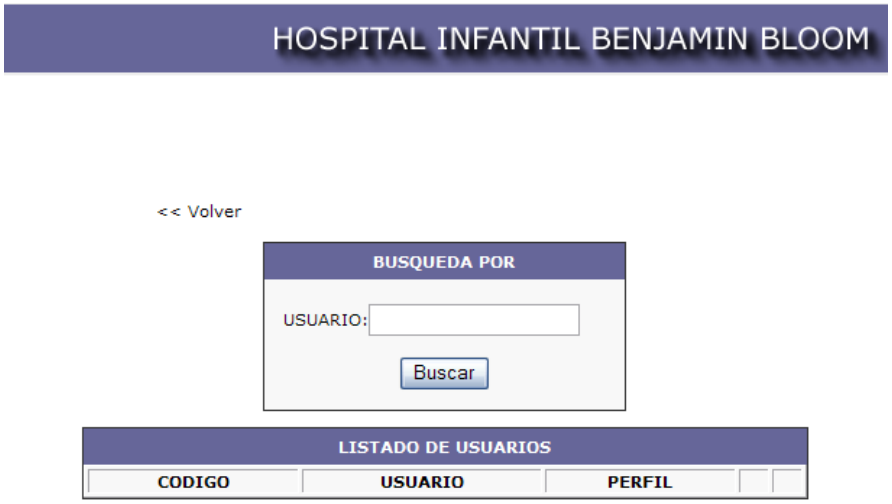


Figura 6.12 Búsqueda de un registro

La información a la que tenemos acceso mediante la búsqueda que realizamos es la que nos muestra la figura 6.13 como vemos es información general que muchas veces no se tiene acceso de manera tan rápida.

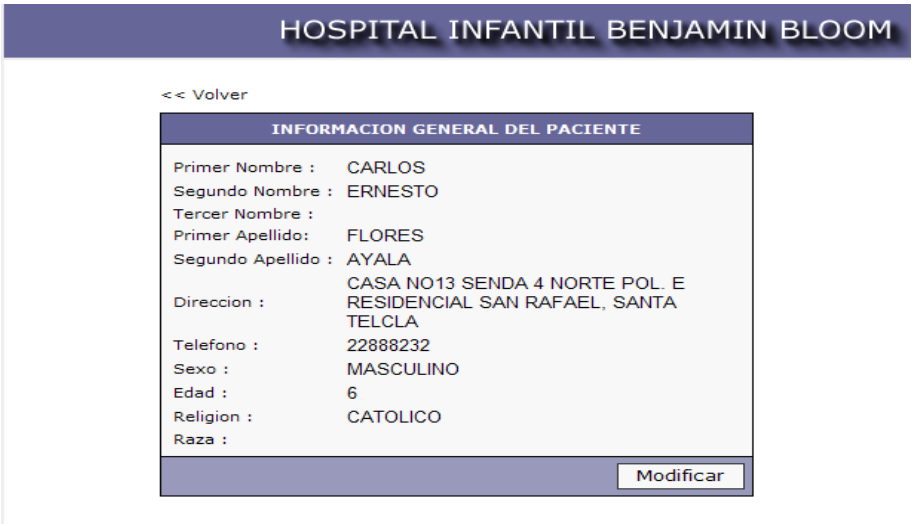


Figura 6.13 Detalle de la información general de un paciente.

En la figura 6.13 tenemos la generación del expediente del paciente

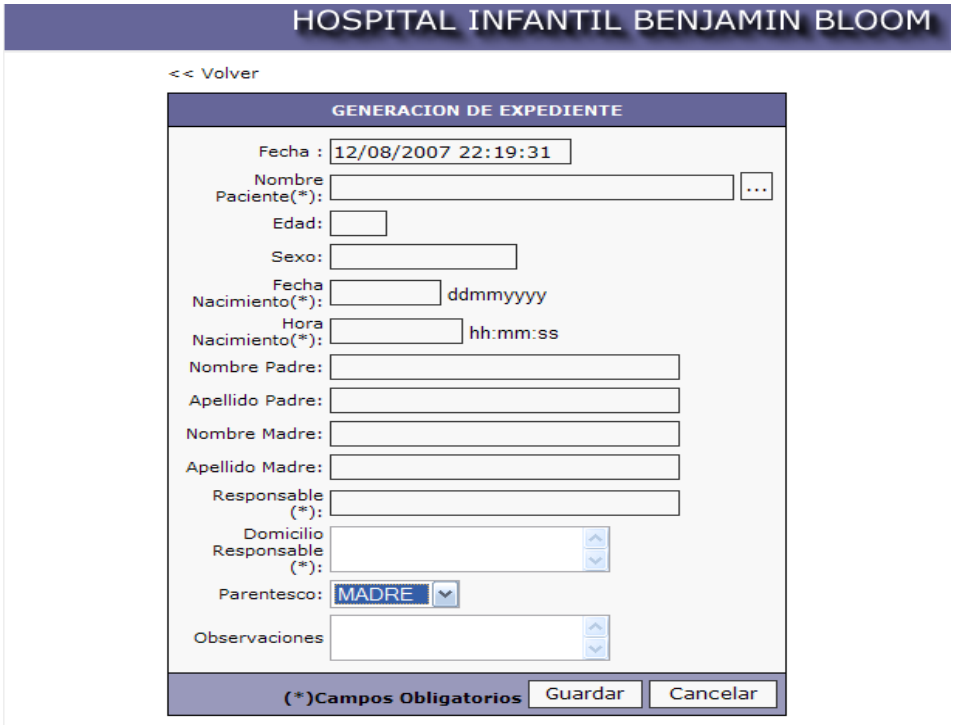


Figura 6.12 Generación de Expediente.

Como pudimos apreciar la aplicación busca ser lo más amigable y sencilla posible ya que en las PDA es importante que la visualización sea óptima y la carga se realice rápidamente, ese fue uno de los criterios que utilizamos a la hora de diseñar la aplicación.

6.7 Bases de datos

Una base de datos o banco de datos es un conjunto de datos que pertenecen al mismo contexto, almacenados sistemáticamente para su posterior uso. En informática existen los SGBD (sistemas gestores de bases de datos), que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada. Las aplicaciones más usuales son para la gestión de información en empresas e instituciones públicas. También son ampliamente utilizadas en entornos científicos con el objeto de almacenar la información experimental. Aunque las bases de datos pueden contener muchos tipos de datos, algunos de ellos se encuentran protegidos por las leyes locales, esto depende del país en donde se encuentre.

6.7.1 Diseño de la base de datos.

A continuación explicamos el diseño de la base de datos simulada, que utilizamos específicamente para nuestra aplicación y que tiene como fin la demostración del sistema solamente, y no para el uso en algún centro hospitalario, aunque fue basada en las visitas que realizamos al Hospital de niños Benjamín Bloom, atacando dos problemas como explicamos en el diagrama de flujo de datos del capitulo 6.2.1 Modelado del proceso flujo de la información, los cuales son la atención de un paciente y la generación de una receta en el área de emergencias, todo esto dentro de las limitantes de nuestro proyecto debido a que son bases de datos simuladas.

En la figura 6.16 tenemos el diagrama completo de la base de datos que diseñamos en ella están tomadas en cuenta las tablas con la información necesaria para configurar, darle mantenimiento y uso a las necesidades básicas que hemos planteado para la solución de los problemas planteados anteriormente.

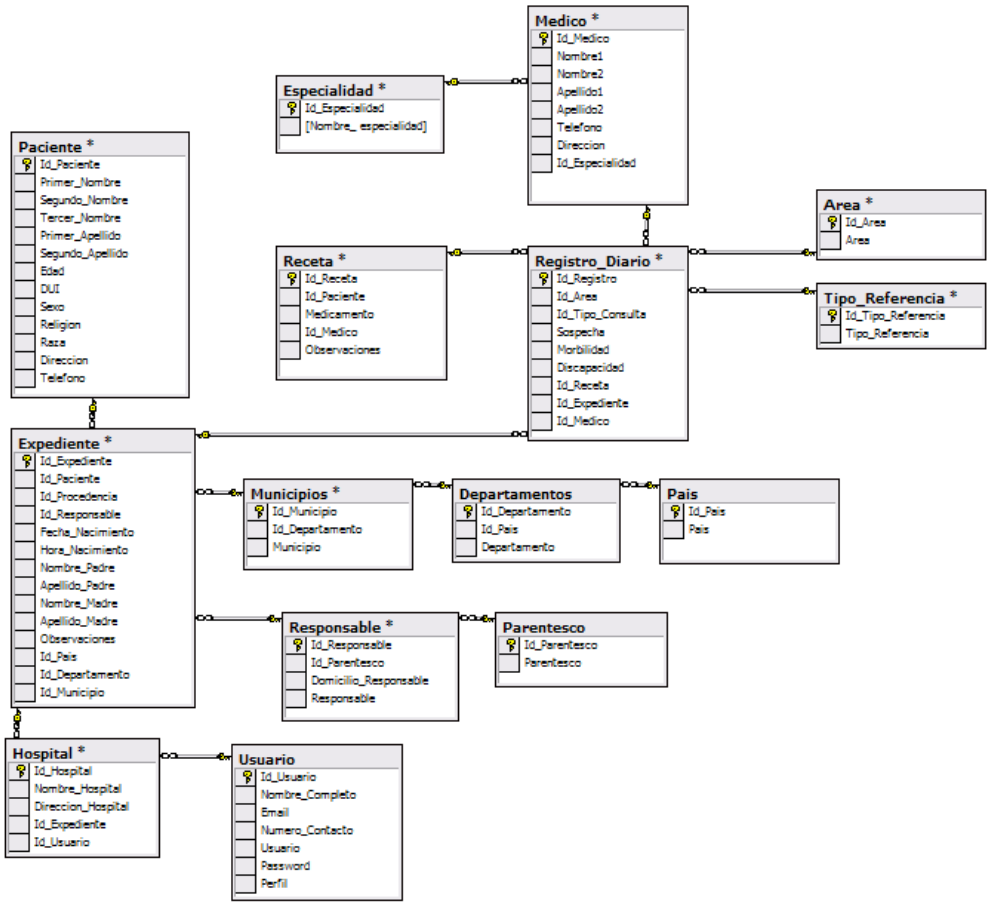


Figura 6.16 Diagrama de relación de tablas.

Vamos a dividir el diagrama en diferentes bloques para facilitar su explicación. En la figura 6.17 tenemos el bloque de tablas que relaciona al registro diario, el cual tiene varias llaves foráneas de otras tablas. En el registro diario es necesario que tengamos la información del médico que realizó la consulta así como también la especialidad de éste. También para controles estadísticos es necesario saber que tipo de referencia tiene y el área de la cual proviene el paciente. La receta también esta asociada al registro del paciente por que es necesario saber cual fue el último medicamento que se le receto y la evolución que ha tenido el paciente.

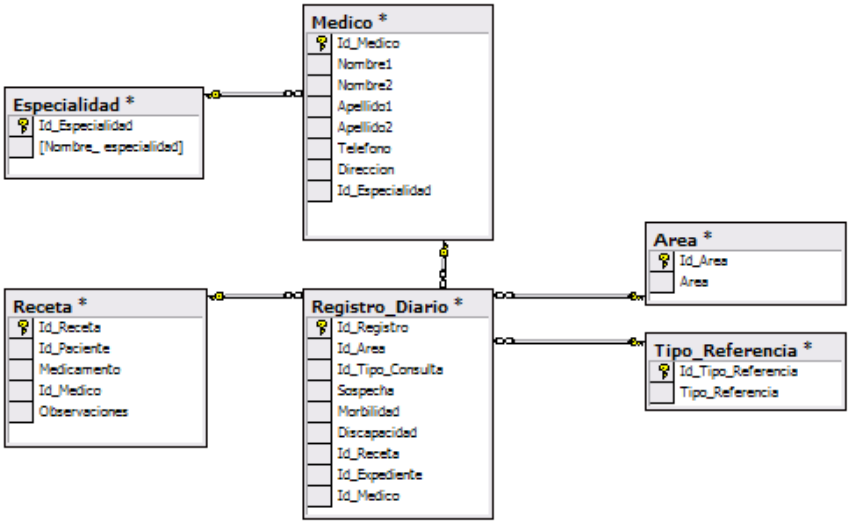


Figura 6.17 Relación tablas Paciente – Medico – Receta.

Como vemos en la figura 6.18 se esta asociando la información básica del paciente con su respectivo expediente el cual hará las veces de su historial médico. (En la tabla Paciente se dejo el campo DUI a pesar de que la aplicación fue basada en un hospital de niños esto para tener una base de datos más genérica).

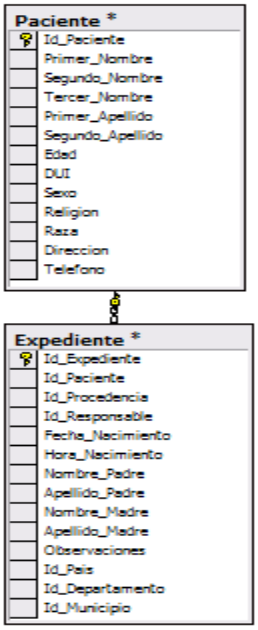


Figura 6.18 Relación tablas Paciente – Expediente.

El expediente esta formado de información general además de información de origen y responsables del paciente. En la figura 6.19 tenemos información propia del expediente

las cuales son municipios, departamentos, país, responsables y parentesco, que servirán par tener una información más amplia y que no esta contenida en la tabla paciente.

Para fines de estadística se lleva también un control rápido de los ingresos y referencias de pacientes en el hospital. Esta información sirve para luego sacar estadísticas que brinden a las autoridades de salud una idea de la situación en la que se encuentra la población. Vemos la relación existente de la tabla Registro_diario de la figura 6.19 que además de tener relación con las tablas Area y Tipo_Referencia, también tiene relación con la tabla Expediente.

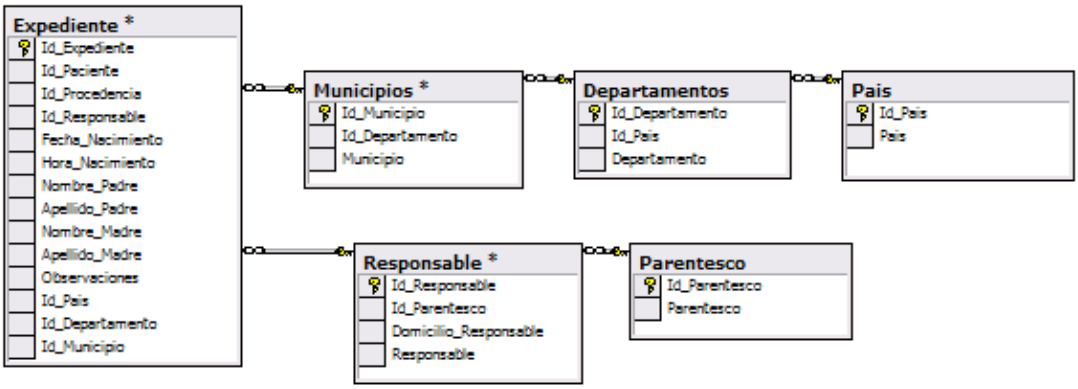


Figura 6.19 Relación Expediente – Responsable – Parentesco.

Tenemos en la figura 6.20 la relación existente entre el expediente y el hospital, donde la llave foránea en la tabla hospital es el Id_Expediente para tener un control del origen hospitalario del expediente.

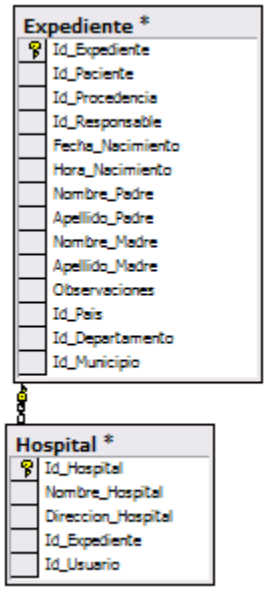


Figura 6.20 Relación tablas Expediente - Procedencia - País - Departamentos - Municipios.

En la figura anterior vemos la asociación del usuario al hospital que pertenece.La tabla usuario que nos muestra la figura 6.21 tiene los campos Id_Usuario que es un índice que lo otorga el sistema de forma automática, Usuario que es el nombre de éste, el respectivo password y su perfil.

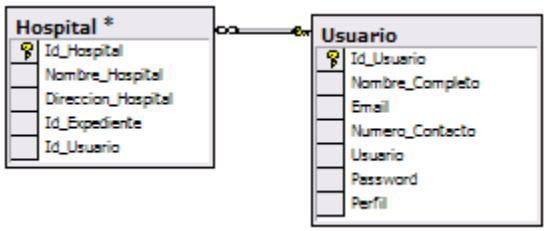


Figura 6.21 Relación tablas Registro_Diario – Area – Tipo_Referencia.

6.8 Protocolos de seguridad

6.8.1 Seguridad interfaz aire

6.8.1.1 WPE

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo de seguridad que brinda protección a las redes inalámbricas. Este protocolo esta incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El protocolo WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas como lo muestra la figura 6.23. En ningún caso es compatible con IPSec (Internet Protocolo Security)

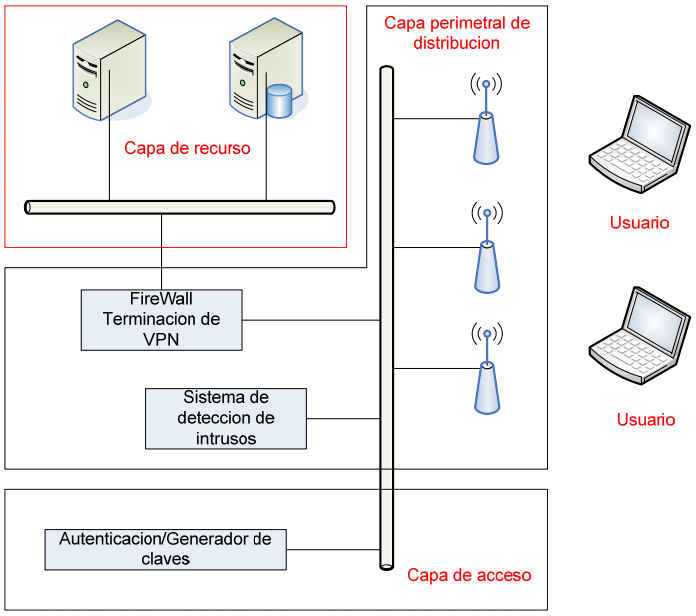


Figura 6.23 Protocolo WEP.

El estándar IEEE 802.11 proporciona procesos de autenticación y cifrado para fortalecer la seguridad de la comunicación, en tal sentido existen diferentes protocolos de seguridad. En el modo de red Ad Hoc, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

El estándar 802.11 especifica una capacidad opcional de cifrado denominada WEP, su intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 (Rivest Cipher 4 ARC4 es el sistema de cifrado de flujo Stream cipher) de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire. Aunque los sistemas WLAN pueden resistir los ataques ilegales pasivos, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP. WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado. Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo HASH (comprobación de integridad) (CRC-32, cyclic redundancy check) al texto en claro, lo que genera un valor ICV (comprobación de integridad). Dicho valor de comprobación de integridad se concatena con el texto en claro. El ICV es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

WEP proporciona dos tipos de autenticación:

- Un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN.
- Una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red.

De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (challenge). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red. La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

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

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

Para el cálculo del algoritmo de encriptación WEP se realiza los siguientes pasos:

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

6.8.1.2 WPA

WPA (Wi-Fi Protected Access) emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

- Para el uso personal doméstico: El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.
- Para el uso en empresarial/de negocios: El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP. AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica.

WPA utiliza la autentificación 802.1X con uno de los tipos extensibles del protocolo de la autentificación (EAP) disponibles hoy. 802.1X es un método de control puerto-basado de acceso de red cableada así como la red inalámbrica. Él fue adoptado como a estándar por el IEEE en agosto de 2001. Consiste en una autenticación a servidores donde se

establece la autenticad del cliente por medio de certificados extendidos previamente por los servidores.

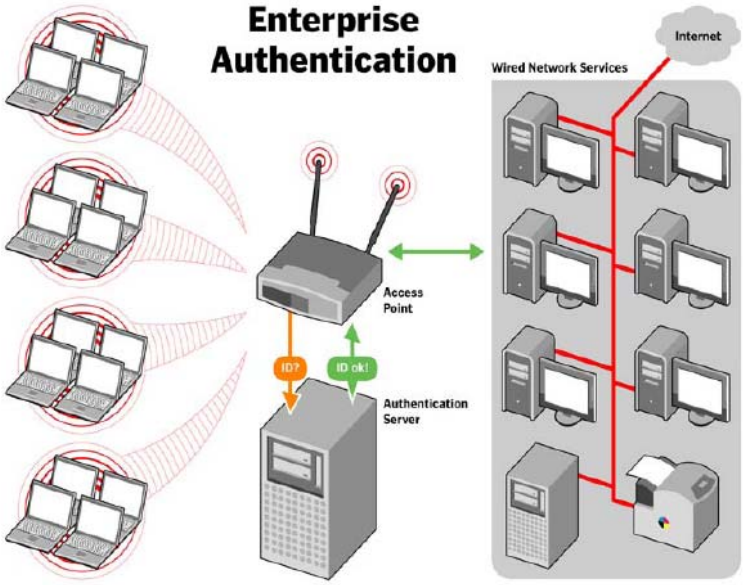


Figura 6.24 Protocolo WAP.

En la tabla 6.8 mostramos una breve comparación de los métodos de encriptación.

	WEP	WPA	WPA 2
Algotitmo de cifrado	**RC4**	**RC4**	**AES**
Longitud de clave	40 bits	128 bits de encriptación 64 bits de autenticación	128 bits
Tiempo de validez	24 bits IV	48 bits IV	48 bits IV
Paquete de clave	Concatenado	Función mixta	No necesita
Integridad de dato	CRC-32	Michael	CCM
Encabezado de dato	Ninguno	Michael	CCM
Contra ataque	Ninguno	Secuencia IV	Secuencia IV
Administración de clave	Ninguno	Basado en EAP	Basado en EAP

Tabla 6.8 Comparación de los protocolos de encriptación.

6.8.2 Seguridad por software.

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debemos de dotar de cuatro características al mismo:

- Integridad: la información no puede ser modificada por quien no está autorizado.
- Confidencialidad: la información solo debe ser legible para los autorizados.
- Disponibilidad: debe estar disponible cuando se necesita.
- Irrefutabilidad: (No-Rechazo o No Repudio) que no se pueda negar la autoría.

Dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad lógica y seguridad física. Es importante conocer algunos términos que nos darán una mejor idea de la seguridad lógica.

- Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- Amenaza: es un evento que pueden desencadenar un incidente en la plataforma o sistema que se este atacando.
- Impacto: consecuencia de la materialización de una amenaza.
- Riesgo: posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.
- Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
- Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un Impacto.

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

- Información: Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.
- Equipos que la soportan: Software, hardware y organización.
- Usuarios: Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Los objetivos para conseguirlo son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los usuarios puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

6.8.2.1 Políticas de Seguridad

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los usuarios tienen sólo los permisos que se les dio. La seguridad informática debe ser estudiada para que no impida el trabajo de los usuarios en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.
- Sensibilizar a los usuarios con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los usuarios deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad.

6.8.2.2 Amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- Un usuario: causa del mayor problema ligado a la seguridad de un sistema informático (por que no le importa, no se da cuenta o a propósito).
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en la computadora abriendo una puerta a intrusos o bien modificando los datos. Estos

programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

- Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.).
- Un siniestro (robo, incendio, por agua): una mala manipulación o una malintención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas: las disputas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

6.8.2.3 Técnicas de seguridad del sistema

A continuación se enuncian algunas técnicas para el aseguramiento del sistema:

- Codificar la información: Criptología (La criptología es el estudio de los criptosistemas: sistemas que ofrecen medios seguros de comunicación en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo), Criptografía (Del griego kryptos (ocultar) y grafos (escribir), literalmente escritura oculta, la criptografía es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos), contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red.
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - anti-spyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

6.8.2.4 Consideraciones de software.

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software pirata o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia. Existe software que es famoso por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades pero permitiendo una seguridad extra.

6.8.2.5 Consideraciones de una red.

Los puntos de entrada en la red son generalmente el correo, las páginas Web y los archivos desde discos, o de computadoras ajenas, como portátiles. Mantener al máximo el número de recursos de red en sólo en modo lectura impide que usuarios infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo. Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas. Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

6.9 Hardware

6.9.1 PDA

En consecuencia a la aplicación y al protocolo de acceso inalámbrico a usar, mostramos a continuación la tabla 6.9 resumen con modelos de PDA's mas comerciales en el mercado mundial.

Características	PALM			Pockect PC		
Modelo	**Tugsten**	**TX**	**Lifedrive**	**HP IPAQ HX 2190**	**HP IPAQ RW 1950**	**DELL AXIM X51**
Puerto USB para sincronización	Si	Si	Si	Si	Si	Si
Infrarrojo	Si	Si	Si	Si	Si	No
Bluetooth	Si	Si	Si	Si	Si	Si
Wi-Fi (802.11 b/g)	No	Si	Si	Si	Si	Si
Procesador	200 MHz	312 MHz	433 MHz	312 MHz	416 MHz	624 MHz
Memoria expandible	Tarjeta SD	Tarjeta SD	Tarjeta SD	Tarjeta SD	Tarjeta SD	Tarjeta SD
Memoria interna	30 ROM/32 RAM	128 MB	256 MB	128 MB	192 MB	256 MB
Precio	Entre $200 y $250	Entre $300 y $450	Entre $500 y $600	Entre $300 y $400	Entre $600 y $700	Entre $500 y $650

Tabla 6.9 Comparación de equipo terminal.

En base a la tabla anterior decidimos utilizar los modelos PALM TX y Pockect PC HP IPAQ RX1950 debido lo siguiente:

- Cumplen las especificaciones mínimas de hardware para la aplicación (procesador de 320 MHz, ROM de 32 Mb, RAM de 64 Mb, Acceso inalámbrico Wi- Fi).
- Cumplen las especificaciones mínimas de software (OS PALM, Windows Mobile, navegador Web).
- Por el precio.
- Por ser dos modelos altamente comerciales.

Las prestaciones de compatibilidad de los sistemas operativos para PDA's seleccionadas anteriormente con algunos lenguajes de programación son las mostradas a continuación en la tabla 6.10:

Compatibilidad Software/Sistema operativo		
Lenguaje de programación	**PALM OS**	**Pocket PC Windows Mobile**
C++	No	Si
Visual Basic	No	Si
Palm Development	Si	No
HTML	Si	Si
PHP	Si	Si

Tabla 6.10 Compatibilidad con lenguajes de programación.

A continuación describimos las características más importantes de los modelos seleccionados:

PALM TX

Figura 6.25 PALM TX[34].

1. Encendido/Apagado.
2. Lápiz Stylus.
3. Conector de Auriculares.
4. Puerto Infrarrojo.
5. Ranura de Expansión.
6. Multiconector.
7. Pantalla TFT de 320x480 píxeles de resolución.
8. Página inicial/Favoritos.
9. Calendario.
10. Navegador de 5 vías.
11. Contactos.
12. Navegador.
13. Barra de estado.

[34] http://www.palm.com/cl/handhelds/TX/specs.html

14. Parlante traseros.

Especificaciones Técnicas:

- Sistema operativo: Palm OS Garnet 5.4
- Memoria: 128MB con 100MB disponible para el usuario (interna).
- Procesador: procesador Intel 312 MHz basado en ARM.
- Pantalla: Pantalla TFT transflectiva a color de 320 x 480. Soporta más de 65,000 colores, orientación modo vertical y horizontal.
- Tecnología inalámbrica: Wi-Fi 802.11b, tecnología inalámbrica Bluetooth 1.1.
- Audio: Parlante
- Conector de auriculares estéreo de 3.5mm estándar.
- Ranura de expansión: Soporta tarjetas MultiMediaCard, SD y SDIO.
- Batería: De Lítio ion recargable de larga vida.
- Power / synC: Multiconector en el dispositivo.Cable de sincronización USB
- Adaptador de AC (108-32 VAC/60Hz)
- Tamaño: 78.2mm A x 120.9mm H x 15.5mm P
- Peso: 5.25 onzas, 148.83 gramos.

Navegador: Blazer 4.3, Características:

- Opciones de visualización: la visualización optimizada minimiza el desplazamiento horizontal y hace que el contenido se adapte a la pantalla. La visualización a pantalla completa proporciona la interfaz familiar de un navegador Web de PC.
- Visualización de la página a pantalla completa: la visualización de las páginas Web en modo horizontal en la computadora de mano Palm T|X mejora aún más tu experiencia de navegación por la Web.
- Guarda imágenes: pulsando y manteniendo la presión sobre cualquier imagen de una página Web podemos guardarla en la memoria interna de la PDA o en una memoria de expansión SD.

Incluye soporte para estándares Web. Cumple con los siguientes estándares de Internet: HTML 4.01, xHTML 1.0, cHTML, WML 1.3, SSL 3.0, HTTP 1.1, JavaScript 1.5, CSS 1.0 y 2.0 (parcial), GIF, GIF animado, JPEG, PNG, BMP y Cookies.

HP IPAQ RX1950

Figura 6.26 HP IPAQ RX1950[35].

Características:

- Sistema operativo: Microsoft Windows Mobile 5.0, con el software Microsoft Office actualizado mejora la productividad con una gestión de datos más eficaz.
- Memoria: Hasta 96 MB de memoria total (64 MB de ROM y 32 MB de SDRAM) y hasta 33 MB de memoria disponible para el usuario que incluye almacenamiento continúo. La ranura SDIO proporciona más almacenamiento y expansión, incluyendo tecnología como la de las cámaras, tarjetas Bluetooth y escáner.
- Procesador: Samsung® SC32442, 300 MHz.
- Tecnología inalámbrica: Wi-Fi (802.11b) integrada para acceso inalámbrico de alta velocidad a Internet y al correo electrónico.
- Peso: 125 g.
- Pantalla: En color TFT QVGA transflectiva de 3.5 pulgadas y 64.000 colores.
- Tamaño: 113.6 mm x 70.6 mm x 13.5 mm.
- Audio interno: Micrófono, altavoz y un conector de 3.5 mm para auriculares estéreo integrados.
- Internet Explorer Mobile.

Con la mayoría de características del Explorer común como por ejemplo:

- Ver historial de páginas visitadas.
- Agregar links a favoritos.
- Descargar y salvar archivos de Internet.
- Ajustar las páginas Web al tamaño de la pda.
- Visualizar imágenes a pantalla completa.

35

6.10 Modelado del sistema de red.

En la figura 6.27 se muestra el modelado del diagrama lógico de red para la aplicación.

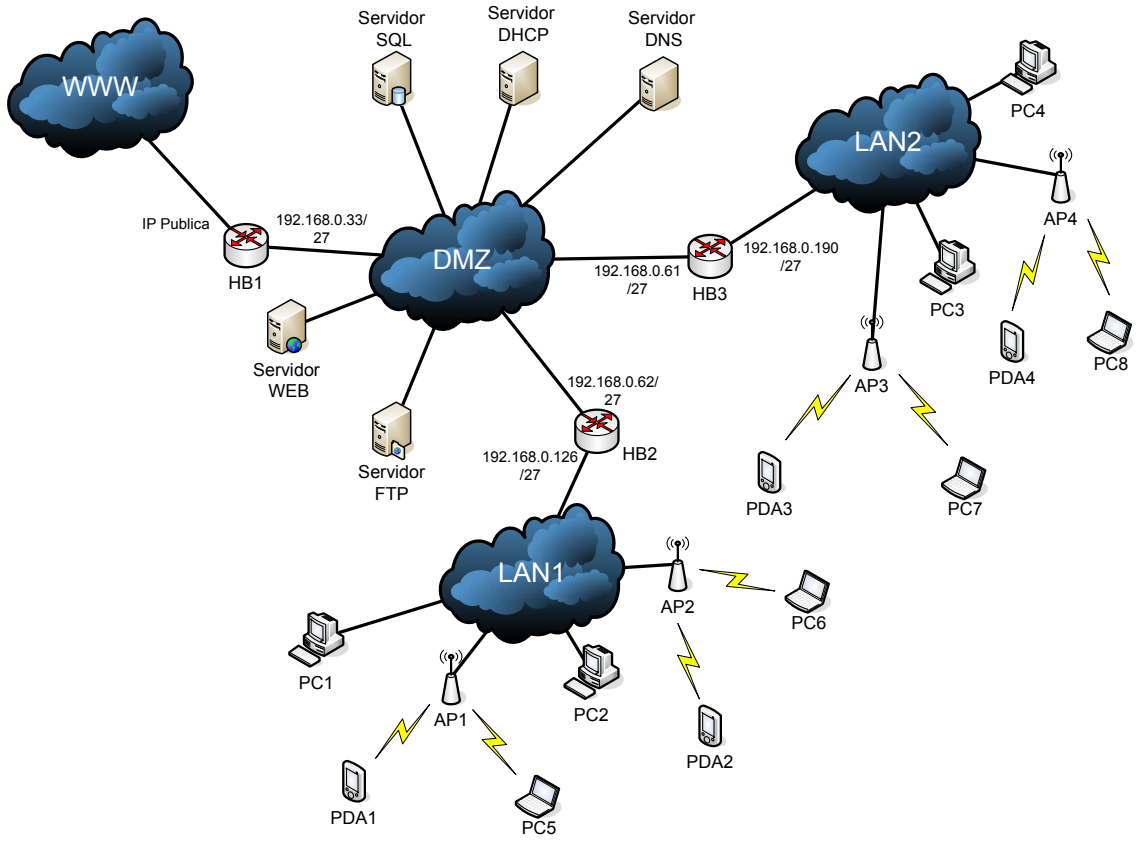


Figura 6.27 Modelado del sistema de red.

En la tabla 6.11 se muestra el subneteo que se genero para el modelado de la red.

Redes	Direccion de red	Direccion de broadcast
DMZ	192.168.0.0	192.168.0.31
LAN1	192.168.0.32	192.168.0.63
Wireless1	192.168.0.64	192.168.0.91
LAN2	192.168.0.92	192.168.0.127
Wireless2	192.168.0.128	192.168.0.159
LAN3	192.168.0.160	192.168.0.191
Wireless3	192.168.0.192	192.168.0.223

Tabla 6.11 Subneteo del sistema de red.

Para poder desarrollar el modelado de la red nos basamos en el modelo OSI. De esta manera describimos el modelado desde la capa 1 hasta la capa 3 de dicho modelo como a continuación se muestra.

6.10.1 Capa física

Dentro de los requerimientos mínimos (protocolos, seguridad, firewall, sistema operativo, interfaces, et.) que se necesitan para proponer la implementación de un router dentro de la red tenemos:

	Caracteristicas	Cisco 2600	Allied Telesyn AR 410	3Com 5600
Protocolos	enrutamiento	OSPF RIP RIP2 IGRP EIGRP	OSFP RIP V1/V2	OSFP RIP V1/V2
	snmp	ok	ok	ok
	Vlan´s	ok	ok	ok
	Trunking Vlan´s	propietario	estándar	estándar
	dhcp	ok	ok	ok
	NAT	ok	ok	ok
	PAT	ok	ok	ok
	QoS	ok	con licencia	ok
	VPN	ok	con licencia	con tarjeta extra
	VoIP	ok	ok	ok
Seguridad	MD5	ok	con licencia	con tarjeta extra
	IPSec	ok	con licencia	con tarjeta extra
	AES	ok	con licencia	con tarjeta extra
	RADIUS	ok	con licencia	con tarjeta extra
Firewall		ACL	con opciones básicas, opciones avanzadas con licencia	con opciones básicas, opciones avanzadas con tarjeta extra
Sistema operativo		IOS propietario de cisco con CLI y acceso Web	SO Propietario, basado en CLI y vía Web	SO Propietario, basado en CLI y vía Web
Interfaces	Fast ETH	ok	ok	ok
	Giga ETH	opcionales tarjetas	no	no
	SYN	V.35 /E1/T1 tarjetas	V.35 /E1/T1 tarjetas	V.35 /E1/T1 tarjetas
	FXS/FXO	opcionales tarjetas	no	opcionales tarjetas
	ADSL	opcionales tarjetas	no	opcionales tarjetas

Tabla 6.12 Comparación de Router's.

En base a la anterior caracterización nos decidimos por utilizar un Router Cisco de la serie 2600, debido a que cumple con la mayor cantidad de requerimientos planteados anteriormente, así también por ser un dispositivo comúnmente y comercialmente usado para aplicaciones similares a la nuestra.

6.10.2 Enlace de datos

A continuación mostramos la configuración del switch y acces point para el modelado del sistema.

Configuración switch1:

Switch>enable

Switch#config terminal
Switch(config)#hostname switch1
Switch1(config)# mac-address-table static 00-13-24-e4-f1-90 interface FastEthernet 0/2 vlan 12
(comando para agregar mac address estáticas a los puertos de el switch, este comando se utilizara como medida de seguridad apra que solo los host autorizados puedan conectarse ala red de acceso este comando se niega ubicando la palabra no antes de todo el código)
Switch1(config)#interface fastethernet 0/1
Switch1(config-if)#switchport access vlan 1 (este comando se utilizara para agregar un Puerto a cierta vlan, esto dependerá de la configuración física de la red para determinar que puertos pertenecen a que vlan´s)
Switch1(config-if)#exit
Switch1(config)#exit
Switch1#vlan database
Switch1(vlan)#vtp v2-mode (configurando la versión de vtp para los puertos trunking de la red, estos se utilizaran para enlazar los switches con el router.)
Switch1(vlan)#vtp domain LAN1
Switch1(vlan)#exit
Switch1#copy run sta

6.10.2.1 Switch

Para la aplicación se ha considerado la implementación de la red de datos basados en un switch de marca cisco modelo catalys. Se tomo esta decisión basado en el des empeño superior del equipo y las características de protocolos e interfaces que soporta.

Interfaces

Puertos convencionales para puntos de red: Ethernet 10/100 Mbps
Puertos para cableado vertical y core de la red: puertos de Fibra óptica (tarjetas sfp/Gibit para fibra monomodo ventana de 1300nm con amplificadores de máximo 20Km, conector SC)

Protocolos
Estos son los protocolos básicos que debe poseer el switch a utilizar.
VLAN´s (debe soportar vlans a)
QoS(calidad de servicios para poder montar servicios IP avanzados en un futuro.)
Spaning tree(Para poder montar características de redundancia y estabilidad en la red de datos.)
VTP (protocolo de trunking para conmutar todas las VLAN´s a una interface del router.)

Configuración:

Configuración de PC.

Para ingresar a los equipos vía consola es necesario hacerlo desde una PC con Hiper Terminal.

Entre a Hiper Terminal y configure los parámetros de conexión de la siguiente manera:

1. Seleccione el puerto COM desde donde se conectara al equipo.
2. Seleccione los parámetros del Hardware

Baud rate	: 9600
Parity	: None
Flow Control	: Hardware
Data bits	: 8
Stop bits	: 1

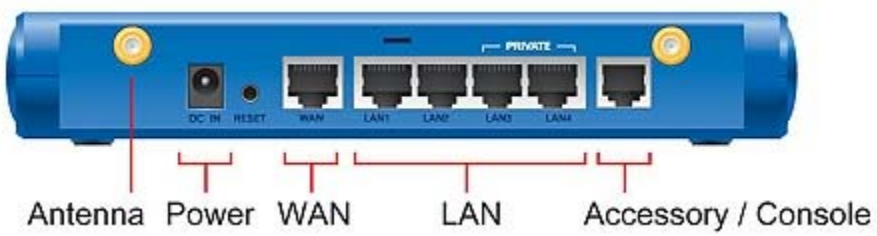
Switch>enable
Switch#config terminal
Switch(config)#hostname switch1
Switch1(config)# mac-address-table static 00-13-24-e4-f1-90 interface FastEthernet 0/2 vlan 12
(Comando para agregar mac address estáticas a los puertos del switch, este comando se utilizara como medida de seguridad apra que solo los host autorizados puedan conectarse ala red de acceso este comando se niega ubicando la palabra no antes de todo el código)
Switch1(config)#interface fastethernet 0/1
Switch1(config-if)#switchport access vlan 1 (este comando se utilizara para agregar un Puerto a cierta vlan, esto dependerá de la configuración física de la red para determinar que puertos pertenecen a que vlan´s)
Switch1(config-if)#exit
Switch1(config)#exit
Switch1#vlan database
Switch1(vlan)#vtp v2-mode (configurando la versión de vtp para los puertos trunking de la red, estos se utilizaran para enlazar los switches con el router.)
Switch1(vlan)#vtp domain LAN1
Switch1(vlan)#exit
Switch1#copy run sta

Esta configuración será la configuración básica para los switch de distribución de datos de la red.

6.10.2.2 Access Point

El equipo Ap que puede utilizarse variar entre las diferentes opciones del mercado, a continuación se presentan las características y procedimientos de configuración de un AP comercial.

Vista posterior



Descripción.

Indicado	***Color***	***Actividad***	***Descripcion***
Φ	verde	encendido	El equipo esta encendido.
((•))	verde	encendido	Indica que las interfaces inalámbricas esta recibiendo señal.
⏚	verde	encendido	Interface Wan recibiendo señal.
1 2 3 4	verde	encendido	Interfaces Lan recibiendo señal.

Figura 6.28 Router Gíreles WIAS – 1000G

Equipo para enrutar trafico de datos en redes cerradas (Lan´s) hacia redes abiertas (Internet), con sistema de contabilidad de trafico (tiempo/paquetes).

Características

LAN
4 Puertos Ethernet para Lan 10/100 BaseTx
Servidor DHCP
Configurables opciones de NAT, para dirección y puertos.
Políticas de acceso para administración configurables
Compatible con protocolos, DHCP, HTTP, SMTP,TLS,SSL,SSH,SMTP v2, POP3,LDAP y H.323(enrutado).
Soporte para conexiones seguras bajo TLS (HTTPS).
Ancho de banda administrable (mediante políticas de conexión)
WAN
1 Puerto Wan 10/100 Base Tx
Soporta conexión en ambientes de direccionamiento estático, Cliente DHCP, PPP.
Soporte para conexiones seguras bajo SSL .
WLAN
Soporta Protocolos IEEE 802.11b y IEEE 802.11g
Protocolos de conexión segura WEP,WPA
Ancho de banda administrable.
WDM configurable para aumentar cobertura.
Agregados
Puerto para Accesorios
Administración de clientes
Listas de acceso
Control de acceso por contraseñas
Registro de facturación (tiempo / volumen de trafico).
Ancho de banda administrable
2 Puertos de LAN privados para administración
Firewall
NAT
DHCP
Gestión de seguridad, tanto para la administración como para el trafico en movimiento.
3 tipos de políticas de administración configurables (route, firewall, listas negras)
Servidores virtuales
Notificación de trafico via e-mail configurable

Configuración de claves de administración.

Conectarse al equipo para administrarlo.
La administración del equipo se lleva acabo vía web (Iexplorer); el equipo solamente es administrable desde los puertos de LAN privadas, para acceder se debe configurar una computadora para ingresar por los puertos de LANs privadas (puertos 3,4 /192.168.2.x, red IP por default; 192.168.2.254 IP del equipo por default).

Ingresar a la interface vía HTML
Para ingresar a la pagina web de administración, se escribe la dirección del equipo (192.168.2.254 IP de fabrica) en la barra de dirección del explorador (Iexplorer).

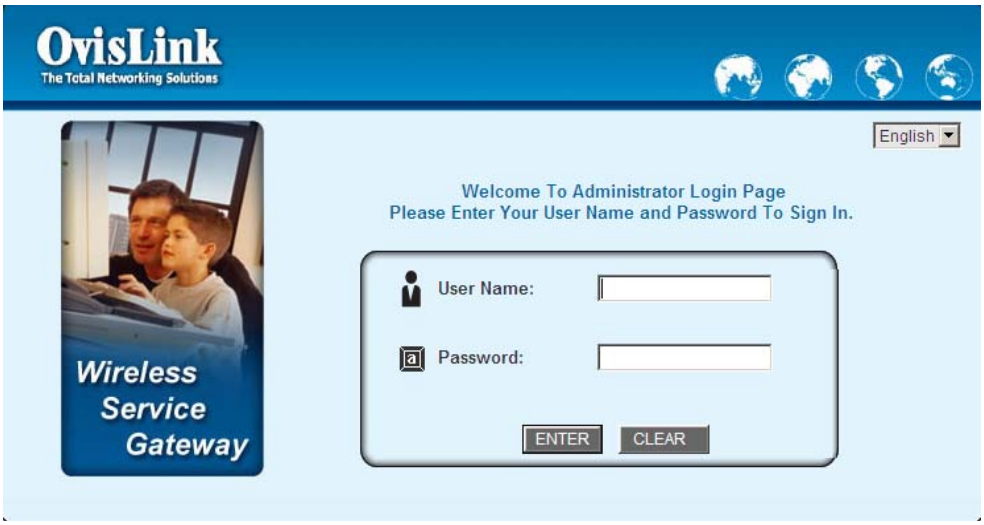


Figura 6.29 Inicio configuración del Router.

Ingresar al menú de administración, como administrador del equipo.
Para ingresar al equipo se puede hacer de 4 formas diferentes, como:
Administrador: se tiene completo acceso a la configuración del equipo y a las cuentas de todos los usuarios
Username: admin
Password: ovislink
Manager: ofrece un acceso limitado al equipo y algunos datos de la configuración no pueden modificarse
Username: manager
Password: ovislink
Operator: ofrece un acceso de monitoreo en el que solo se puede crear y modificar datos referentes a la demanda de los usuarios.
Username: operator
Password: ovislink
Cliente: no se tiene acceso a la administración, ni al monitoreo, solo es posible recibir y mandar trafico.
Username: *** (impuestos por el administrador)
Password: *** (impuestos por el administrador)

Para llevar acabo la administración de contraseñas es necesario entrar como administrador.

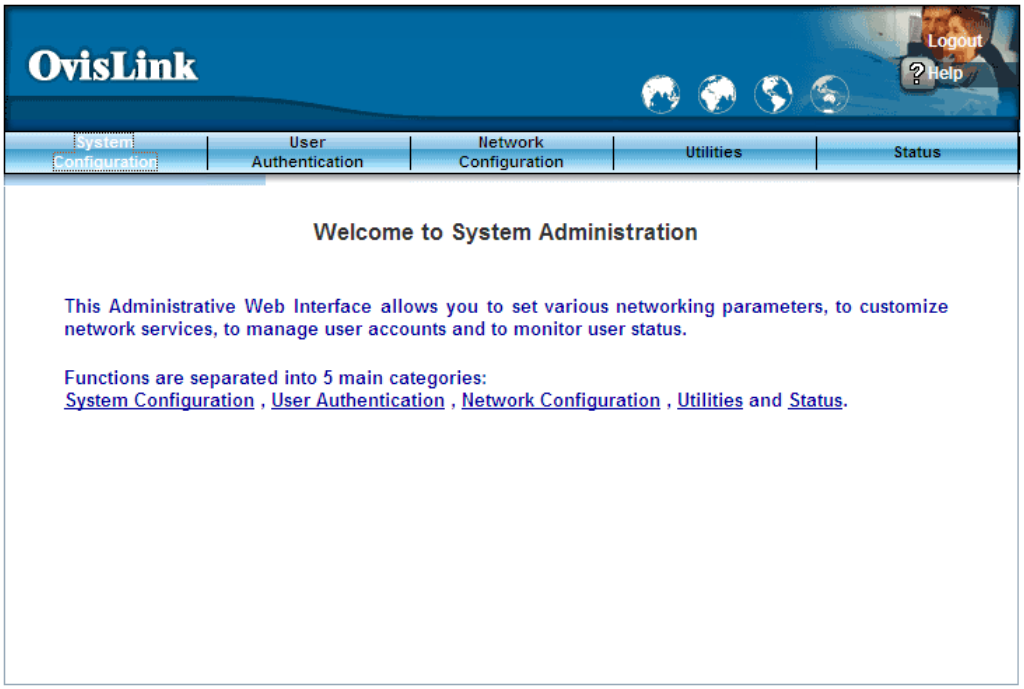


Figura 6.30 Pantalla de Bienvenida al administrador

Seleccionar el item de "**Utilities**". Figura 6.31.

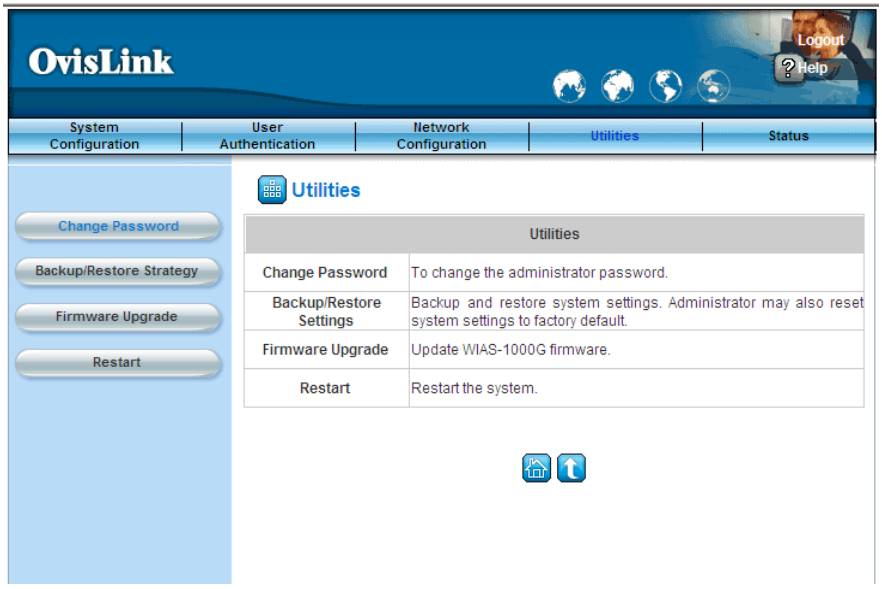


Figura 6.31 Selección de Utilities.

Seleccionar la opción de "**Change Password**", para modificar las contraseñas de todos los modos de administración. Figura 6.32.

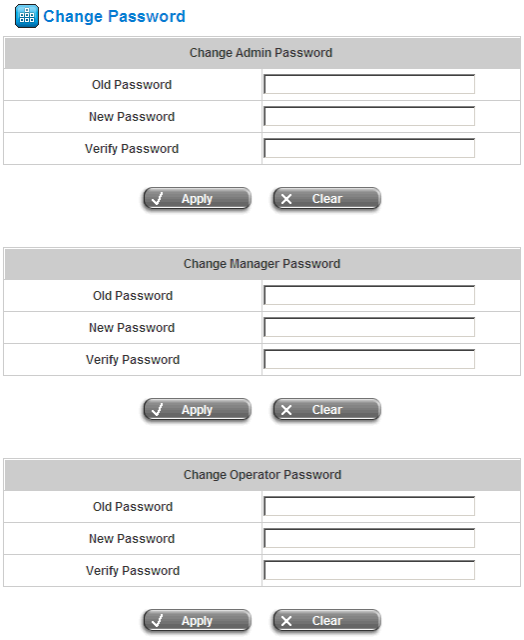


Figura 6.31 Cambio de contraseñas

Para guardar los cambios en necesario dar un click en el botón de "**Apply**"

Configuración de LAN.

Conectarse al equipo para administrarlo.
La administración del equipo se lleva acabo vía web (Iexplorer);el equipo solamente es administrable desde los puertos de LAN privadas, para acceder se debe configurar una computadora para ingresar por los puertos de LANs privadas (puertos 3,4 /192.168.2.x, red IP por default; 192.168.2.254 IP del equipo por default).

Ingresar a la interface vía HTML
Para ingresar a la pagina web de administración, se escribe la dirección del equipo (192.168.2.254 IP de fabrica) en la barra de dirección del explorador (Iexplorer).

Para llevar acabo la administración de los datos de red es necesario entrar como administrador.(user:admin/pass:ovislink). Figura 6.29.

Seleccionar el item de “System Configuration”

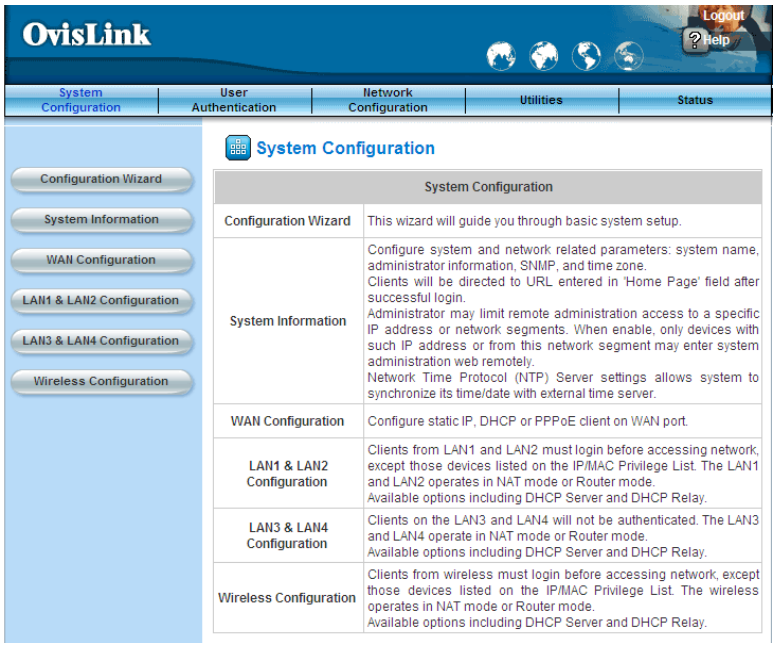


Figura 6.32 System configuration.

Seleccionar las LAN a configurar.
La configuración de los puertos LAN es compartida y no en configurable por los puertos separadamente, Las LAN convencionales comparten la configuración y las LAN privadas (el equipo solo es administrable desde estos puertos) poseen otra configuración

Configurar los datos de la red.
IP PNP:

User Authentication: se refiere al acceso ala red; si el acceso va a ser abierto a todos los que tenan conexión o si es estrictamente necesario que el cliente ingrese por medio de una contraseña.

Operación Mode: Se configura la forma en como se va acceder a redes externas, este puede hacerse de 2 formas: en modalidad Router, la dirección es enrutada hacia el destino, conservando su dirección IP y el puerto del origen (red interna), y la modalidad NAT, en la que el trafico puede salir, pero las direcciones de la red interna sufren un NAT (cambio de dir IP/puerto, útil para no revelar el direccionamiento interno, ni los datos de topología de la red interna) para poder salir hacia redes externas.

IP address: se refiere a la dirección IP del puerto de LAN en el equipo. (Esta dirección será pasada como gateway a los usuarios).

Mask: se refiere ala mascara de la dirección IP del puerto de LAN en el equipo (esta define el tamaño de la red)

DHCP Server Configuration: el servicio de DHCP tiene tres modalidades.

Disable: se inhabilita el servicio, por lo que los usuarios deben asignar los parámetros de red para poder acceder a ella.
Enable: habilita el servicio por lo que es necesario configurar los datos de:
Start IP address, se define a partir de que dirección se iniciara la asignación de direcciones a los clientes.

End IP address, se define hasta que dirección finalizara la asignación de direcciones (estos parámetros definen el banco de direcciones que se asignaran/las direcciones deben estar en la red del equipo, ya que de lo contrario no podra enlasar los clientes)

Preferred DNS server: define cual será el servidor DNS por defecto de los clientes

Alternate DNS server: define un servidor alternativo de DNS por si el principal es inalcanzable.

Domine Name: el nombre de dominio de la red.

Lease Time: se define el tiempo máximo que un host puede retener la dirección asignada. (Una dirección IP asignada aun host, no será asignada a ningún otro host)

Reserved IP Address List: nos da la posibilidad de asignar IP por defecto a ciertos equipos, para que a estos siempre se les asigne la misma dirección (esta opción es general mente utilizada para dar servicio de DHCP a servidores, de impresión u otros equipos en la red que deben poseer una dirección conocida por todos los integrantes de la red)

Enable DHCP Relay: se habilita el equipo para que enrute el servicio de DHCP desde otro equipo, proporcionado por la dirección IP configurada.(opción utilizada cuando el DHCP es dado por otro equipo ya sea dentro o fuera de la red / servidor, router, etc.)

Guardar los Cambios dando Click en el Boton de Apply.

Configuración de WAN

Conectarse al equipo para administrarlo. Figura 6.29.
La administración del equipo se lleva acabo vía web (Iexplorer); el equipo solamente es administrable desde los puertos de LAN privadas, para acceder se debe configurar una computadora para ingresar por los puerto de LAN privadas (puertos 3,4 /192.168.2.x, red IP por default; 192.168.2.254 IP del equipo por default).

Ingresar a la interface via HTML
Para ingresar a la pagina web de administración, se escribe la dirección del equipo (192.168.2.254 IP de fabrica) en la barra de dirección del explorador (Iexplorer).

Para llevar acabo la administración de los datos de red es necesario entrar como administrador.(user:admin/pass:ovislink)

Seleccionar el item de “System Configuration”

Seleccionar “WAN Configuration”.

La configuración de la WAN puede hacerce de 3 modos diferentes según el tipo de entorno en el que se conecte el equipo para nuestro caso, este puede ser:
Dynamic IP Address: utilizada cuando el equipo es un cliente de DHCP (este sera nuestro caso para que los router cisco brinden el direccionamiento vía DHCP).

Guardar los Cambios dando Click en el Boton de Apply.

Configuración protocolo de Seguridad.

Conectarse al equipo para administrarlo.
La administración del equipo se lleva acabo vía web (Iexplorer); el equipo solamente es administrable desde los puertos de LAN privadas, para acceder se debe configurar una computadora para ingresar por los puertos de LANs privadas (puertos 3,4 /192.168.2.x, red IP por default; 192.168.2.254 IP del equipo por default).

Ingresar a la interface vía HTML
Para ingresar a la pagina web de administración, se escribe la dirección del equipo (192.168.2.254 IP de fabrica) en la barra de dirección del explorador (Iexplorer).

Para llevar acabo la administración de los datos de red es necesario entrar como administrador.(user:admin/pass:ovislink)

Seleccionar el item de “System Configuration” Figura 6.32.

Seleccionar las Wireless Configuration.

En este menú se configuran todos los parámetros de la red inalámbrica.
SSID: nombre con la que los usuarios identificaran a la red.Sync to ticket habilita para que este dato se incluya en el ticket del cliente.
Channel: canal de transmisión de la red.
Transmission Mode: modo de transmisión (Mised Default), puede elegir entre 11Mb y 54 Mb.
Security: despliega una ventana donde se habilita el protocolo WEP para una acceso seguro a la red.

Configuración de protocolo WEP

1.Dar click en el vínculo de Securit
2. Seleccionar “Enable”
3. Seleccionar el tamaño de la clave a utilizar (64/128 bits), con una clave más grande la seguridad es mejor.
4. Seleccionar el modo de cifrado (HEX/ASCII), si el modo de cifrado es hex, la Clave solo puede contener números y letras de la A hasta la F. El tamaño de la clave depende del siguiente cuadro.
Tamaño\modo HEX ASCII
64 bits 10 caracteres 5 caracteres
128 bits 26 caracteres 13 caracteres
5.Guardar los cambios con el boton “Apply”
Modo de operación: selecciona el modo en el que se tratara el trafico de las wlan, si se elige nat secles aplica nat y salen con la ip de wan, si se selecciona route,la ip es ruteada y no se le aplica nat.

IP address: define la ip de la interface WLAN (192.168.3.254 por default).
Mask: define la mascara de la red.
DHCP: se puede habilitar DHCP para que las ip se asignen de forma dinámica. En esta modalidad es necesario definir el inicio y fin de la asignación, así como un DNS y el nombre decdominio.
Guardar los Cambios dando Click en el Boton de Apply.

Con esto configuramos el Access point para nuestra aplicación.

6.10.3 Red

La etapa de red esta diseñada de acuerdo a las consideraciones de seguridad, crecimiento y escalabilidad del sistema. La seguridad limitara el acceso de los usuarios tanto en el uso de las redes internas como el acceso a Internet, para ello se hace uso de listas de acceso que limitan el trafico de protocolos y servicios especiales dentro e la red, omitiendo así trafico no deseado como correos electrónicos, mensajeria (MSN, yahoo msn, google talk, etc), administradores de descarga (Torrents, Ares, etc.), etc. Convirtiendo así la configuración de red en una firewall de bajo nivel, donde se están limitando los paquetes no deseados, y solamente se procura el trafico de red deseado, que para nuestro caso son los paquetes http (puerto 80 ó 8080) y paquetes propios de las bases de datos, para realizar las consultas del caso (SQL puertos 443 y 520).

El sistema esta diseñado de tal manera que pueda crecer a futuro no solo en numero de usuarios, sino también en redes, permitiendo así anexar otros hospitales o clínicas al sistema, y permitiendo la interacción de estas sin descuidar las políticas de ruteo, y discriminación de paquetes. Cada una de las redes esta diseñada para soportar el tráfico de consultas de hasta 50 usuarios, en el caso que estos aumentaran, el hardware destinado al ruteo debería de escalarse a uno de características superiores para atender las peticiones sin problema.

Por otra parte la topología de red permite el acceso a Internet, de esta manera se puede escalar el acceso al sistema desde Internet, sin embargo para esto, es necesario definir nuevas políticas de acceso y modificar algunos dictámenes de seguridad, para velar por la seguridad de la información. La utilización del acceso por medio de Internet de este sistema, podría dar como resultado el acceso de esta información inclusive desde terminales móviles celulares, ó los pilares para el acceso mediante diferentes tecnologías futuras como Wimax.

A continuación mostramos la configuración de los router's del modelado del sistema de red.

Configuración HB1:

```
Router>enable
Router#config terminal
Router(config)#host HB1
HB1(config)#ip access-list extended politica1
HB1(config-ext-nacl)#permit icmp any any
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 80
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 8080
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 443
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 520
```

```
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 25
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 80
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 8080
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 443
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 520
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 25
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 80
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 8080
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 443
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 520
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 25
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 80
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 8080
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 443
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 520
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 25
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 80
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 8080
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 443
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 520
HB1(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 25
HB1(config-ext-nacl)#exit
HB1(config)#interface eth0/0
HB1(config-if)#no shutdown
HB1(config-if)#ip address 192.168.0.33 255.255.255.224
HB1(config-if)#ip nat inside
HB1(config-if)#ip access-group politica1
HB1(config-if)#exit
HB1(config)#interface ser0/0
HB1(config-if)#no shutdown
HB1(config-if)#ip address X.X.X.X x.x.x.x[36]
HB1(config-if)#ip nat outside
HB1(config-if)#exit
HB1(config)#access-list 1permit 192.168.0.0 0.0.0.255
HB1(config)#ip nat inside source list 1 interface serial0/0 overload
HB1(config)#router rip
HB1(config-router)#network 192.168.0.32
HB1(config-router)#exit
HB1(config)# ip route 0.0.0.0 0.0.0.0 y.y.y.y[37]
HB1(config)#exit
HB1#copy run stat
```

Configuracion HB2:

```
Router>enable
Router#config terminal
Router(config)#host HB2
HB2(config)#ip access-list extended politica1
HB2(config-ext-nacl)#permit icmp any any
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 80
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 8080
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 443
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 520
```

[36] X.x.x.x dependera de la ip que el proveedor de servicios de Internet proporcione
[37] Y.y.y.y dependeta de la ip del siguiente salto (default gateway) que proporcione el ISP

```
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 25
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 80
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 8080
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 443
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 520
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 25
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 80
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 8080
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 443
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 520
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 25
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 80
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 8080
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 443
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 520
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 25
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 80
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 8080
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 443
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 520
HB2(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 25
HB2(config-ext-nacl)#exit
HB2(config)#interface eth0/0
HB2(config-if)#no shutdown
HB2(condif-if)#exit
HB2(config)#interface eth0/0.1
HB2(config-subif)#description DMZ VLAN1
HB2(config-subif)#encapsulation dot1q 1
HB2(config-subif)#ip address 192.168.0.62 255.255.255.224
HB2(config-subif)#ip access-group politica1
HB2(config-subif)#exit
HB2(config)#interface eth0/0.2
HB2(config-subif)#description LAN1 VLAN2
HB2(config-subif)#encapsulation dot1q 2
HB2(config-subif)#ip address 192.168.0.90 255.255.255.224
HB2(config-subif)#ip access-group politica1
HB2(config-subif)#exit
HB2(config)#interface eth0/0.3
HB2(config-subif)#description Wireless1 VLAN3
HB2(config-subif)#encapsulation dot1q 3
HB2(config-subif)#ip address 192.168.0.126 255.255.255.224
HB2(config-subif)#ip access-group politica1
HB2(config-subif)#exit
HB2(config)#router rip
HB2(config-router)#network 192.168.0.32
HB2(config-router)#network 192.168.0.64
HB2(config-router)#network 192.168.0.92
HB2(config-router)#exit
HB2(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.33
HB2(config)#ip dhcp pool subnet1
HB2(dhcp-config)#network 192.168.0.32 255.255.255.224
HB2(dhcp-config)#defaul-router 192.168.0.33
HB2(dhcp-config)#dns-server 192.168.0.35
HB2(config)#ip dhcp pool subnet2
HB2(dhcp-config)#network 192.168.0.64 255.255.255.224
HB2(dhcp-config)#defaul-router 192.168.0.90
```

```
HB2(dhcp-config)#dns-server 192.168.0.35
HB2(config)#ip dhcp pool subnet3
HB2(dhcp-config)#network 192.168.0.92 255.255.255.224
HB2(dhcp-config)#defaul-router 192.168.0.126
HB2(dhcp-config)#dns-server 192.168.0.35
HB2(config)#exit
HB2#copy run stat
```

Configuracion HB3:

```
Router>enable
Router#config terminal
Router(config)#host HB3
HB3(config)#ip access-list extended politica1
HB3(config-ext-nacl)#permit icmp any any
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 80
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 8080
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 443
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 520
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.32 0.0.0.31 any port 25
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 80
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 8080
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 443
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 520
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.64 0.0.0.31 any port 25
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 80
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 8080
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 443
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 520
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.128 0.0.0.31 any port 25
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 80
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 8080
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 443
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 520
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.160 0.0.0.31 any port 25
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 80
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 8080
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 443
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 520
HB3(config-ext-nacl)#access-list 1 permit tcp 192.168.0.192 0.0.0.31 any port 25
HB3(config-ext-nacl)#exit
HB3(config)#interface eth0/0
HB3(config-if)#no shutdown
HB3(condif-if)#exit
HB3(config)#interface eth0/0.1
HB3(config-subif)#description DMZ VLAN1
HB2(config-subif)#encapsulation dot1q 1
HB3(config-subif)#ip address 192.168.0.61 255.255.255.224
HB3(config-subif)#ip access-group politica1
HB3(config-subif)#exit
HB3(config)#interface eth0/0.2
HB3(config-subif)#description LAN2 VLAN4
HB2(config-subif)#encapsulation dot1q 4
HB3(config-subif)#ip address 192.168.0.158 255.255.255.224
HB3(config-subif)#ip access-group politica1
HB3(config-subif)#exit
```

```
HB3(config)#interface eth0/0.3
HB3(config-subif)#description Wireless2 VLAN5
HB2(config-subif)#encapsulation dot1q 5
HB3(config-subif)#ip address 192.168.0.190 255.255.255.224
HB3(config-subif)#ip access-group politica1
HB3(config-subif)#exit
HB3(config)#router rip
HB3(config-router)#network 192.168.0.32
HB3(config-router)#network 192.168.0.128
HB3(config-router)#network 192.168.0.160
HB3(config-router)#exit
HB3(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.33
HB3(config)#ip dhcp pool subnet4
HB3(dhcp-config)#network 192.168.0.128 255.255.255.224
HB3(dhcp-config)#defaul-router 192.168.0.158
HB3(dhcp-config)#dns-server 192.168.0.35
HB3(config)#ip dhcp pool subnet3
HB3(dhcp-config)#network 192.168.0.160 255.255.255.224
HB3(dhcp-config)#defaul-router 192.168.0.190
HB3(dhcp-config)#dns-server 192.168.0.35
HB3(config)#exit
HB3#copy run stat
```

Con estas configuraciones logramos terminar el diseño de la red que detallamos en la figura 6.27.

Esta red esta diseñada para nuestra aplicación aunque tiene toda la capacidad de convertirse en una red para una aplicación a gran escala ya que todo el equipo utilizado es el que se utiliza para proyectos reales.

Future lines.

Las tecnologías de telecomunicación están denotando una clara tendencia hacia los datos y las tecnologías basadas en IP, prueba de ello son las discusiones sobre el nuevo estándar de IPv6, en tal sentido los proyectos basados en esta tecnología, no serán fácilmente descontinuados, sino que tendrán una escalabilidad y alcances mas grandes.

En el futuro se espera que tengamos en nuestro país instituciones medico hospitalarias, mas preparadas y abiertas al uso de tecnologías de la información para mejorar los procesos internos y traducirlos en una mejor atención a los usuarios, en tal sentido proyectos como el que se expone en este trabajo, servirán como base para diseñar y crear nuevos y mas complejos sistemas de acceso, haciendo uso de otras redes como la red celular, Wimax u otras tecnologías de acceso futuras, en las que se procure el trafico Ip.

Se espera que en el futuro, los avances en la fabricación de equipos portátiles, puedan tener al posibilidad de mostrar no solo información en texto plano, sino, información dinámica mas significativa como, imágenes medicas de alta definición (rayos X, encefalogramas, ultrasonofragias, etc), y mediciones corporales en tiempo real, para tener un monitoreo constante y mas detallado de los pacientes, y esto con las tecnologías de la información que ayude a documentar mejor un caso y se traduzca en mejores diagnósticos, o inclusive en el descubrimiento de nuevas enfermedades, que por falta del monitoreo continuo no se han detectado.

Conclusiones

Es importante a la hora de implementar una solución tecnológica de este tipo no buscar la más cara y compleja sino por lo contrario es importante mantener y buscar una solución lo más simple posible para que a medida evolucione el equipo y aplicaciones nuestra solución le pueda seguir los pasos a dichos avances.

Se debe considerar que dentro de la implementación de un proyecto de gran envergadura participen un grupo de personas multidisciplinarias (Ingenieros, médicos, personal administrativo etc.) para enriquecer este tipo de aplicaciones, y a su vez sigan las recomendaciones y normas de organismos internacionales y de otras entidades en países donde el tema este un poco más depurado, por ejemplo casos como el de Europa, EE.UU. y Canadá.

A la hora de planificar la instalación de equipo radiante, se debe tener en cuenta la situación de escenarios especiales como los de la sala de cuidados intensivos ya que es una de las zonas más delicadas en un hospital por la situación en la que están los pacientes en estado crítico.

Las entidades de salud tales como el Ministerio de Salud Pública de nuestro país deberían de realizar seminarios para la educación y la sensibilización a profesionales que trabajan en entornos médicos sobre los efectos de aplicaciones tecnológicas como el que proponemos, ya que ayudan a hacer mas eficiente los servicios que ofrecen los hospitales, y abren una puerta a un mundo de muchas posibilidades, teniendo en cuenta siempre un previo estudio del efecto de una implementación inalámbrica dentro del hospital que con una correcta planeación traería muchos beneficios a los pacientes y a los mismos médicos.

Lo ideal cuando se va a implementar una aplicación como la que proponemos es que el equipo médico sea expuesto a condiciones reales de funcionamiento para ver como se comportan cuando los irradia un campo electromagnético, esto para evitar cualquier problema que no se tenga contemplado dentro del diseño.

El campo de acción de nuestro proyecto es muy amplio y aún falta mucho camino que abarcar en las áreas de gestión y administración, docencia, consultas, terapia, diagnóstico, laboratorios, cuidados intensivos, quirófanos etc.

Se debe tener una política de calidad continua que incluya planificación, controles y garantías, para contener cualquier contingencia que ocurra.

Otro aspecto a tomar en cuenta es el tema de la seguridad y confidencialidad, se debe de crear una política que lleve a que un profesional no falte a la confianza que le da su paciente y alimente en él la ética que todo médico debe de tener, la aplicación puede ofrecer muchos niveles de seguridad tanto de software como de hardware pero no hay nada que pueda evitar que alguien cometa un ilícito con la información a la que tiene acceso.

Referencias.

Bibliografíca.

- "La situación de las tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes (Wi-Fi)". Grupo de Nuevas Actividades Profesionales. Colegio Oficial de Ingenieros de Telecomunicación. Octubre 2004.
- "Informe sobre emisiones electromagnéticas de los sistemas de telefonía móvil y acceso fijo inalámbrico". Colegio Oficial de Ingenieros de Telecomunicación. Editor: José Ignacio Alonso Montes. Octubre 2001.
- "La gestión de frecuencias en entornos sanitarios". Victoria Ramos González, José Luis Monteagudo Peña. Instituto de Salud Carlos III, Madrid. Libro de Ponencias Mundo Internet 2004, pp. 507–513.
- "Cuadro nacional de atribución de frecuencias". Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Ministerio de Ciencia y Tecnología. Junio 2005.
- "Telemedicine glossary". 5ª Edición. Editor: Luciano Beolchi. European Information Society Directorate–General. Bruselas. Septiembre 2003.
- "Guía de protección de datos personales para servicios sanitarios públicos". Agencia de Protección de Datos de la Comunidad de Madrid. 2004.
- "Seguridad electromagnética en telemedicina". Victoria Ramos González. Instituto de Salud Carlos III, Madrid, 2004.
- "Telemedicina: construyendo la sanidad del futuro". José Luis Monteagudo Peña. BIT nº 136, noviembre-diciembre 2002. pp 48-55.
- "Electromagnetic compatibility in médical equipment: a guide for designers and installers". William D. Kimmel, Daryl D. Gerke. Interpharm Press, New York 1995.
- "Electromagnetic compability of médical devices with mobile communications". Médical Device Agency Device bulletin DB9702. Londres. 1997.
- "Use of handheld wireless communication devices in hospitals and electronic interference with médical equipment". Morrissey, J. MOHCA. Mobile Healthcare Alliance. 2002.
- "Electronic médical devices and emi". Silberberg, J.L. Reference Guide. Compliance engineering. Center for devices and radiological health, FDA Food and Drugs Administration. 1996.

Web

- http://www.acemtic.com/pages/prensa_b.php?idart=36

Última visita 10-05-2007

- http://www.ieee.org

Última visita 12-05-2007

- http://uluru.ee.unsw.edu.au/~tim/projects/measure.11/2003/thesis.pdf

Última visita 10-02-2007

- http://de.wikipedia.org/wiki/IEEE_802.11n

Última visita 10-10-2006

- http://ic.esimecu.ipn.mx/pdf/quinto/ANSIAN.PDF

Última visita 01-04-2007

- http://www.wikipedia.es

Última visita 23-05-2007

- http://www.snarc.net/pda/pda-treatise.htm

Última visita 09-02-2007

- http://www.microsoft.com/spanish/msdn.php

Última visita 20-08-2006

- http://msdn.microsoft.com/msdnmag/issues/06/12/windowsce/Default.aspx?loc=es#S2

Última visita 30-03-2007

- http://www.palmsource.com/palmos/garnet.html

Última visita 15-11-2006

Anexos.

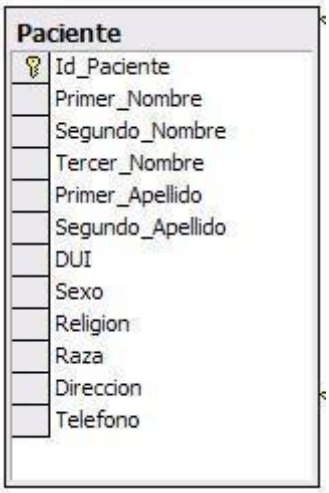
Diccionario de los campos.

1-Tabla Medico.

Nombre de columna	Tipo de dato	Longitud
Id_Medico	bigint	8
Nombre1	varchar	25
Nombre2	varchar	25
Apellido1	varchar	25
Apellido2	varchar	50
Apellido3	varchar	25
Telefono	varchar	8
Direccion	varchar	200
Especialidad	varchar	100

Llave Primaria
Id_Medico

2-Tabla Paciente.



Nombre de columna	Tipo de dato	Longitud
Id_Paciente	bigint	8
Primer_Nombre	varchar	30
Segundo_Nombre	varchar	30
Tercer_Nombre	varchar	30
Primer_Apellido	varchar	30
Segundo_Apellido	varchar	30
DUI	varchar	11
Sexo	varchar	20
Religion	varchar	30
Raza	varchar	30
Direccion	varchar	200
Telefono	varchar	8
edad	varchar	10

Llave Primaria
Id_Paciente

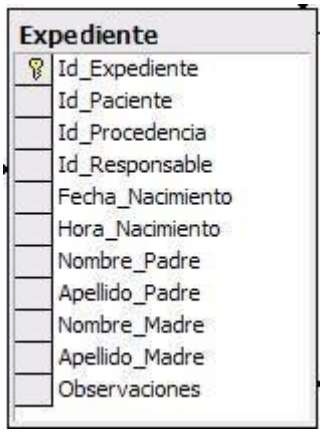
3-Tabla Receta.

Nombre de columna	Tipo de dato	Longitud
Id_Receta	bigint	8
Id_Paciente	bigint	8
Medicamento	bigint	50

Nombre de columna	Tipo de dato	Longitud
Id_Medico	bigint	8
Observaciones	char	150

Llave Primaria
Id_Receta

4-Tabla Expediente.



Nombre de columna	Tipo de dato	Longitud
Id_Expediente	bigint	8
Id_Paciente	bigint	8
Id_Procedencia	bigint	8
Id_Responsable	bigint	8
Fecha_Nacimiento	smalldatetime	4
Hora_Nacimiento	timestamp	8
Nombre_Padre	varchar	50
Apellido_Padre	varchar	50
Nombre_Madre	varchar	50
Apellido_Madre	varchar	50
Observaciones	varchar	500

Llave Primaria
Id_Expediente

5-Tabla Departamentos

Nombre de columna	Tipo de dato	Longitud
Id_Departamento	bigint	8
Departamento	varchar	50

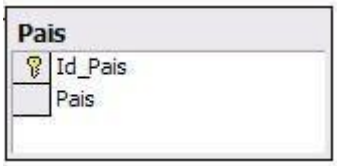
Llave Primaria
Id_Departamento

6-Tabla Municipios

Nombre de columna	Tipo de dato	Longitud
Id_Municipio	bigint	8
Id_Departamento	bigint	8
Municipio	varchar	50

Llave Primaria
Id_Municipio

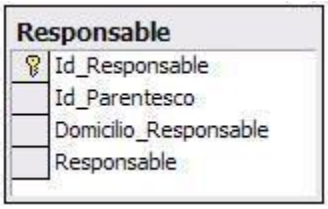
7- Tabla País



Nombre de columna	Tipo de dato	Longitud
Id_Pais	bigint	8
Pais	varchar	50

Llave Primaria
Id_Pais

8-Tabla Responsable



Nombre de columna	Tipo de dato	Longitud
Id_Responsable	bigint	8
Id_Parentesco	bigint	8
Domicilio_Responsable	varchar	100
Responsable	varchar	50

Llave Primaria
Id_Responsable

9-Tabla Parentesco

Nombre de columna	Tipo de dato	Longitud
Id_Parentesco	bigint	8
Parentesco	varchar	50

Llave Primaria
Id_Parentesco

10-Tabla Registro_Diario

Nombre de columna	Tipo de dato	Longitud

Id_Registro	bigint	8
Id_Area	bigint	8
Id_Tipo_Consulta	bigint	8
Sospecha	char	10
Morbilidad	char	10
Discapacidad	char	10
Ingreso_Hospitalario	char	10
Id_Tipo_Referencia	bigint	8
Id_Expediente	bigint	8

Llave Primaria
Id_Registro

11-Tabla Area

Nombre de columna	Tipo de dato	Longitud
Id_Area	bigint	8
Area	varchar	50

Llave Primaria
Id_Area

12-Tabla Tipo_Referencia

Nombre de columna	Tipo de dato	Longitud
Id_Tipo_Referencia	bigint	8
Tipo_Referencia	varchar	50

Llave Primaria
Id_Tipo_Referencia

13- Usuarios

Nombre de columna	Tipo de dato	Longitud
Id_Usuario	bigint	8
Nombre_Completo	varchar	150
Email	varchar	75
Numero_Contacto	varchar	11
Usuario	varchar	50
Password	varchar	255
Perfil	varchar	50

Llave Primaria
Id_Usuario