INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRONICA, COMPUTACION, INFORMACION Y COMUNICACIONES

ANALISIS DE LA SEGURIDAD EN APLICACIONES DE REDES MOVILES DE TERCERA GENERACION PARA EL ESTABLECIMIENTO DE ARQUITECTURAS, POLITICAS Y CONTROLES

T E S I S

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACION DE LAS TELECOMUNICACIONES

POR

JOANA ALEJANDRA HERRERA SUAREZ

MONTERREY, N. L. MAYO 2005

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRONICA, COMPUTACION, INFORMACION Y COMUNICACIONES

ANALISIS DE LA SEGURIDAD EN APLICACIONES DE REDES MOVILES DE TERCERA GENERACION PARA EL ESTABLECIMIENTO DE ARQUITECTURAS, POLITICAS Y CONTROLES

T E S I S

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACION DE LAS TELECOMUNICACIONES

POR

JOANA ALEJANDRA HERRERA SUAREZ

MONTERREY, N. L. MAYO 2005

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓNY COMUNICACIONES

Análisis de la seguridad en aplicaciones de redes móviles de tercera generación para el establecimiento de arquitecturas, políticas y controles

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN DE LAS TELECOMUNICACIONES

POR:

Joana Alejandra Herrera Suárez

MONTERREY , N.L. Mayo 2005

INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE MONTERREY

DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

PROGRAMAS DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

Los miembros del comité de tesis recomendamos que la presente tesis de la Ing. Joana Alejandra Herrera Suárez sea aceptada como requisito parcial para obtener el grado académico de Maestro en Administración de las Telecomunicaciones.

Comité de tesis:

Jorge Carlos Mex Perera Ph.D.
Asesor

Gabriel Campuzano Treviño Ph.D
Sinodal

José Ramón Rodríguez Cruz Ph.D.
Sinodal

David Alejandro Garza Salazar Ph.D.
Director del Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.

MAYO 2005

Análisis de la seguridad en aplicaciones de redes móviles de tercera generación para el establecimiento de arquitecturas, políticas y controles

POR:

Joana Alejandra Herrera Suárez

TESIS

Presentada al Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración en las Telecomunicaciones

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

MAYO 2005

Dedicatoria

A mis padres porque a pesar del esfuerzo y sacrificio que significa la realización de este sueño, me apoyaron incondicionalmente brindándome todo su amor, cariño y confianza.

A mis hermanos a quienes admiro mucho y que siempre me han acompañado en los momentos más importantes de mi vida alentándome a dar lo mejor de mí para lograr mis metas.

A mi familia pilar fundamental de mi vida y de mis valores, por enseñarme que a pesar de la distancia puedo contar con su afecto, apoyo y comprensión.

A Emilio que siempre estuvo conmigo a lo largo de este camino renovando mis fuerzas en los momentos más difíciles.

A mis amigos quienes creyeron en mí y estuvieron siempre dándome ánimos en los momentos de tristeza y celebrando los pequeños logros para alcanzar el triunfo.

Agradecimientos

A Dios por estar conmigo día con día, llevándome de la mano a lo largo de la vida, fortaleciendo mi fe y otorgándome la sabiduría para vencer cualquier obstáculo que se presente para lograr mis metas.

A mi asesor, el Dr. Carlos Mex por guiarme en esta difícil carrera contra el tiempo y demostrar gran interés en la materialización de este proyecto.

Al Dr. Ricardo Pineda quien me ayudó a sentar las bases para poder continuar el desarrollo de este proyecto sobre un camino de conocimientos claros y firmes.

A todas las personas que contribuyeron de alguna manera en la realización de una de mis más grandes ilusiones.

Tabla de contenido

Lista de figuras

Lista de tablas

Capítulo 1. Introducción

1.1 Antecedentes

Las tecnologías inalámbricas han tenido mucho auge y desarrollo en estos últimos años, en particular una que ha experimentado un crecimiento espectacular es la telefonía celular. Desde sus inicios los teléfonos celulares han revolucionado enormemente las actividades que realizamos diariamente y se han convertido en una herramienta primordial para la gente común y de negocios; las hace sentir más seguras y las hace más productivas. (Jiménez, 2003)

A pesar de que fue concebida estrictamente para la voz, conforme ha ido evolucionando la tecnología celular también ha sido capaz de brindar otro tipo de servicios, como datos, audio y video.

Pero no sólo la telefonía ha cambiado drásticamente la forma de comunicarnos, el Internet ha hecho realidad lo que en los años 70's el visionario de las comunicaciones Marshall McLuhan denominó la "Aldea Global". En muy pocos años el Internet se ha consolidando como una poderosa plataforma que ha cambiado el mundo de la información, otorgándole mayor dinamismo y una dimensión internacional, o "globalizada".

El Internet constituye el más democrático de todos los medios masivos de comunicación, por una muy baja inversión, le permite a cualquiera llegar en forma directa, rápida y económica a la información sin importar donde se encuentre, así la comunicación, junto con la información, ha sido una de las opciones más interesantes y sobre todo más usadas por los internautas. Mediante el correo electrónico, videoconferencia y demás mecanismos, dos personas pueden estar en contacto e intercambiar información al instante. (Collado, Hispamedia, 2003)

La posibilidad de acceder a la Red vía móvil y la aparición de móviles de tercera generación, permite un acceso más inmediato y más rápido, así como mayores ingresos derivados del pago de contenidos que vía PC son de carácter gratuito. (CEPREDE, 2004)

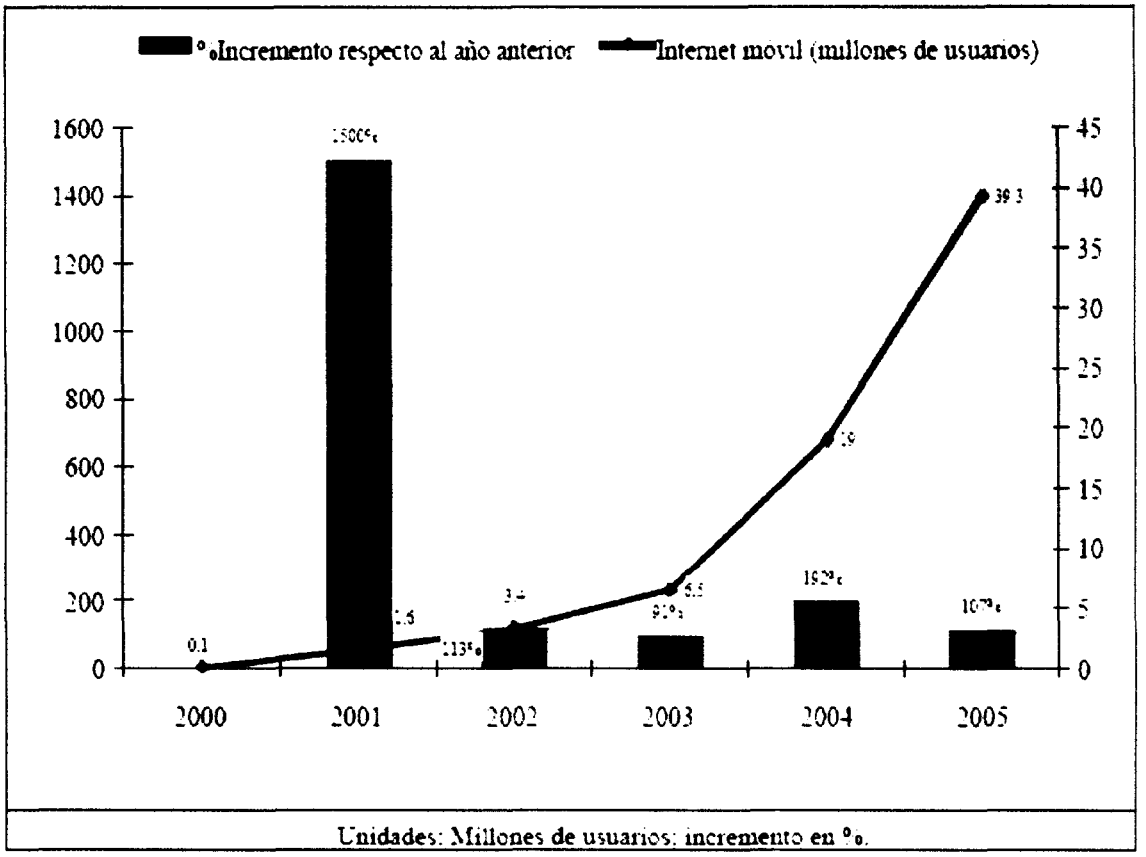

Figura 1. Evolución esperada de Internet móvil a nivel mundial
Fuente: Micrologic Research.

Como se muestra en la figura 1, la evolución de Internet móvil a nivel mundial es claramente creciente, de los 1,6 millones de usuarios que en ese entonces accedían a Internet mediante los móviles, se esperaban ser 39,3 millones en 2005, según un informe de Micrologic Research. En cuanto al crecimiento en el número de personas que utilizan este medio va disminuyendo a medida que pasa el tiempo y se consolida el mercado de los móviles. Si bien, el crecimiento esperado para 2005 seguía siendo superior al 100%. (CEPREDE, 2004)

Tanto los sistemas de Internet como los sistemas inalámbricos se están expandiendo a pasos acelerados. En la interacción de estas áreas de crecimiento encontramos al Internet Móvil, como una de las más interesantes oportunidades de negocio. La explosión del Internet ha cambiado la forma en que obtenemos información y realizamos negociaciones. Ahora tercera generación introduce valor que se extiende más allá de los límites.

El desafío es unir la cobertura de telefonía móvil y la base de usuario asociada con la Internet y otras aplicaciones multimedia y servicios de *información*

y, dado que la mayor parte de estos servicios serán ofrecidos por medio de la Internet, una de las características de 3G es dar Internet móvil añadiendo una completa y amplia gama de nuevas posibilidades y oportunidades. (Torrealba, Ericsson, 2000, 2004)

1.2 Problema

Las redes móviles crecen y cambian para convertirse de redes que ofrecen un único servicio inicial de voz a redes IP (redes que utilizan los protocolos TCP/IP para su funcionamiento por ejemplo Internet) por lo que, se vuelve mucho más difícil ejercer el mismo nivel de control sobre las aplicaciones, servicios y datos que se mantiene actualmente.

También se debe tener en cuenta que muchas veces no basta únicamente con protegernos de las posibles amenazas que provienen de Internet. La mejora tecnológica que se produce constantemente en las telecomunicaciones ha llevado a la proliferación de ataques y comportamientos maliciosos que anteriormente eran imposibles. Lo que antes hubiera tardado meses y años, en la actualidad con los anchos de banda mejorando cada día pasa a ser cuestiones de días o incluso horas. (Verdejo, Scheffler, Schnor 2004)

Las funciones que manejan mecanismos de seguridad son una parte importante de la inteligencia de una red móvil. Por diversas razones, la necesidad de tales funciones es considerablemente mayor en redes móviles que en redes fijas; los dispositivos móviles son mucho más susceptibles de ser perdidos o robados y el acceso vía radio deja abierta la intromisión en las ondas. (Ericsson, 2004)

Las redes móviles existentes tienen algunas características que trabajan a favor de una operación segura aún bajo potenciales debilidades de la arquitectura de seguridad. (Scheffler, Schnor, 2004)

- Autenticación confiable del usuario
- Diseño de redes cerradas
- Propiedad de hardware y software
- Diseño único de servicio
- Control dedicado y diferente
- Baja complejidad

Como los multi-servicios futuros de las redes móviles permitirán el acceso a un grupo mucho más diverso de usuarios y servicios, la arquitectura de seguridad necesita ser flexible para lidiar con las nuevas amenazas emergentes debido a la nueva tecnología y escenarios.

Podemos afirmar entonces, que el reto consiste en proporcionar una transición transparente a una nueva integración de servicios con una nueva

arquitectura, sin comprometer la seguridad y la confiabilidad de las redes. Y ya que la gestión de la seguridad aún no es una práctica común en las organizaciones el diseño e implementación de políticas, controles y procesos no resulta del todo fácil, sobre todo cuando no se trata de una tecnología madura como tercera generación, que aún no tiene penetración mundial.

Además debido a que cada operador mantiene un esquema de servicios diferente, el diseño de un esquema de seguridad único y una arquitectura genérica que abarque todas las aplicaciones resulta casi imposible.

1.3 Hipótesis

Las aplicaciones de E-mail, Localización y M-Health en redes móviles de tercera generación no cuentan con un esquema totalmente completo y eficiente que integre la tecnología con el establecimiento de políticas y controles para proteger la información.

1.4 Objetivo

Analizar la seguridad en las redes móviles de tercera generación, identificando algunas de las aplicaciones relevantes, así como sus correspondientes vulnerabilidades, posibles amenazas y determinar sus riesgos e impacto para proponer un posible modelo de arquitectura que soporte la integración de servicios, así como el establecimiento de políticas y directrices que permitan una efectiva gestión de la seguridad.

1.5 Alcances y Limitaciones

Para restringir el problema de forma que sea tratado en ésta tesis, el estudio se limitará las tres aplicaciones que resulten más relevantes después de aplicar diversos criterios de evaluación y selección.

1.6 Metodología y Métodos

Para el desarrollo de la tesis se utilizará la consulta y análisis de diversas fuentes bibliográficas especializadas en el tema, las cuales proporcionarán las bases y sustentarán el contenido del documento.

Además se utilizará el Estándar ISO 17799 el cual proporciona un marco general para desarrollar el Sistema de Administración de la Seguridad, cubriendo un conjunto de dominios de la seguridad que van desde los controles en accesos físicos, configuración de equipos, personal y procesos entre otros.

1.7 Contribución Esperada

El análisis profundo de las aplicaciones críticas en la Integración de servicios en el Internet móvil, permitirá identificar los puntos más vulnerables a diversas amenazas que podrían poner en riesgo la integridad de los servicios ofrecidos por las empresas que ofrecen aplicaciones de tercera generación.

Además en base a los resultados obtenidos con la aplicación del ISO 17799 se realizará una propuesta de arquitectura de seguridad adecuada para la integración de servicios y el establecimiento de políticas y controles para gestionar adecuadamente la seguridad en tercera generación.

Capítulo 2. Hacia Tercera Generación

La historia de la telefonía móvil nos remonta hasta 30 años atrás, cuando en 1973 se estableció el primer contacto telefónico con éxito usando un terminal portátil. Esta llamada tuvo como protagonistas a Martin Cooper, un ejecutivo de Motorola, y Joel Engel, un importante ejecutivo de Bell Labs. Como es de esperar viendo los protagonistas de la primera llamada por móvil, el terminal usado fue un Motorola, más concretamente un DynaTAC 800OX.

Todo esto se pudo realizar gracias a 15 años de investigación y una inversión de 150 millones de dólares. No fue hasta 1983 cuando el DynaTAC de Motorola consiguió la licencia de comercialización. Ese mismo año se monta el primer sistema de telefonía móvil, uniendo las ciudades Americanas de Washington y Baltimore.

El funcionamiento de aquella primera tecnología móvil se basaba en el envío por parte del terminal de una señal a las antenas receptoras instaladas en la zona donde se encontraba el usuario del teléfono. En aquellos primeros años, cada antena receptora cubría alrededor de 15 manzanas a la redonda. Estos pulsos eran cursados a una central que procesaba la señal y elegía el mejor canal para concretar la llamada. A medida que el usuario se desplazaba físicamente, la central transportaba la señal de antena en antena, para brindar la continuidad en la conversación telefónica. (MasterMagazine, 2004)

En un inicio a telefonía móvil era comunicación únicamente a través de la voz en cualquier momento y lugar, sin embargo la evolución constante le está permitiendo ofrecer otro tipo de servicios de conectividad total, es decir, comunicación de voz, datos, imágenes, información, entretenimiento, transacciones y videos.

La evolución histórica de la telefonía móvil se puede observar en diversas generaciones, descritas a continuación.

2.1 Primera Generación

La primera generación de sistemas celulares fue diseñada y optimizada para transmisiones análogas de señales de voz de suscriptores móviles. En esta generación la interacción entre diferentes redes era raramente implementada y, en consecuencia, un suscriptor no podía usar servicios otorgados por otra red más que de la cual estaba suscrito. (Clapto, 2001)

En 1970 EU planeaba su red celular, por lo tanto, Inglaterra, Alemania y las ciudades Escandinavas, también empezaron a planear sus propios sistemas. Cada sistema utilizaba diferentes bandas de frecuencia y protocolos para la señalización entre unidades móviles y las estaciones base.

A finales de los 70's la FCC ordenó que un único estándar debería ser desarrollado antes de que las licencias para sistemas celulares fueran asignados. La EIA (Electronics Industry Association) formó un comité estándar y estandarizó el protocolo AMPS (Advanced Mobile Phone System) para EU. Este ha probado ser el más exitoso estándar análogo de todos. Las redes AMPS son ampliamente desarrolladas y pueden ser encontradas en todos los continentes.

En 1985 TACS (Total Acces Communication System) fue introducido en el Reino Unido. TACS es relativamente parecido al AMPS de Norte América. La especificación TACS original era extendida y conocida como ETACS que fue desarrollada primeramente en las regiones de Asia y Pacífico. Otros sistemas celulares que fueron desarrollados en paralelo eran: el sistema NMT (Scandinavia's Nordic mobile Telephone) el cual sería el primer sistema análogo disponible comercialmente, introducido en Suecia y Noruega; el C450 de Alemania; el NTT (Japan's Nipón Telephone & Telegraph).

La mayoría del éxito en los sistemas análogos son los estándares NMT, AMPS y TACS, los cuales aún continúan en vigencia.

2.2 Segunda Generación

Con el incremento de la demanda de teléfonos celulares en Europa, algunos fabricantes empezaron a buscar nuevas tecnologías que pudieran superar los problemas de señales pobres y desempeño.

A principios de los 90's la segunda generación de sistemas celulares móviles fue introducida. Basada en tecnología digital se introdujeron nuevas características y servicios, como la calidad de voz que fue digitalizada y ha sido mejorada a lo largo de los años hasta el punto de exceder la calidad que ofrecen los sistemas análogos FM.

Los esfuerzos de investigación fueron directamente hacia tecnologías wireless para proveer alta calidad, libre de interferencias y un mejor desempeño.

Existen cuatro estándares principales para los sistemas de segunda generación:Global System for Mobile (GSM) communications y sus derivados, Digital AMPS (DAMPS), Code Division Múltiple Acces (CDMA, IS-95) y Personal Digital Cellular (PDC), los cuales describiremos brevemente a continuación. (Saavedra, 2004)

2.2.1 GSM

La llegada de GSM (Global System for Mobile Communications) para la segunda generación de sistemas celulares fue un gran paso. GSM es un sistema abierto que fue creado debido a la necesidad de un estándar móvil común que

funcionara a través de toda Europa y el deseo de una transmisión digital compatible con datos y que pudiera contener mayor privacidad.

La introducción de las tarjetas SIM (Suscriber Identity Module) y el protocolo MAP (Mobile Application Part) permitió la interacción perfecta entre diferentes redes, permitiendo a los usuarios moverse a través del mundo. (Clapto, 2001)

Las necesidades que busca satisfacer el sistema GSM son las siguientes:

- Uso más eficiente de las bandas de frecuencias: Como respuesta se acuerda usar RF (Radio frecuencia) digital en vez de analógica.

- Mayor calidad de voz: Usando en este caso digitalización de 13 bits muestreada a 8KHz y empleando complejos codificadores de voz.

- Más confiabilidad: Eficiente control de errores durante la transmisión por aire, usando codificación por bloque para el 20% más importante de bits, seguida de codificación convencional al 70% (20% importante anterior y el 50% menos importante), dejando el restante 30% sin codificar.

- Seguridad: Necesidad de obtener una comunicación móvil libre de interferencias, sin pérdidas en la cobertura minimizando posibles inconvenientes propios de un enlace en movimiento (desvanecimiento de la señal, dispersión del tiempo).

- Mejorar el proceso de traspaso de la transmisión de una celda a otra (Handoff): Como respuesta, GSM incorpora el MAHO (Mobile Assisted Hand-Off) en que el teléfono envía constantemente datos acerca de la recepción de su celda y de las celdas vecinas proporcionando información para evaluar mejor el traspaso y hacerlo más confiable, independientemente de la velocidad del móvil. (Rappaport, 1996)

2.2.2 Digital-AMPS (D-AMPS)

D-AMPS, también conocido como US-TDMA (United States-Time Division Multiple Acces) es utilizado en América, Israel y algunos países de Asia. Este sistema es compatible con su antecesor AMPS, sin embargo éste último utiliza un canal de control analógico, mientras que US-TDMA utiliza un canal de control digital (DCCH). Una de las 12 ventajas con US-TDMA es que las unidades móviles pueden conmutar entre una operación analógica a una digital y viceversa [Selian, 2001]. Este sistema fue inicialmente definido como el estándar IS-54, pero después evolucionó a TIA/EIA-136-C. Junto con GSM están basados en el esquema de TDMA, en el cual varios usuarios comparten un mismo canal

mediante la asignación de ranuras de tiempo de la trama de datos. (Saavedra, 2004)

2.2.3 CDMA (IS-95)

Es un protocolo propuesto por QUALCOMM y estandarizado en los EU como IS-95. La idea básica que incrementó la capacidad en el estándar es el uso del canal de banda ancha, en el cual muchos usuarios con diferentes códigos digitales cada uno y un espectro extendido pueden compartir el canal al mismo tiempo sin hacer interferencia unos con otros. (Clapto, 2001)

CDMA incrementa la capacidad del sistema entre 10 y 15 veces comparado con AMPS, y por más de 3 veces comparado con TDMA, por lo que la industria reconoce a CDMA como una tecnología superior comparada con la utilizada en GSM/TDMA, sin embargo no es la más utilizada en el mundo ya que no ofrece un roaming internacional como GSM.

2.2.4 Personal Digital Cellular (PDC)

PDC es el estándar de segunda generación de Japón, anteriormente se le conocía como JDC (Japanese Digital Cellular), pero debido a su interés para dar a conocer el sistema fuera de dicho país, se le cambió el nombre a Personal Digital Cellular. Sin embargo la estrategia no trajo los resultados obtenidos ya que no hubo interés por parte de otros países y el sistema sólo se utiliza en Japón. (Saavedra, 2004)

2.3 Segunda Generación Mejorada

El término de Generación 2.5 es utilizado para referirse a aquellos sistemas que se han actualizado y mejorado respecto a las redes de segunda generación. Dichas actualizaciones proveen casi las mismas capacidades planeadas para los sistemas de Tercera Generación (3G). Sin embargo es difícil decir, en un sentido técnico, cuándo un sistema de 2G llega a ser un sistema de 2.5G. Generalmente, un sistema GSM de 2.5G incluye una o todas las siguientes tecnologías: High Speed Circuit Switched Data HSCSD), General Packet Radio Services (GPRS), y Enhanced Data Rates for Global Evolution (EDGE). (Saavedra, 2004)

2.3.1 High Speed Circuit Switched Data (HSCSD)

HSCSD es la forma más fácil de proveer una velocidad de conexión mayor. Esto significa que en lugar de utilizar sólo una ranura de tiempo, una estación móvil puede utilizar varias ranuras para una conexión de datos. En las actuales implementaciones comerciales, el máximo número de ranuras que se pueden utilizar son 4.

2.3.2 GPRS

El primer servicio de datos introducido en las redes de GSM es llamado GPRS (General Packet Radio Service), el cual asigna algunas divisiones de tiempo para el tráfico de datos. La asignación de estas divisiones provee de una capacidad de "downstream" de 115kbps y de "upstream" de 53kbps. La capacidad actual es de 40kbps. El tráfico de GPRS puede tomar divisiones de tiempo libres, o pueden dedicarse divisiones. La capacidad asignada a GPRS es compartida por todos lo usuarios en la celda. Mientras que la máxima capacidad por división de tiempo es de 21.4kbps, el estándar define cuatro niveles de codificación de corrección adelantada, por lo tanto la capacidad utilizable por división de tiempo en utilización es de 10kbps. Aun así, la capacidad es limitada por el equipo del usuario (Rappaport, 1996).

2.3.3 EDGE

EDGE es una buena alternativa económica para los operadores móviles que dejan introducir gradualmente nuevos servicios para sus abonados ya sea en forma independiente o complementaria a UMTS. El próximo paso para los operadores móviles GSM/GPRS en su camino hacia los servicios móviles de próxima generación es EDGE el cual les brinda una solución que les permite comenzar a ofrecer servicios 3G en lugar de esperar a recibir las subastas del espectro RF para lanzar UMTS. Este es un tema de importancia ya que muchos países de América latina y Europa Oriental han sufrido constantes postergaciones en el otorgamiento de licencias del espectro. Con EDGE un operador podrá elegir desplegar EDGE, y cuando el mercado se muestre claramente preparado para los servicios UMTS, podrá continuar con la evolución de su red GSM. (Saavedra, 2004)

2.4 Tercera Generación

2.4.1 IMT-2000

IMT-2000 provee una estructura para el acceso inalámbrico mundial enlazando los diferentes sistemas de redes terrestres y satelitales [UIT,2003]. Las capacidades de este estándar incluyen un amplio rango de servicios de voz, de datos y multimedia con una calidad igual o mejor que las redes de telecomunicaciones fijas en diferentes ambientes de radio. El objetivo de IMT-2000 es proveer una cobertura universal que permita a los equipos móviles tener el mismo roaming a través de múltiples redes. (Garg, 2002)

La UIT ha aprobado una serie de recomendaciones técnicas o estándares que definen las características principales de los sistemas de IMT-2000 (Saavedra, 2004).

Las características fundamentales de IMT – 2000 son:

- Gran uniformidad de diseño en todo el mundo;
- Compatibilidad de servicios dentro de IMT – 2000 y con las redes fijas;
- Gran calidad de servicio;
- Utilización de una terminal portátil en todo lugar y en todo momento;

La arquitectura de las redes de 3G está basada en dos características principales: Una es que las redes de telefonía celular móvil deben de estar estructuradas para maximizar la capacidad de la red, y la otra es la de poder ofrecer servicios multimedia independientemente del lugar donde se encuentre el usuario final. (Selian, 2003)

WCDMA y CDMA2000, basados en CDMA son los estándares de 3G que han cobrado mayor importancia para IMT-2000. (Hernández, 2003)

2.4.2 UMTS

El sistema UMTS (Universal Mobile Telecommunications System) es uno de los más destacados en tercera generación. Es planteado como evolución de los sistemas GSM (Global System for Mobile Communications) y GPRS (General Packet Radio Service), y su especificación corre a cargo del foro 3GPP (3rd Generation Partnership Project).

Uno de los principales objetivos de UMTS es facilitar el acceso a una mayor gama de servicios que sus predecesores, incluyendo el soporte de aplicaciones multimedia y, en general, de aquéllas para las que la capacidad de las actuales redes GSM/GPRS resulta insuficiente. Para la consecución de este objetivo, resulta imprescindible la adopción de tecnologías adecuadas a la naturaleza multiservicio de UMTS, capaces de satisfacer los requisitos de QoS (Quality of Service) de cada aplicación y, al mismo tiempo, garantizar el uso eficiente de los recursos de red. Estos aspectos resultan especialmente críticos en la red de acceso, por la escasez de recursos que habitualmente caracteriza a este tramo en todo sistema de comunicaciones móviles celulares.

Las especificaciones de la red de acceso radio terrestre UMTS (UTRAN) establecen el empleo de WCDMA (Wideband Code Division Multiple Acess) en la interfaz radio y de ATM1 (Asynchronous Transfer Mode) en la infraestructura de transmisión fija. La combinación de estas tecnologías sienta las bases para el despliegue de una red de acceso multiservicio con garantías de QoS. (García, Alvarez, Vázquez, Berrocal, Vinyes, 2004)

UMTS es utilizada actualmente por más de tres millones de abonados y está creciendo a mayor velocidad que GSM en el mismo punto de su historia y se espera que futuras evoluciones tales como High Speed Downlink Packet Access (HSPDA) llevarán la eficiencia espectral de datos de UMTS a más del doble e

incrementarán las velocidades de datos máximas a más de 14 Mbps. (3G américas, 2004)

2.4.3 WCDMA y CDMA2000

En WCDMA no se requiere un sincronizador en la estación base mientras que en CDMA2000 es necesario para proporcionar una disminución de la latencia y una reducción de llamadas caídas durante un handoff suave. (Hernandez, 2003)

El sistema WCDMA tiene dos modos de operación, FDD y TDD. En el modo FDD el enlace de subida y de bajada utilizan bandas de frecuencia separadas. En el modo TDD tanto el enlace de subida como el de bajada utilizan la misma frecuencia portadora. (Hernandez, 2003)

Capítulo 3. La convergencia

El problema principal de seguridad en tercera generación radica en la interacción de una red de telefonía móvil convencional con los servicios que ofrece una red IP. Esto significa que los operadores tienen la oportunidad de ofrecer mayores aplicaciones que se basan en el Internet dando lugar a lo que se conoce como Internet Móvil, una parte importante en la estructura de los servicios ofrecidos por 3G. Esto también significa que cuando la información penetre a la red pública de Internet, esta información estará expuesta a las mismas amenazas que acechan a cualquier red IP.

Para poder comprender como se da esta convergencia primero se describirá el entorno de la red de Internet para tener bases de su funcionamiento, y posteriormente se hará la explicación del Internet Móvil, el cual como se mencionó anteriormente, alberga diversas aplicaciones que interactúan activamente en el mundo de la tercera generación.

En la siguiente figura se muestra un ejemplo de la interacción de algunas partes integrantes de 3G.

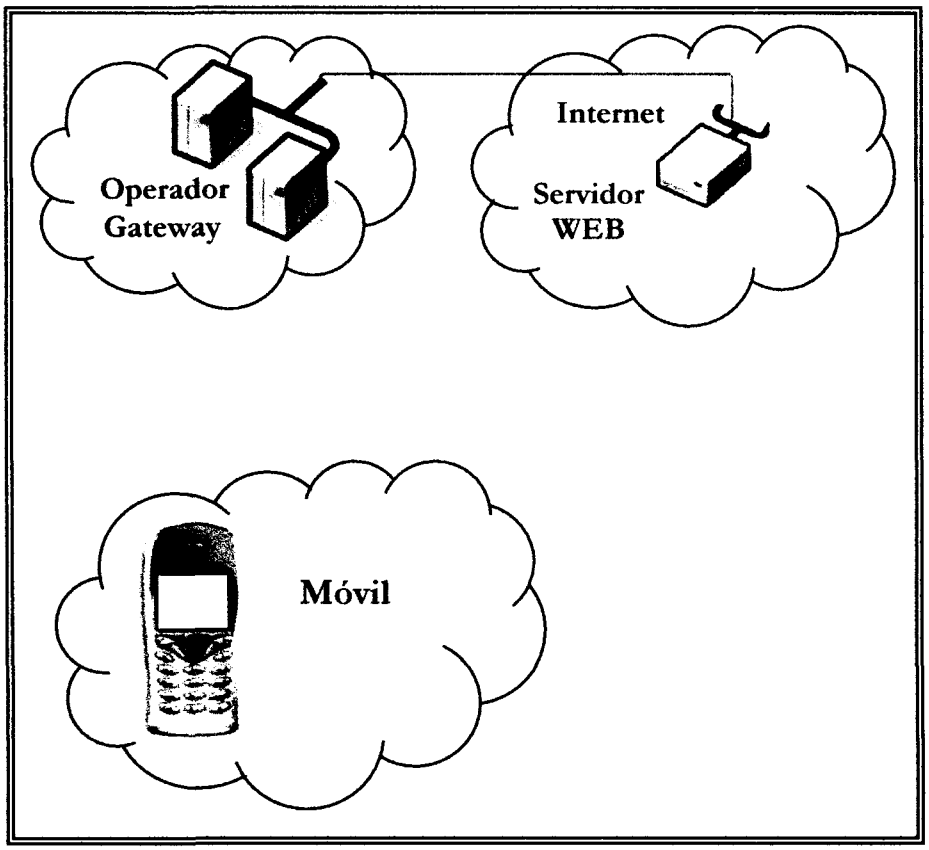

Figura 2. Interacción de algunos componentes principales de tercera generación.

3.1 Internet

Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica. (Chova, 2004)

La palabra Internet es una combinación de las palabras "International Network of Computer", lo que significa Red Internacional de Computadoras. Es una red de ordenadores conectados alrededor del mundo que ofrece diversos servicios a sus usuarios como pueden ser el correo electrónico, el chat o la web.

Todos los servicios que ofrece Internet son llevados a cabo por miles de ordenadores que están permanentemente encendidos y conectados a la Red, esperando que los usuarios les soliciten los servicios y sirviéndolos una vez son solicitados. Hay servidores para cada aplicación, los que ofrecen correo electrónico, otros hacen posible las conversaciones por chat, otros la transferencia de ficheros o la visita a las páginas web y así hasta completar la lista de servicios de Internet. (Alvarez, SF)

Internet surgió de las investigaciones realizadas por el Departamento de Defensa Nacional de los Estados Unidos en 1960. Según Hauben (1997). El primer objetivo fue la creación de una red segura para la transmisión de mensajes en tiempo de guerra. Este medio fue escogido porque permitía la redirección de los mensajes y además, podía funcionar aún si una parte estaba destruida por cualquier motivo. Para eso, se buscaba una forma de dividir los mensajes en varias partes, cada una mandada de manera independiente a fin de asegurar una confidencialidad máxima. Este método es conocido como "sistema de paquetes". (Chamero, 1999)

Las investigaciones tecnológicas militares del Advanced Research Projects Agency (DARPA), un organismo dentro del Departamento de Defensa de Estados Unidos, que durante la guerra fría en los años sesenta y setenta coordinaba el desarrollo del predecesor de Internet, llamado ARPANET, tenía el fin de establecer una estructura de información y comunicación tan descentralizada, que pudiera sobrevivir a un ataque militar. A finales de los años setenta y a partir de los ochenta se instalaban más y más redes de computadoras para usos académicos y civiles como USENET en 1979 y BITNET en 1981 en los Estados Unidos, Minitel-Téletel en 1981 en Francia, y WELL en 1985 también en Estados Unidos.

En los años ochenta NSFNET de la Nacional Science Foundation de Estados Unidos remplazó a ARPANET como columna vertebral de Internet con

velocidad superior. Después de su exitoso lanzamiento con recursos públicos, Internet se comercializó en los años noventa. El mundo reticular de computadoras consistía, según datos de la Unión Internacional de Telecomunicaciones (UIT), en el mes de agosto de 1981, en un total de 213 servidores y no más de unos miles de usuarios. Este número creció exponencialmente desde esta fecha. La UIT estima que en julio de 1999 existían ya 56 millones de servidores y 190 millones de usuarios en el mundo. (Corona, 2003)

La penetración de Internet a nivel mundial a partir del 2000 se muestra a continuación en la Tabla 1.

Regiones	Población (2004 Est.)	Usuarios, (año 2000)	Usuarios,dato más reciente	Crecimiento (2000-2004)	% Poblacion (Penetracion)	(%) de Usuarios
Africa	893,197,200	4,514,400	**12,937,100**	186.6 %	1.4 %	1.6 %
Asia	3,607,499,800	114,303,000	**257,898,314**	125.6 %	7.1 %	31.7 %
Europa	730,894,078	103,096,093	**230,886,424**	124.0 %	31.6 %	28.4 %
Oriente Medio	258,993,600	5,284,800	**17,325,900**	227.8 %	6.7 %	2.1 %
Norte America	325,246,100	108,096,800	**222,165,659**	105.5 %	68.3 %	27.3 %
Latinoamerica / Caribe	541,775,800	18,068,919	**55,930,974**	209.5 %	10.3 %	6.9 %
Oceania	32,540,909	7,619,500	**15,787,221**	107.2 %	48.5 %	1.9 %
TOTAL MUNDIAL	**6,390,147,487**	**360,983,512**	**812,931,592**	**125.2 %**	**12.7 %**	**100.0 %**

Tabla 1. Estadísticas Mundiales de Internet con respecto a la Población, fuente. www.ExitoExportador.com, Nielsen//NetRatings, ITU, NIC's, ISP's y otras fuentes confiables

3.1.1 Funcionamiento

Como lo afirma el director de Cisco, Howard Charney (2001), "nadie controla la Internet, no está ubicada en un lugar en particular ni dirigida por una sola persona, es una red hecha de millares de redes que se encuentran por todo el mundo, gobernada a la vez por miles de personas".

La tecnología básica que utiliza Internet se denomina conmutación de paquetes. Este concepto evolucionó a partir de otros anteriores a los que solía unirse bajo el término conmutación de mensajes. A diferencia de las redes telefónicas, en las que los dispositivos (por ejemplo teléfonos y aparatos de fax) se conectan mediante circuitos conmutados de extremo a extremo que permanecen en su sitio hasta que finaliza la comunicación, los sistemas de conmutación de mensajes y de paquetes envían unidades de información (mensajes y paquetes respectivamente) que funcionan a modo de "postales electrónicas": un ordenador

genera una postal que envía a otro ordenador de la red. Ésta se va reenviando de un ordenador a otro hasta llegar a su destino.

Los enlaces de comunicación que interconectan los ordenadores están dedicados a pares de ordenadores concretos, y las postales electrónicas se reenvían a través de estos canales. Así, los paquetes y mensajes ocupan los canales de transmisión sólo durante el tiempo que están circulando por ellos, e inmediatamente después éstos vuelven a estar disponibles para transportar otros paquetes o mensajes una vez los primeros han atravesado el enlace entre los ordenadores. A los ordenadores que reenvían paquetes a través de Internet se los denomina routers. (Cerf, 2004)

Todos los equipos que están conectados a Internet deben emplear el mismo lenguaje para comunicarse, estos lenguajes de comunicación entre ordenadores se llaman protocolos. El lenguaje de Internet es el denominado TCP/IP y está formado por dos protocolos o niveles de comunicación. (Baluma, 2001)

Ya que este es el protocolo común utilizado por todos los elementos conectados a Internet, de manera que éstos puedan comunicarse entre sí, hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible ya que es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. (Soto, SF)

IP, es el mecanismo básico por el cual los paquetes de Internet se envían por toda la red. TCP transmite secuencias de datos entre los ordenadores conectados a Internet descomponiéndolas en paquetes de Internet y enviándolos a su destino mediante el Protocolo de Internet utilizando un sistema de almacenamiento y reenvío a través de la red.

Internet está diseñado para que un número aleatorio y elevado de redes puedan interconectarse y funcionar de manera independiente. Todas las redes cuentan con los mismos estándares en cuanto a protocolos de comunicación se refiere, y son estos estándares los que permiten que Internet funcione como una enorme y (aparentemente) uniforme colaboración de cientos de miles de redes públicas y privadas. (Cerf, 2004)

3.1.2 Arquitectura

3.1.2.1 Acceso

La conexión de un usuario cualquiera a Internet se produce mediante una **red de acceso**, controlada y administrada por un Proveedor de Servicios de Internet (PSI o **ISP**, Internet Services Provider). El acceso en sí se puede producir mediante el empleo de tecnologías diversas, como la Red Telefónica Básica (RTB), la Red Digital de Servicios Integrados (RDSI), la Línea Asimétrica Digital de Abonado (ADSL, Asymetric Digital Subscriber Line) o líneas dedicadas tipo X.25, Frame Relay, etc. Por regla general, el precio del acceso es función del tiempo de conexión y de la velocidad de transmisión ofrecida. En la tabla 2 se muestra una comparación orientativa de las velocidades de acceso proporcionadas por algunas tecnologías. (VADEMECUM, 2002)

Tecnología	Velocidad de acceso
RTB	Hasta 56 kbps
RDSI	64-128 kbps
ADSL	Hasta 2 Mbps
Frame Relay	64 kbps – 2 Mbps
X.25	300 bps – 2 Mbps

Tabla.2: Comparativa de velocidades de acceso de distintas tecnologías

El Proveedor de Servicios, una vez establecida la conexión, asigna una dirección IP a la máquina que se conecta, de forma que quede completamente visible para el resto de máquinas de Internet.

3.1.2.2 Tránsito

La red de acceso del ISP se conecta a los grandes backbones de tránsito de Internet, operados casi en su totalidad por compañías privadas. Estas redes ofrecen un servicio de interconexión global entre ellas y con otros ISP, alcanzándose de esta forma un mallado mundial. Entre las redes de acceso y tránsito existen tres tipos de relaciones, que definen la arquitectura general de Internet:

- **Clientes**. Los pequeños ISP son clientes de los grandes proveedores, anunciándoles la información necesaria para alcanzar a los usuarios que acceden a través de sus redes.

- **Proveedores.** Las grandes redes globales proveen a los ISP de un servicio de interconexión con otros ISP del mundo.

- **Peers**. Algunos ISP de tamaño mediano y grande se interconectan directamente para intercambiar información de direcciones IP sin que intervenga un proveedor de tránsito. De esta forma se consigue una mayor rapidez al acceso de los contenidos dentro de una determinada zona geográfica, como un país o un continente. De la misma forma, los proveedores de tránsito mantienen una relación de "peering" entre ellos para el intercambio de información IP. Las relaciones de peering pueden ser mediante enlaces directos o mediante puntos de interconexión públicos (IX, Internet Exchanges). (VADEMECUM, 2002)

En la figura 3 se muestra una visión general de la arquitectura de Internet y el tipo de relación entre las distintas redes que la componen.

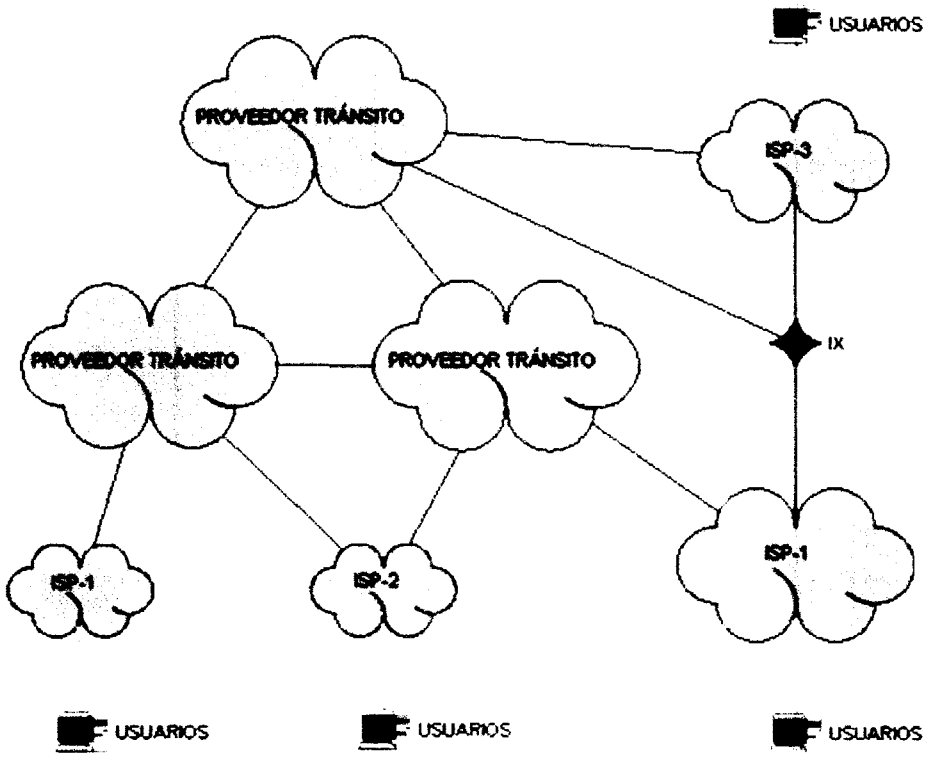

Figura 3: Arquitectura de interconexión global de Internet

Cualquier red que se interconecte con otras para formar la Internet y que esté bajo un mismo dominio administrativo conforma lo que se denomina sistema autónomo (AS, Autonomous System), y se identifica con un número específico asignado por los organismos reguladores de Internet. En la figura 3, todos los ISP

y proveedores se identificarían con su propio número de sistema autónomo. (VADEMECUM, 2002)

3.2 Internet Móvil

Tener la información en la punta de los dedos es uno de los grandes logros que ha traído la revolución tecnológica por la que hemos transitado en las últimas décadas. Aunque lo anterior es sólo cierto en la medida que nuestros dedos estén cerca de una computadora, normalmente, sobre un escritorio. Sin embargo, basta con que el propietario de esos dedos salga a caminar para que se corte todo alcance oportuno a la información. De ahí la importancia que hoy están adquiriendo los avances que se dan en el ámbito de 3G, donde a través del Internet Móvil, los usuarios accesan a diversas fuentes de información. (Publicaciones EMB, 2003)

Es importante entender el funcionamiento del Internet Móvil, para comprender las aplicaciones que los operadores de telefonía ofrecen a los usuarios en tercera generación.

Internet Móvil es un sistema de comunicación ideal que, al igual que Internet y la Telefonía Móvil en sus inicios, indicará el futuro rumbo de las comunicaciones y determinará la forma en que los agentes económicos intercambiarán bienes y servicios en la nueva economía. De la validez de estas perspectivas están persuadidas las operadoras de telefonía móvil, las cuales dedican sus mayores esfuerzos al desarrollo de servicios y aplicaciones para Internet Móvil. (Tendencias Digitales, 2004)

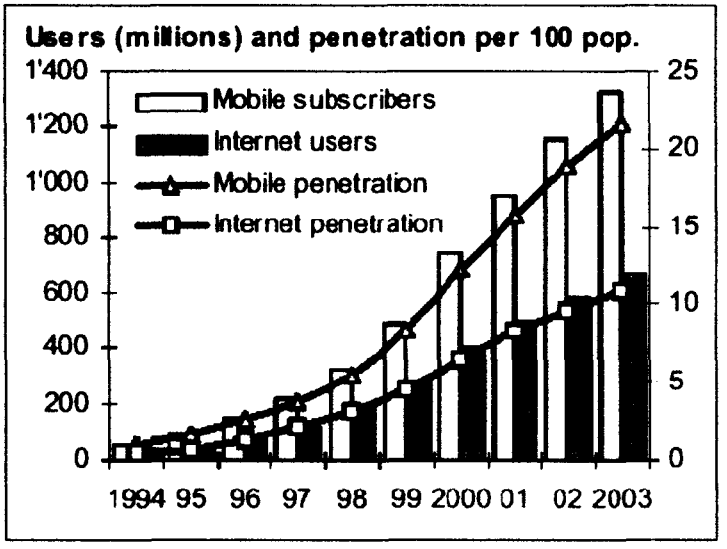

Figura 4. Penetración de Internet y de Internet Móvil
Fuente: Base de Datos de indicadores mundiales de la ITU

En la figura 4 se muestra la penetración del Internet Móvil en comparación con el Internet hasta el año 2003. A principios del 2004 se identificaron 1,320 millones de usuarios de celulares y 665 millones de usuarios móviles. (Hernández, 2004)

Si bien es cierto que los clientes podrán realizar múltiples operaciones que van desde consultar sus cuentas bancarias, transferir fondos instantáneamente o acceder a información sobre viajes, tal como lo hacen hoy día desde sus equipos de computación. Todo ello motivado por abaratamiento de costos y ahorro de tiempo, consecuencias naturales de la aplicación de nuevas tecnologías.

La seguridad inalámbrica también será un asunto que los proveedores de esta tecnología están obligados a tomar en cuenta para combatir a los posibles hackers inalámbricos que aparezcan. Para enfrentar con éxito esta amenaza, son muchas las apreciaciones que el personal de TI debe considerar al migrar entre el mundo inalámbrico (wireless) y el mundo cableado, toda vez que la gran mayoría de errores de seguridad que se han cometido se deben a la falta de estrategias y planeación adecuada de las diversas topologías de comunicación que se han establecido.

El proveedor de servicios de comunicaciones inalámbricas que considere esto como una prioridad dentro de su estrategia, puede llevar la delantera en un mercado cada vez más exigente, que entiende la importancia de la seguridad en la red y de blindar sus transacciones. Sin embargo, muchos son los retos pendientes para que esta nueva plataforma tecnológica realmente logre cubrir todas las expectativas de la mejor manera posible y al menor costo. (Tendencias Digitales, 2004)

3.3 Arquitectura para tercera generación

A continuación se detallan los distintos componentes que constituyen la infraestructura básica sobre la que construir el conjunto de servicios que forman la tercera generación (ver la Figura 5). Se distinguen varios tipos de componentes (Chamorro, Mercado, Núñez, Gómez, 2001):

1. **Los medios y pasarelas de acceso**. Constituyen el punto de entrada de los usuarios al sistema y existe un componente para cada tecnología utilizada en el acceso.

2. **Los servidores.** Consiste en un conjunto de sistemas, cuya labor es la de prestar servicios internos de traducción, autenticación, información de sesiones, información de localización, etc., sobre los cuales se apoyan los servicios de 3G que se ofrecen a los usuarios.

3. **Los servicios.** Forman la parte final de la cadena de la provisión de servicios de 3G. En ellos residen los servicios, los contenidos y la

información que se distribuye, mediante algún tipo de medio o pasarela de acceso, hacia los usuarios de tercera generación.

4. **Las plataformas de gestión.** Forman el entramado para la gestión del equipamiento de red y de los servicios, así como de la gestión de los clientes; siendo necesario para que una operadora pueda prestar de forma eficiente los servicios de 3G.

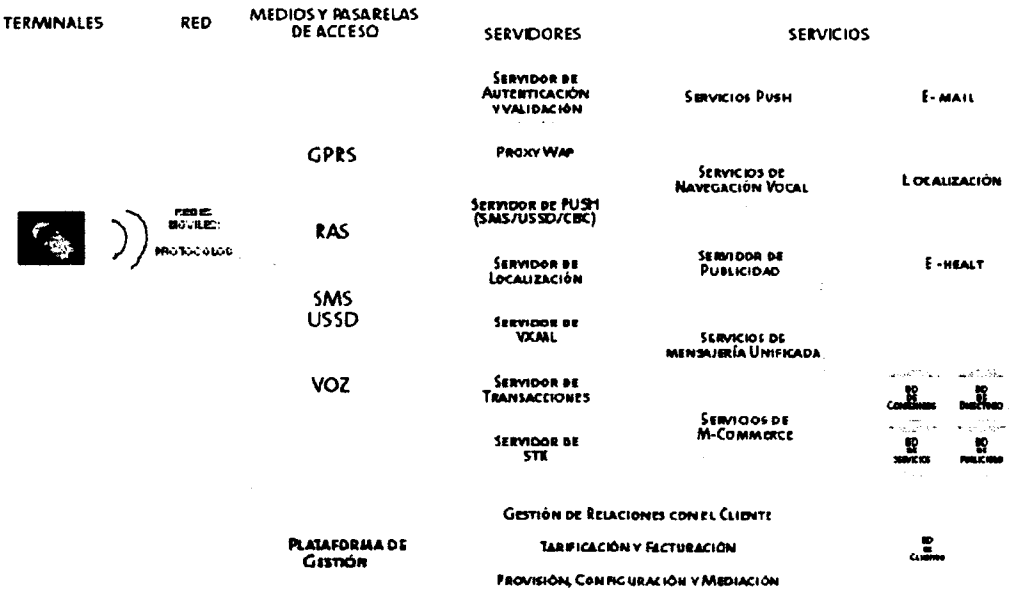

Figura 5. Componentes de tercera generación

3.3.1 Aplicaciones

El Internet Móvil como base de 3G forma un nuevo modelo para negocios y usuarios de las comunicaciones. Para conocer las necesidades dinámicas de éste nuevo ambiente de datos móviles, los desarrolladores están creando una nueva generación completa de aplicaciones de servicios. (Steinbock, Noam, 2003)

A continuación se describen algunas de las aplicaciones:

- Servicios PUSH
- Navegación Vocal
- Publicidad
- Mensajería unificada
- M-Commerce
- E-mail
- Localización
- M-health

3.3.1.1 Servicios PUSH

Este tipo de servicios, así como los servicios de alertas, los ofrece una plataforma de alta escalabilidad que facilita el acceso a los contenidos publicados por algún proveedor de información bajo demanda del cliente, mediante el envío de un mensaje de texto.

Esta plataforma integrará tanto contenidos propios, gestionados localmente, como contenidos externos, recogidos directamente de los proveedores de información en un formato de intercambio predeterminado (XML, WML, HTML, etc., y utilizando múltiples protocolos de transferencia como HTTP, FTP, etc.), y compatibilizará las peticiones de información recibidas on-line (reenviándolas adecuadamente al proveedor) con el envío de aquellos mensajes programadas por el usuario, para que se le envíe cierta información cuando se produzca o el proveedor lo notifique al servicio (servicio de alertas preprogramadas).

Para un mayor aprovechamiento del potencial de este tipo de servicios, es necesario implementar una gestión flexible de los distintos canales de contenidos, así como dar soporte a la personalización de los contenidos por parte del usuario. La entrega de la información se realiza empaquetándola en uno o varios mensajes de texto, existiendo la posibilidad de enviar mensajes gráficos (texto + imagen), si el terminal móvil del usuario lo soporta, concatenar varios mensajes, de forma transparente al cliente (superando la limitación de los 160 caracteres), e incluso utilizar otro tipo de facilidades de que comienzan a disponer los terminales, como la descarga de menús dinámicos (DMCP) o los lenguajes de hipertexto (TTML). (Chamorro, Mercado, Núñez, Gómez, 2001)

3.3.1.2 Navegación Vocal

El acceso a contenidos o aplicaciones de Internet también se puede realizar mediante la interfaz más natural que poseemos los humanos: la voz. Con dicho objetivo se puede utilizar un lenguaje llamado VoiceXML, el cual, es un lenguaje estándar basado en marcas, subconjunto de XML, diseñado para describir interacciones vocales. La utilización de este lenguaje permite definir aplicaciones y contenidos de forma muy similar (aprovechando, por tanto, los conocimientos y la tecnología previa) a como se hace mediante el lenguaje HTML, en el cual se basa la navegación por la Internet fija.

Para ir accediendo a los contenidos, es necesaria en Internet Móvil una aplicación capaz de interpretar las páginas VoiceXML e ir realizando las interacciones con el usuario. Esa aplicación que constituye la interfaz vocal con el usuario es un navegador VoiceXML.

El Navegador proporciona al cliente los contenidos, mediante voz sintetizada a partir de texto (Text to Speech) o mediante reproducción de archivos de audio, y recibe del cliente comandos, o entradas de datos, mediante recepción

de tonos DTMF, reconocimiento de voz (palabras aisladas o palabras en contexto de frase -word spotting) o grabación de voz. También permite otras funcionalidades que proporciona la red telefónica, tales como la transferencia de llamadas, las desconexiones, etc.

Dadas las diferencias entre la interacción mediante WAP o HTML y la interacción vocal, idealmente las aplicaciones y contenidos vocales deben ser estructurados y estar concebidos con tal fin. Sin embargo, también es posible reaprovechar contenidos ya existentes, bien directamente de los proveedores de contenidos (mejor opción) o bien de las páginas ya existentes HTML o WML.

Esta última labor, debe realizarse mediante herramientas de extracción de contenidos; esto es, herramientas que son capaces de reconocer la estructura de una página HTML o WML, y son capaces de procesar dichas páginas para obtener las partes significativas y generar páginas VoiceXML con dichos contenidos. (Chamorro, Mercado, Núñez, Gómez, 2001)

3.3.1.3 Publicidad

Las plataformas de publicidad permiten ofrecer servicios de inserción de publicidad en el entorno de 3G. Las plataformas de inserción de publicidad se originaron en el entorno web y consisten, básicamente, en plataformas software que realizan las siguientes funciones: (Chamorro, Mercado, Núñez, Gómez, 2001)

- **Almacenar la información de las campañas publicitarias de los anunciantes.** En estas campañas se define el targeting de la inserción de publicidad, es decir, el conjunto de criterios que se deben cumplir para que un anunciante desee ofrecer su publicidad a un cliente.

- **Pronosticar la cantidad de espacio publicitario disponible que un portal de Internet va a permitir ofrecer.** De esta manera se obtiene un inventario de espacios publicitarios disponibles, que permitirá definir cuánto y cuándo habrá sitio disponible para insertar más publicidad.

- **Recibir, dinámicamente, cuando se produce la descarga de una página, la petición de un contenido publicitario.** A partir de esta petición, la plataforma realiza la selección del contenido que mejor se ajuste a las características del cliente al que se va a servir, utilizando toda la información disponible. Al mismo tiempo, el sistema lleva a cabo la anotación del contenido que se sirve, para posteriores usos de facturación y estadísticas.

- **Almacenar información estadística y generar informes, para el seguimiento por parte de los anunciantes del éxito de sus campañas.** El éxito se mide según el número de impresiones (número de veces que un anuncio se muestra al cliente) y el número de veces

que un cliente sigue el enlace correspondiente con un anuncio publicitario.

En el entorno de tercera generación, los medios susceptibles de admitir contenidos publicitarios son: contenidos WAP, mensajes cortos y contenidos Web. Dentro de estos medios los servicios, en los que se puede considerar la inserción de publicidad, son: acceso y navegación por contenidos Web o WAP, alertas y notificaciones SMS y comunicación personal con SMS.

Así, para el entorno Web, los servicios publicitarios se centran en la inserción de banners en páginas, que pueden ser seguidos para alcanzar la Web del anunciante. Este modelo es extrapolable al entorno WAP, con los wanners (WAP-banners), con el mismo propósito.

En el servicio de mensajes cortos, los servicios de inserción de publicidad se centran en la adición de publicidad a alertas, notificaciones o mensajes personales y en servicios promocionales; consistentes en la difusión de mensajes, con fines exclusivamente publicitarios, a un conjunto de clientes que comparten alguna característica que los hace objeto de interés para el anunciante. (Chamorro, Mercado, Núñez, Gómez, 2001)

3.3.1.4 Mensajería unificada

La mensajería unificada se define como el conjunto de servicios que permite enviar y recibir cualquier tipo de mensaje (voz, e-mail, SMS y Fax) a través de cualquier método de acceso (teléfono por voz, teléfono por SMS, teléfono por WAP, PC a través de HTML, PDAs, etc.). (Chamorro, Mercado, Núñez, Gómez, 2001)

Los servicios que debe ofrecer una solución de mensajería unificada completa son:

- Buzón unificado, en el que se almacenen e-mail, mensajes de voz, fax, mensajes cortos, imágenes, vídeo, música, etc.

- Acceso al buzón unificado, mediante diferentes tipos de interfaz de usuario: voz desde teléfono fijo o móvil, PC y PDA (usando protocolos POP, IMAP y HTTP), teléfono móvil por WAP, teléfono móvil por SMS, fax, etc.

- Envío de mensajes al buzón, tales como: mensajes de voz desde teléfono móvil o fijo, e-mail (desde PC, PDA o teléfono móvil), fax desde máquina de fax y mensajes cortos (desde PC, PDA o teléfono móvil).

3.3.1.5 M-Commerce

El m-commerce es el paso siguiente en la evolución del e-commerce y puede resumirse en "la venta de servicios de datos y productos a través de terminales móviles". En realidad, la infraestructura para las soluciones m-commerce no difiere significativamente de las necesarias para el e-commerce, salvo en que se ofrece un servicio a un nuevo tipo de terminales. E-commerce ofrece acceso a cualquiera, sobre cualquier dispositivo y en cualquier momento; el m-commerce añade "en cualquier lugar".

El m-commerce añade valor al e-commerce, dotándolo de movilidad y acceso desde múltiples terminales además de proporcionar nuevas vías para la captación de clientes, y permitir retener clientes actuales de los servicios de e-commerce. Los campos de aplicación del m-commerce son muy diversos. (Chamorro, Mercado, Núñez, Gómez, 2001)

Algunos ejemplos de ellos son:

- **Transacciones bancarias.** Son los servicios proporcionados en la actualidad por los bancos en/a través de Internet, permitiendo a los usuarios usar firmas y certificados digitales para:

    a) Obtener información de cuentas personales (extractos, saldos, etc.).
    b) Transferir fondos a cuentas bancarias.
    c) Recibir notas de alerta sobre información bancaria sensible para el usuario.
    d) Gestionar pagos de facturas electrónicas, en diferido, especiales, etc.
    e) Líneas de crédito.

- **Operaciones de bolsa:**

    a) Información sobre cotizaciones.
    b) Gestión de la cartera de acciones (compra/venta).

- **Billetes (e-ticketing).** Reserva, compra del billete, facturación, pago y acuse de recibo, que pongan a disposición otras empresas como compañías de transportes, parques temáticos, empresas de espectáculos, etc.

- **Compras.** Posibilidad de realizar los mismos procesos, existentes en Internet, de comercio electrónico a través de los dispositivos móviles. Estas funcionalidades ya están disponibles en portales y tiendas virtuales. Ejemplos de estos servicios serían:

a) Búsqueda de productos.
b) Selección de productos.
c) Avisos.
d) Pedidos.
e) Seguimiento de pedidos.

- **Juegos y apuestas.** Este es un campo no del todo desarrollado en Internet, que se compenetra perfectamente con los servicios de comercio electrónico hasta ahora comentados.

3.3.2 Aplicaciones del análisis

Las aplicaciones elegidas para el estudio de la tesis son E-mail, Localización y M-Health descritas más adelante. La razón por la que se han escogido estas aplicaciones en particular, se debe a lo siguiente:

- **E- mail:** El servicio de e-mail es una de las aplicaciones clásicas con mayor auge en el mercado como se demuestra en la figura 6, por lo tanto es de gran importancia el impacto en el negocio que causaría un ataque a su seguridad. Los problemas de seguridad que se enfrentan es este servicio son tradicionales ya que es una aplicación bastante conocida.

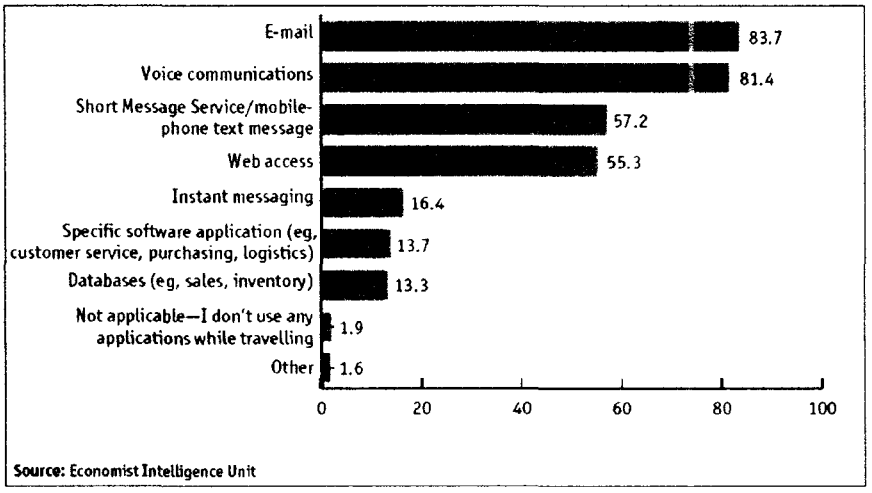

Figura 6. Aplicaciones más usadas

- **Localización:** Esta aplicación representa uno de los servicios más novedosos ofrecidos por las redes de tercera generación. Además es una aplicación diferente y con mayor valor agregado con respecto a los servicios convencionales prestados en las generaciones anteriores, y por esto mismo, en el futuro puede resultar una aplicación de gran popularidad tanto para los operadores como para los usuarios.

- **M-Health**: Esta aplicación resulta de gran interés y aunque no podemos decir que sea un servicio propio de la tercera generación, su arquitectura para el propósito de esta tesis resulta muy interesante, ya que el acceso se realiza a través de 3G. Este es un ejemplo claro de aplicaciones que, a pesar de no ser propiamente pertenecientes a tercera generación, la utilizan como base para ser montada.

Una razón importante del porqué se seleccionan únicamente tres aplicaciones, es que el análisis de todos los servicios que pueden ser ofrecidos en tercera generación puede resultar excesivamente tardado.

3.3.2.1 E-mail

El correo electrónico o e-mail es, actualmente, una de las mejores maneras de mantenerse en contacto no sólo con amigos, sino que es también un método para estar al día y a la vanguardia en los negocios. Las mayores innovaciones con respecto este servicio son las que atañen a la tecnología móvil, ya que, el e-mail es de las herramientas que más debe tenerse a la mano, y es por eso que toda la nueva tecnología cibernética móvil hace especial énfasis en su uso. (Iza, 2000)

Este es uno de los servicios que más han revolucionado al mundo ya que la vida se facilita considerablemente, por ejemplo, en cuanto a los memorandos en las empresas, ahora no es necesario ir de lugar en lugar repartiéndolos, con tan sólo enviar un mail, el problema queda resuelto.

Es importante considerar que, siempre y cuando se cuente con las prevenciones de costumbre, como tener un antivirus en perfecto estado, la seguridad del correo electrónico quedará garantizada. (Iza, 2000)

Existen varias formas de recibir un e-mail en un dispositivo móvil. Esto es hecho con el uso de aplicaciones y la tecnología subyacente que hace esto posible. Con servicios de e-mail basados en Web, un browser es usado para accesar a la interfase del e-mail en el dispositivo móvil. Con una implementación de e-mail cliente servidor la interfase del usuario es proveída por el cliente de e-mail, el cual interactúa con un servidor de correos para mandar y recibir mensajes de correos. Esto es similar a los clientes de correos usados en una PC como Microsoft Outlook. (Nokia, SF)

En algunos clientes de e-mail, los correos son automáticamente recuperados cuando el e-mail es recibido. En otros clientes de correo los usuarios deciden cuando y cada cuanto el correo debe ser recuperado

En la siguiente figura se muestra el flujo de información para esta aplicación de forma general o resumida.

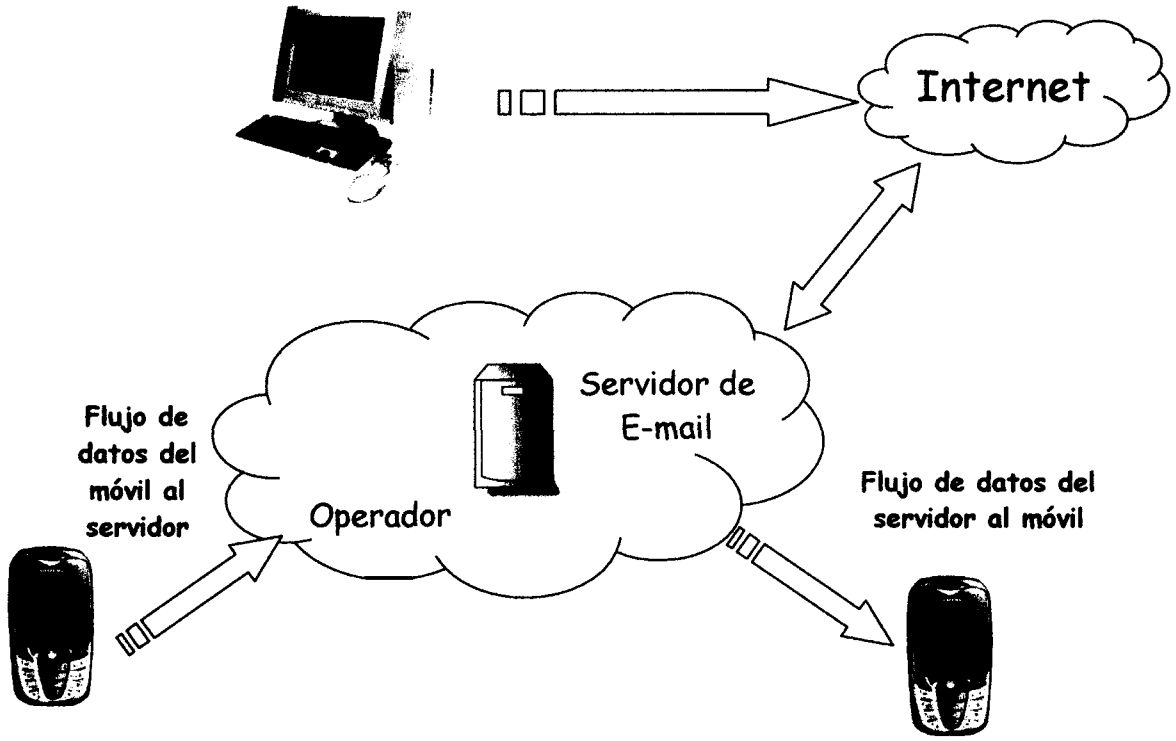

Figura 7. Flujo de información para el E-mail

3.3.2.2 Localización

Los servicios basados en la localización son aplicaciones móviles que relacionan el contenido del mensaje con la posición estimada del terminal, de forma que aporten un valor añadido al usuario final. (Voces, 2003)

La localización es un tema de gran interés para los operadores de la red móvil, por la gran cantidad de aplicaciones y servicios que se pueden ofrecer a los usuarios basados en la posición desde la que se efectúa la llamada. (Aranda, del a Paz, Berberana, González, 2001)

En la figura 8 se representa en general el flujo de información para los servicios basados en localización.

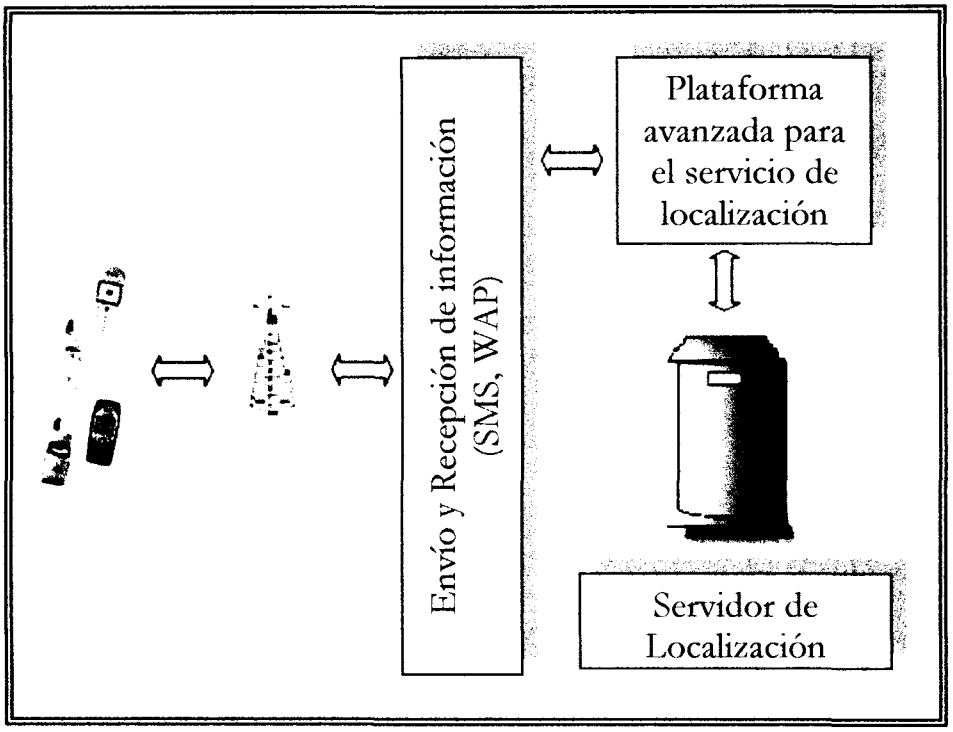

Figura 8. Flujo de información general de los servicios basados en localización

Los servicios de telefonía móvil basados en localización pueden ser divididos en varias categorías que permiten al operador diferenciarse de sus competidores, proveyendo servicios de última generación, fidelizando e incrementando el número de clientes. (Voces, 2003)

Básicamente existen cuatro tipos de servicios de localización móvil:

- **Servicios por activación automática (Trigger Services):** se inician cuando el usuario entra en un área determinada. Son adecuados para aplicaciones publicitarias o de facturación. (Bernardos, 2003)

- **Servicios de información basados en la posición (Location-based Information Services):** el usuario del servicio demanda información de algún tipo, que varía según su posición. Muchos de ellos permiten encontrar establecimientos cercanos al demandante de información, por ejemplo farmacias, restaurantes, cines y cajeros automáticos entre otros.

- **Servicios de seguimiento por terceros (Third Part Tracking Services):** contemplan tanto aplicaciones corporativas como de consumidor, donde la información de la localización es requerida por un tercero (amigo, familiar, empresa, etc). Se pueden utilizar para

gestión de flotas, búsqueda de personas, información bursátil y asesoramiento rápido por mencionar algunos.

- **Servicios de asistencia al usuario final (End User Assistance Services):** están diseñados para proveer al usuario de unas condiciones de red segura si éste se encuentra en dificultades. Servicios de asistencia en carretera u otros servicios de emergencia están dentro de este grupo. (Bernardos, 2003)

Los operadores móviles deben facilitar la creación de aplicaciones por desarrolladores independientes a través del desarrollo de herramientas de creación de servicios además, deben basar su estrategia en la coordinación entre los desarrolladores y los distribuidores de aplicaciones de localización. (Voces, 2003)

En Estados Unidos existen normas que obligan a que los centros de llamadas de emergencias determinen la localización desde donde la llamada es hecha. Europa se encuentra en un momento donde el número de llamadas a centros de emergencia esta creciendo desde terminales móviles y la necesidad de conocer desde donde se originan dichas llamadas está aumentando considerablemente. Por esta razón la Unión Europea creó una directiva que estipula que los miembros de la comunidad europea deben obligar a los operadores móviles a especificar la localización de una móvil al número 112 Europeo de emergencia.

Los servicios basados en posicionamiento móvil ya cuentan con aplicaciones en mercados tanto europeos como asiáticos, algunos ejemplos son:

En Francia, la compañía de móviles Orange ofrece tres grupos de servicios de localización móvil:

- "A proximité", un servicio que señala puntos de interés e información sobre eventos.

- "Chat", un servicio que permite a los usuarios, que se encuentran en áreas cercanas, intercambiar mensajes cortos.

- "Juegos basados en localización"- incluye el Mushi, un animal virtual que puede ser visto en un terminal móvil en la misma localización en varias ocasiones.

Otros juegos han sido testados e implementados en diversas ocasiones, incluyendo Geoquest, "la caza del tesoro", donde ciertas respuestas a preguntas sólo se pueden enviar desde específicas localizaciones.

Telia en Suecia es uno de los pioneros en esta área, el primer servicio fue lanzado en el año 2000. Aunque ofrece el mayor portafolio de servicios, 13, todavía no ha conseguido que sean de uso masivo. Algunos de ellos son:

- Siete servicios de localización.
- Dos servicios patrocinados por la administración general de correos y un distribuidor.
- Dos servicios de seguimientos de flotas.
- Un servicio de encuentro de amigos (Openwave´s Friend Zinder). Un juego (Bothfighters by It´s Alive).

En Corea del Sur, SK Telecom tiene diversos servicios de localización, todos ellos son realizados vía WAP, algunos de ellos son: (Voces, 2003)

- Un servicio de encuentro de amigos, que permite al usuario localizar de común acuerdo a sus compañeros en un rango de un kilómetro.
- Un servicio de "auto-localización", permite enviar al usuario un mapa mostrando su localización y acompañándolo de un mensaje a otro usuario móvil.
- Información sobre la localización de puntos de interés y ocio.
- Un servicio que ofrece información de la localización de las paradas de autobuses que se soliciten.

Se cobra por cada petición de posicionamiento. En Corea del Sur, además las llamadas a los servicios de urgencia son localizables, y algunos coches van equipados para el envío automático de su posición a su compañía de seguros en caso de accidente.

Otro tipo de ventajas que pueden ofrecer los servicios de localización se observan en el entorno empresarial, por ejemplo para compañías dedicadas al control y gestión de flotas, distintos tipos de mensajerías, ambulancias, taxis o alquiler de maquinaria agrícola. (waymovil, 2002)

También resulta especialmente útil para empresas que cuentan con una importante fuerza en su departamento comercial y, en definitiva, para todas aquellas que cuentan con un determinado tipo de trabajadores, como comerciales o personal técnico, que realizan su labor profesional fuera de las instalaciones de la propia compañía. Para ellas es tremendamente útil conocer la ubicación y poder localizar a sus empleados en cualquier momento y con gran exactitud, con lo que se obtiene un mejor control del personal y por lo tanto una mayor optimización de los tiempos de trabajo.

Ciertamente los servicios basados en localización móvil ofrecen grandes ventajas, sin embargo, existen también riesgos que los operadores deben tomar en cuenta al desarrollar sus aplicaciones, los principales peligros atentan contra la intimidad de los usuarios, algunos de ellos pueden ser: (Arregocés, 2003)

- La localización de una persona en contra de su voluntad.
- Una persona puede suplantar al dueño del móvil, activando con el operador el servicio de localización para tenerlo controlado.
- Se pueden crear historiales de todos los sitios en los que ha estado una persona.

A pesar de todas las aplicaciones interesantes, los operadores deben tomar en cuenta el interés de los usuarios, si les interesa que se sepa dónde se encuentra a cada momento. Esta decisión debe depender de cada persona, es el propio usuario el que tiene que dar permiso para que lo localicen y el que controla quiénes lo hacen y las horas en las que se activa el servicio. (Arregocés, 2003)

3.3.2.3 M-Health

El tiempo y el espacio constituyen barreras entre los proveedores del cuidado de la salud (health-care) y sus pacientes y entre los proveedores mismos. Los pacientes en áreas rurales, en escenas de accidentes, en un submarino, etc., están la mayor parte del tiempo lejos de un apropiado proveedor del cuidado de la salud. Las telecomunicaciones se han presentado como una poderosa herramienta para eliminar estas barreras. Con la introducción de la banda ancha y las comunicaciones digitales, es posible enviar audio, video y datos cuando y como se necesite. (Tachakra, Wang, Istepanian, Song 2003)

La industria del cuidado de la salud puede ser mejorada al adoptar dispositivos y aplicaciones inalámbricas, las cuales pueden proporcionar mejoras en la exactitud de los datos, reducir errores y resultar en una mejora del cuidado de los pacientes. De acuerdo a un estudio realizado por la Asociación de Evaluación de Tecnología, se espera que el número de dispositivos en el cuidado de la salud se triplique en el 2005.

Los beneficios de la tecnología inalámbrica se pueden ilustrar con diversos ejemplos. La información de los pacientes puede ser obtenida por los profesionales del cuidado de la salud desde cualquier localización ya que pueden estar conectados a los sistemas de información de la institución. Los médicos accesan a los historiales de los pacientes, resultados de laboratorios e información farmacéutica, entre otros. La Telemedicina Móvil (M-Health) es una nueva y evolucionante área de la telemedicina que explota los recientes desarrollos en redes Móviles para diversas aplicaciones.

En la figura 9, podemos observar el flujo de información general para M-Health.

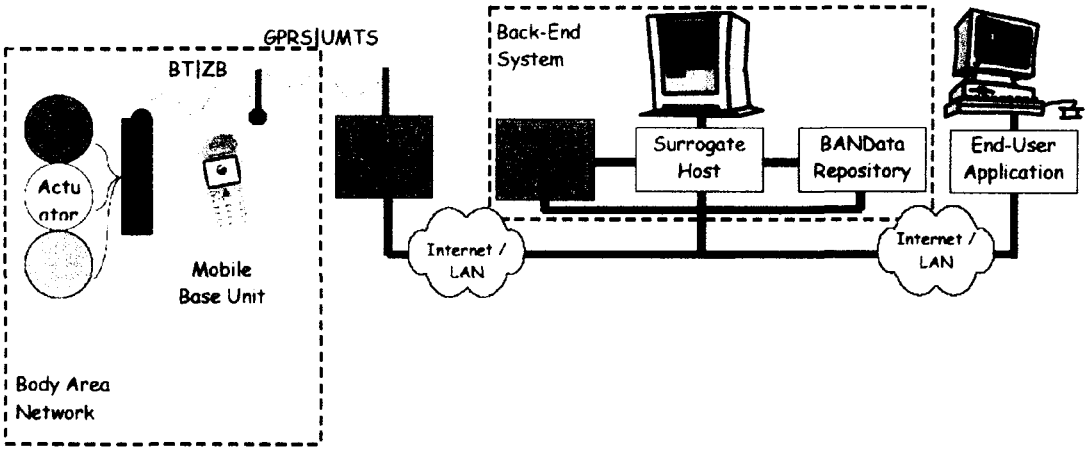

Figura 9. Flujo de información típico para M-Health

Aunque las nuevas tecnologías en telecomunicaciones móviles emergieron recientemente, sus ventajas para enviar la información vía multimedia en grandes cantidades, son observadas por el sector del cuidado de la salud. El M-Health no está muy lejos, como se muestra en los siguientes ejemplos.

- **MobiHealth**

MobiHealth es un proyecto fundado por la Comisión Europea. El Consorcio une a 14 socios de 5 ciudades Europeas y representa todas las disciplinas relevantes. El consorcio incluye Hospitales, proveedores de servicios médicos, universidades, operadores de redes móviles, proveedores de servicios e infraestructura móvil, y proveedores de hardware. (MobiHealth, 2004)

El sistema de MobiHealth permite a los pacientes estar monitoreando su salud desde un ambiente totalmente móvil. Los usuarios utilizan un sistema de monitoreo ligero llamado BAN (Body Area Network), el cual, está personalizado para sus propias necesidades de salud. Así, un paciente que requiera monitoreo por largos o cortos períodos de tiempo no tiene que permanecer en el hospital para el servicio y puede realizar sus actividades normales diarias.

El BAN, mencionado anteriormente, es la clave de la parte móvil del sistema y Su diseño se basa en el concepto de PAN (Personal Area Networks). Los dispositivos en el Body Area Network, son normalmente sensores que reúnen datos médicos acerca del paciente como presión en la sangre, pulso, nivel de glucosa y electrocardiogramas (ECG) entre otros. Aparte de los sensores si fuera necesario sería posible incluir también activadores, como la insulina. (S´anchez, Perramon, Mart´ı, Delgado, 2004)

El servidor donde se almacena la información, se llama sistema Back-End, y está localizado generalmente en el hospital o centro de salud donde, los

usuarios finales (doctores, enfermeras u otro profesional en salud) puedan monitorear los datos del paciente con una aplicación específica. También es posible un proveedor de servicios externo, si no hay suficientes recursos computacionales disponibles en el hospital.

- **Programa espacial NASA**

Uno de los usos más importantes de M-Health es para el programa espacial, el cual se apoya en las telecomunicaciones para enviar operaciones médicas de rutina. Por medio de un dispositivo, se recolecta audio, video y datos del paciente desde el espacio. La capacidad e los datos incluyen, electroencefalograma (ECG por su significado en inglés), ritmo cardíaco, oxigenación de la sangre y presión de la sangre. Las capacidades video médicas incluyen el ojo, la piel, la oído-nariz-garganta, y la proyección de imagen macro general. Un estetoscopio electrónico permite la colección de datos de la auscultación. Los datos obtenidos son compatibles con el sistema de comunicación del vehículo espacial para ser enviados a la tierra. (Tachakra, Wang, Istepanian, Song 2003)

- **Servicios de emergencia en la ambulancia**

Este sistema de M-Health consiste de dos componentes principales: una unidad móvil para la ambulancia y una estación base receptora para la conexión de la Intranet del hospital. Los datos del paciente como signos vitales, audio e imágenes de video de las actividades de cuidado desde el interior de la ambulancia son transmitidos en tiempo real al centro de trauma usando comunicaciones celulares digitales inalámbricas y tecnología Intranet en el hospital.

- **Sistema de Monitoreo Casero "Biotronik"**

Este dispositivo creado en Alemania, permite a los doctores vigilar de cerca los corazones de sus pacientes entre las visitas a los consultorios. El dispositivo incluye un transmisor que envía información a un teléfono celular transportado por el paciente. El teléfono envía la información a un centro de servicio de una compañía donde es transmitida vía fax al doctor del paciente. Entre otras ventajas que se ofrecen con esta tecnología es que, el dispositivo puede ser programado para recolectar datos de acuerdo a las necesidades del paciente, desde una vez al día hasta una vez al mes. Además este dispositivo funciona desde cualquier lugar en el que se ofrezca servicio de telefonía Móvil digital.

- **TeleCardio-FBC**

Es un sistema de la telemedicina desarrollado y desplegado en el Brasil para permitir a cardiólogos en la unidad de la cardiología y de la cirugía cardiovascular cooperar con otros médicos. El sistema permite reducir costos

proporcionando cuidado médico especializado en cardiología para pacientes que viven lejos de las áreas metropolitanas. Este sistema original fue diseñado considerando computadoras de escritorio como la única plataforma, como consecuencia, el acceso a las funcionalidades de los sistemas en diferentes plataformas computacionales no era posible.

Un nuevo sistema llamado TeleCardio Móvil fue desarrollado tomando las ventajas de los avances de tercera generación, para proveer acceso en línea a la información en el sistema TeleCardio-FBC a través de asistentes personales digitales y teléfonos Móviles conectados a Internet por medio de módems inalámbricos.

TeleCardio Móvil consiste en dos sistemas de plataforma independientes, M-TeleCardio y WapCardio. M-Telecardio permite el acceso a todas las funcionalidades de TeleCardio-FBC por medio de asistentes personales digitales, como palm y laptops, conectadas a Internet por medio de módems inalámbricos. WapCardio proporciona información importante, por ejemplo, las peticiones de la consulta y los resultados alejados de procedimientos médicos, a los médicos en los teléfonos móviles usando la tecnología de WAP.

En México esta tecnología aún está en sus comienzos y apenas se está implantando la tecnología E-Health.

- **Programa E-Salud**

Este programa tiene como propósito el de contribuir a mejorar la salud de la población y ampliar la cobertura de los servicios, con prioridad para los habitantes de localidades con los niveles de mayor marginación, mediante un sistema telemático de alto contenido social; poner al alcance de la población información en salud que contribuya al desarrollo humano, individual y de la sociedad en su conjunto, a través de información en línea, y apoyar la capacitación y educación continua del personal de salud. (E-Salud, 2004)

En este propósito de incorporar a la salud las tecnologías de la información y las telecomunicaciones participan la Secretaría de Salud, el Instituto Mexicano del Seguro Social, el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, Petróleos Mexicanos, la Secretaría de la Defensa Nacional e Instituciones y organismos del sector privado en coordinación con el Sistema Nacional e–México.

La integración de la salud, las tecnologías de la información y las telecomunicaciones permitirá la arquitectura y la construcción de una nueva forma de organización y funcionamiento de los servicios de salud, donde la innovación sea factor clave para un cambio con sentido y rumbo. Un cambio que permita transformar la administración tradicional en salud, mediante procesos más

eficientes orientados a la atención del ciudadano y al logro de un sistema de salud mejor comunicado y más inteligente.

Actualmente, se espera poder consolidar dos proyectos: la Telemedicina y Portal E-Salud.

Telemedicina está dirigido a apoyar a los trabajadores de la salud de todos los niveles de atención en el diagnóstico y tratamiento de enfermedades, la gestión y gerencia de servicios de salud, así como a reforzar la capacitación continua del personal médico, técnico y administrativo de los centros de salud, clínicas y hospitales generales. En suma, Telemedicina se orienta a apoyar y mejorar las capacidades del personal de las instituciones para impulsar así una mayor calidad en los servicios de salud.

La apertura del Portal e–Salud busca mantener informada a la población en general sobre actividades de promoción de la salud y prevención de daños, además de la realización de trámites y gestiones gubernamentales en materia de salud.

A través de Telemedicina y del Portal e–Salud se podrá difundir la política sanitaria, los contenidos de los programas de acción del sector salud y de las campañas sobre tópicos de difusión prioritaria para las instituciones, así como establecer un sistema de rendición de cuentas y trasparentar la administración de los servicios de salud. (E-Salud, 2004)

- **Retos de M-Health**

La meta común actual en la tecnología de información médica es el diseño e implementación de las soluciones de la telemedicina, las cuales proporcionan a los pacientes con enfermedades crónicas, servicios móviles que mejoran su calidad de vida además de soportar y optimizar su tratamiento en caso de emergencia.

Sin embargo, esto podría requerir sensores micro-tecnológicos para ser usados en aplicaciones móviles, modularidad, una red de comunicación inalámbrica, inteligencia local en forma de una unidad de información móvil muy poderosa, conexión a una red global y un sistema concluyente diseñado para mejorar la efectividad de los procedimientos relacionados con el cuidado de la salud. (Tachakra, Wang, Istepanian, Song 2003)

El primer paso para fortalecer el M-Health es construir los dispositivos correctos para manejar las necesidades de la industria. "Uno de los mayores retos para la aceptación de aplicaciones móviles es obtener el factor apropiado, así como una tasa de desempeño adecuada".

El reto en la industria móvil, una vez convenciendo a la industria del cuidado de la salud para adoptar tecnología inalámbrica, es conseguir los dispositivos en un tamaño manejable.

Capítulo 4. Seguridad

Los sistemas celulares de tercera generación han mejorado en cuanto a características de seguridad, han mejorado la seguridad de los sistemas de segunda generación, haciéndolos más robustos ante los servicios no autorizados y el eavesdropping. (Salkintzis, 2004)

Sin embargo, a pesar de estas mejoras, existen todavía riesgos de seguridad en las redes que no necesariamente tienen que ver con el plano tecnológico o que no son exclusivas de las redes 3G.

Hoy en día ya no se trata de adquirir un sistema donde instalar un cortafuegos perimetral (y quizás el software necesario) y considerar el problema resuelto. Las herramientas y los servicios requeridos para el funcionamiento diario de la actividad empresarial presentan fallos de seguridad y estos posibilitan el uso indebido por parte de usuarios no autorizados. El crecimiento constante del número de herramientas automatizadas para explotar las vulnerabilidades está reduciendo los conocimientos técnicos requeridos para llevarlos a cabo, convirtiéndose, cada vez más, en ataques automatizados y no dirigidos. (Colorado, 2004)

Un único agujero de seguridad puede comprometer toda la infraestructura corporativa. Por ejemplo, una instalación anónima de un sistema operativo no actualizado con los últimos parches de seguridad y conectado a Internet sin ningún tipo de protección es rastreada, analizada y comprometida en menos de quince minutos.

Ya que tercera generación está relacionada directamente con las redes IP, sufre de sus vulnerabilidades, Internet (que es una red IP) por ejemplo es un entorno hostil y los atacantes están buscando los puntos más débiles de una organización y, a pesar de un diseño que procure protegerlos, no se tiene nunca la total certeza de la efectividad de las medidas adoptadas. Las pruebas de seguridad tratan de ser la respuesta, proporcionando la información necesaria que indique si la política de seguridad y los sistemas funcionan.

Pero no sólo Internet es un entorno tremendamente hostil, sino que también las redes corporativas son objeto de ataque. Cada vez es más común que accedan a las compañías elementos externos que provienen de entornos de un menor nivel de seguridad en los que se confía sin tomar ninguna medida. Estamos hablando, por ejemplo, de los operadores que ofrecen las aplicaciones de 3G.

También es frecuente la contaminación de infraestructuras a través de equipos portátiles de empleados (o visitantes externos) que han estado expuestos y han sido infectados por virus, gusanos y otros códigos maliciosos en otros entornos. Claramente, la seguridad perimetral puede ser insuficiente para proteger la organización.

En la siguiente figura se ilustran las principales preocupaciones que actualmente se tienen debido a la gran importancia que ha cobrado la información, como activo en una organización.

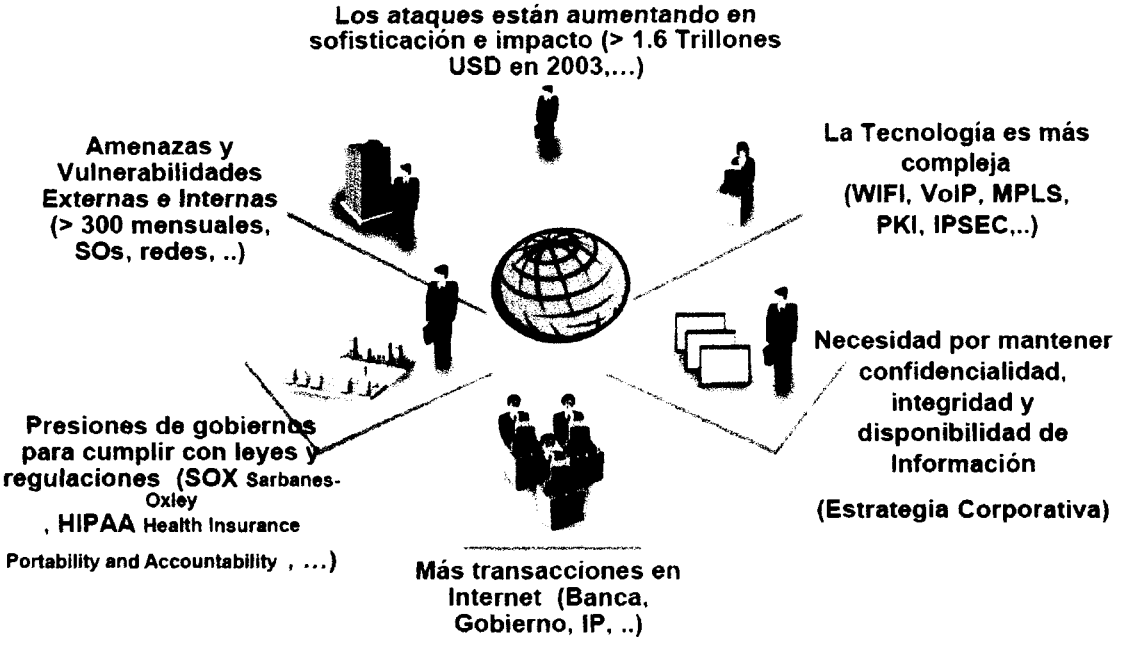

Figura 10. Preocupaciones actuales en Seguridad de la Información. Fuente. Ing. Ricardo Morales, Administración de Riesgos de Seguridad de Información.

El problema es: ¿cómo detectar las distintas formas en las que la seguridad corporativa puede quedar comprometida? ¿Cómo descubrir los "focos de infección" más probables? ¿Cómo determinar el nivel de riesgo que asume la compañía?

Las pruebas de intrusión, la detección de vulnerabilidades en sistemas, las auditorias de seguridad y el análisis de riesgos son algunos de los métodos que pueden proporcionar una visión de la seguridad real de la empresa, tanto de su estado como de su posible evolución. (Colorado, 2004)

4.1 Arquitectura y dimensiones básicas de seguridad

La arquitectura de seguridad se define teniendo en cuenta dos conceptos principales a saber: **las capas y los planos**. Las capas de seguridad tienen que ver con los requisitos aplicables a los elementos de red y sistemas que constituyen la red extremo a extremo. El sistema de capas proporciona una perspectiva jerárquica de la seguridad extremo a extremo de la red basada en la seguridad capa por capa. (UIT, 2003)

Hay tres capas de seguridad: **la capa de infraestructura, la capa de servicios, y la capa de aplicaciones**. Una de las ventajas del modelo de capas es que se garantiza la seguridad extremo a extremo aun cuando se utilicen diferentes aplicaciones. Cada capa tiene sus propias vulnerabilidades y, por tanto, se han de definir medidas para contrarrestarlas en cada una de ellas.

La capa de infraestructura comprende los dispositivos de transmisión de red, así como los elementos que la componen. Por ejemplo, son parte de dicha capa los routers, los centros de conmutación y los servidores, así como los enlaces de comunicación entre ellos.

La capa de servicios tiene que ver con la seguridad de los servicios de red que los proveedores prestan a sus clientes, yendo desde servicios básicos de transporte y conectividad, como las líneas arrendadas, hasta los servicios de valor añadido como la mensajería instantánea.

La capa de aplicaciones tiene que ver con la seguridad de las aplicaciones de red a las que acceden los usuarios, y que van desde las básicas como el correo electrónico hasta las sofisticadas como la colaboración en vídeo, en la que se utilizan transferencias de video mucho más elaboradas, por ejemplo para el diseño de automóviles.

El segundo eje central del marco de trabajo tiene que ver con la seguridad de las actividades que se efectúan en una red. Para ello, se definen tres planos de seguridad que representan los tres tipos de actividades protegidas que se realizan en ella: **1) el plano de gestión, 2) el plano de control, y 3) el plano usuario final.**

Estos planos de seguridad corresponden a necesidades de seguridad particulares relativas a las actividades de gestión de red, control de red o señalización, así como a las de usuario final. El plano de seguridad de gestión, tiene que ver con las actividades relacionadas con, por ejemplo, la configuración de un usuario o una red, y otras.

El plano de seguridad de control se relaciona con los aspectos de señalización necesarios para establecer (y modificar) la comunicación extremo a extremo a través de la red, sin importar el medio y la tecnología utilizados en ella.

El plano de seguridad de usuario de extremo tiene que ver con la seguridad cuando se accede y utiliza la red; en este plano también se considera la seguridad de flujos de datos del usuario extremo.

Además de los dos ejes principales compuestos por las capas de seguridad y planos de seguridad (tres de cada uno de ellos), en el marco se definen también tres dimensiones. Desde un punto de vista puramente arquitectural, estas

dimensiones se aplican a cada una de las componentes de la matriz 3 por 3 formada entre las capas y los planos, de tal manera que se puedan tomar medidas para contrarrestar los problemas de seguridad correspondientes. En la figura 11 se indican los planos, capas y dimensiones de seguridad de la arquitectura de seguridad. (UIT, 2003)

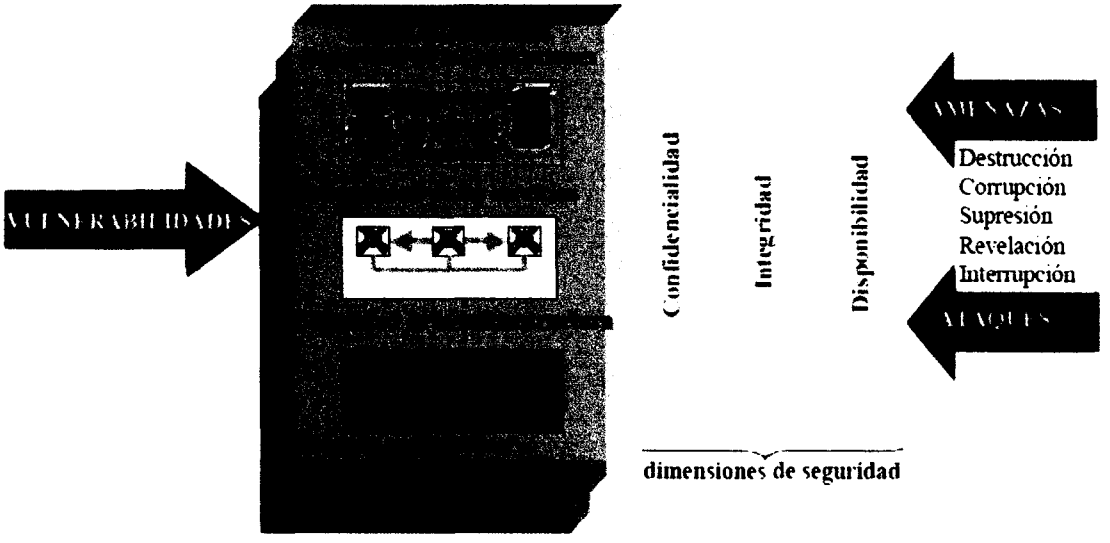

Figura 11. Elementos Estructurales de la Seguridad
Fuente: Unión Internacional de Telecomunicaciones.

4.2 Confidencialidad

Una de las razones principales para buscar la seguridad en las telecomunicaciones es el propio concepto de privacidad, algo que se conoce comúnmente como el derecho que tiene cada persona para controlar quién recopila y almacena información relacionada con ella, qué tipo de información y quién tiene acceso a ésta. Además, este concepto tiene que ver con los medios técnicos necesarios (por ejemplo, la criptografía) para garantizar que la información sólo llegue a los destinatarios deseados, de tal manera que solamente aquellas partes explícitamente autorizadas puedan recibirla e interpretarla.

4.3 Integridad

Propiedad que consisten en que los datos no han sido alterados de una manera no autorizada. Además, la integridad de los datos garantiza que la información esté protegida contra las siguientes operaciones no autorizadas: modificación, supresión, creación, y copia de los datos.

4.4 Disponibilidad

Garantiza que una interrupción de la red no impida el acceso autorizado a los elementos de ésta, la información almacenada, los flujos de información, los servicios y las aplicaciones. (UIT, 2003)

4.5 Seguridad en 3G

Entre los protocolos más importantes de tercera generación se encuentra el UMTS, por lo que las bases de la seguridad se describen de acuerdo a este protocolo en particular.

Los principios de seguridad de UMTS se basan en un desarrollo de los elementos difundidos para sistemas de segunda generación, tales como GSM y GPRS. Algunos de los fundamentos de seguridad que se mantienen, con o sin modificaciones, de los sistemas de segunda generación son:

- Autenticación de los usuarios para acceder a los servicios
- Cifrado de la interfaz de radio
- Confidencialidad de la identidad del usuario en la interfaz de radio aumentando el nivel de seguridad
- Las características de seguridad de aplicaciones del SIM
- Elementos de seguridad independientes del usuario

UMTS ofrece nuevas características de seguridad en diversos aspectos como aplicaciones, visibilidad y movilidad.

En cuanto a las aplicaciones ofrece a los proveedores la posibilidad de crear servicios más confiables para el usuario. Las principales mejoras que UMTS ofrece son:

- Autenticación de la entidad de la aplicación, propiedad que permite que dos aplicaciones sean capaces de corroborar su identidad.
- Autenticación del origen de los datos de aplicación, propiedad que permite a la aplicación receptora verificar el origen de los datos recibidos.
- Integridad de los datos de aplicación, propiedad que permite a la aplicación receptora comprobar que los datos enviados por la aplicación par no han sido modificados.
- Detección de reenvío de datos de aplicación, propiedad por la que una aplicación es capaz de detectar que los datos recibidos no han sido reenviados.
- Integridad en la secuencia de datos de aplicación, propiedad que permite que una aplicación verifique los datos recibidos estén en la secuencia correcta.

- Comprobante de recepción, propiedad que permite a la aplicación origen demostrar que la aplicación receptora ha recibido los datos enviados.
- Confidencialidad de los datos de aplicación, propiedad que permite que los datos de la aplicación no sean conocidos por elementos no autorizados.

UMTS también proporciona mayor visibilidad de las operaciones de seguridad disponibles, por ejemplo.

- Interacción de encriptación en la red de acceso, propiedad que permite al usuario conocer si los datos están protegidos por confidencialidad en la conexión de red de radio en concreto cuando se establecen llamadas no cifradas.
- Indicación de encriptación completa, propiedad que permite al usuario conocer si los datos de usuario están protegidos pos confidencialidad en todo el camino de comunicación.
- Indicación del nivel de seguridad, propiedad que permite al usuario conocer el nivel de seguridad que ofrece una red visitada, en particular cuando el usuario se mueve a una red con inferior nivel de seguridad, por ejemplo, de 3G a 2G.

Los sistemas móviles GSM y UMTS comparten una estructura de red para la conmutación de paquetes sustancialmente equivalente, ya que UMTS hereda la arquitectura creada para GSM, por ello su sistema de gestión de movilidad es similar, y está basado en el protocolo GTP (GPRS Tunnelling Protocol) definido por ETSI para gestionar la movilidad en las redes GPRS. (González, telefónica, 2001)

Dado que UMTS mantiene los fundamentos de GSM y GPRS, se puede afirmar en definitiva que, más que una revolución, UMTS es una evolución natural de estas tecnologías, y lo verdaderamente importante no es la propia tecnología, sino las posibilidades que esta brinda, para enriquecer la seguridad en las aplicaciones ofrecidas por las organizaciones.

4.6 Vulnerabilidades

Una vulnerabilidad de seguridad es un defecto o debilidad en el diseño, implementación o funcionamiento de un sistema que podría ser utilizado para violar su seguridad. Una vulnerabilidad de seguridad no es un riesgo, amenaza o ataque. (UIT, 2003)

Hay cuatro tipos de vulnerabilidades:

- **Modelo de amenaza**, que resulta de la dificultad para prever amenazas futuras.

- **Diseño y especificación**, producida de errores o descuidos en el diseño del protocolo que lo hacen inherentemente vulnerable.

- **Implementación**, que se produce como resultado de errores en la implementación del protocolo.

- **Funcionamiento y configuración**, que resulta de la utilización errónea de opciones en las implementaciones o de políticas insuficientes de instalación (por ejemplo, cuando el administrador de red no facilita la utilización de la encriptación en una red WiFi, o cuando escoge un cifrado de trenes que no es suficientemente robusto).

- **Vulnerabilidades específicas.**

Existen muchos problemas potenciales con la seguridad de 3G, a continuación se mencionan algunos: (Salkintzis, 2004)

- El IMSI (Internacional Mobile Subscriber Identity), es el identificador permanente del sistema móvil. Para propósitos de seguridad, la red deriva un TMSI (Temporary Mobile Suscriber Identity) desde el IMSI y pide al móvil usar el TMSI. Sin embargo, el IMSI es enviado en un texto claro al VLR/SN (Visitor Location Register/Serving Node) cuando asigna el TMSI al usuario. Esto es necesario porque los procedimientos de no autenticación y la clave de aceptación (AKA por sus siglas en inglés) pueden ser desempeñadas antes que la identidad del dispositivo se conozca.

- La transmisión del IMEI (Internacional Mobile Equipment Identity) no está protegida.

- La arquitectura no protege contra vectores de autenticación comprometidos que aún no han sido usados para autenticar el USIM (Universal Suscriber Identity Module). Así, la red es vulnerable para ataques usando vectores de autenticación comprometidos que han sido interceptados entre generación en el centro de autenticación y usado en la red.

- Mala protección de equipos y/o elementos de almacenamiento (instalación física). (Carrera, 2005)

- Situaciones no previstas, gusanos o bien límites no especificados (hardware y software).

- Negligencia, vagancia, estupidez, ambición (humanas).

4.7 Amenazas

Una amenaza de seguridad es una violación potencial de la seguridad que puede ser activa, es decir que existe la posibilidad de un cambio deliberado y no autorizado del estado del sistema, o pasiva, cuando hay amenaza de revelación no autorizada de la información sin que se modifique el estado del sistema. (UIT, 2003)

Ejemplos de amenazas activas son la usurpación de identidad, como entidad autorizada, y la negación de servicio. Un ejemplo de amenaza pasiva es la escucha clandestina tendiente a robar contraseñas no cifradas. Estas amenazas pueden provenir de piratas informáticos, terroristas, vándalos, del crimen organizado, o pueden tener origen en alguna entidad estatal, pero en muchas ocasiones provienen del interior mismo de la organización.

Ejemplos:

- Virus
- Divulgación de contraseñas
- Accesos indebidos
- Fuga de informaciones
- Piratería
- Basura informática
- Robo
- Fraudes

4.8 Riesgos

Un riesgo de seguridad ocurre cuando se combinan una vulnerabilidad y una amenaza de seguridad. Por ejemplo, un problema de programación que origine desbordamiento en una aplicación de sistema operativo (es decir una vulnerabilidad) que se asocie con el conocimiento de un pirata, y las herramientas y acceso correspondientes (es decir, una amenaza) puede degenerar en un riesgo de ataque al servidor Internet.

Las consecuencias de los riesgos de seguridad son las pérdidas, y corrupción de datos, la pérdida de privacidad, el fraude, el tiempo fuera de servicio, y la disminución de la confianza del público. (UIT, 2003)

4.9 Ataques

Existen ciertos ataques que pueden ser lanzados tomando ventaja de las vulnerabilidades anteriormente mencionadas, a continuación se mencionan algunos de ellos. (Salkintzis, 2004)

- **Imitación de la red.**

Hay al menos dos maneras de lanzar este tipo de ataque:

1. Suprimiendo la encriptación entre el usuario y el atacante. En este ataque, el agresor imita una estación base falsa, mientras se comunica con el usuario e intenta engañar al usuario dentro de la supresión del cifrado de la comunicación.

2. Forzando el uso de una llave cifrada comprometida. En este caso, el atacante imita una estación base y debe poseer un vector de autenticación comprometido. Con esta información, el agresor puede forzar al usuario a usar el vector comprometido y su llave asociada, ya que el usuario no tiene control sobre la llave cifrada que se usa en la comunicación.

- **Imitación del usuario.**

Hay al menos tres maneras de lanzar este tipo de ataque.

1. Usando un vector de autenticación comprometido para hacerse pasar por un usuario válido.

2. Usando una simple repetición. En este caso el atacante, escucha una secuencia de autenticación entre un usuario válido y la red. El agresor entonces, intenta autenticarse con la red repitiendo la misma secuencia de autenticación.

3. Usando el canal hijacking. Este ataque puede ser logrado de varias maneras, pero la básica es que el agresor engaña a la red en el canal de una llamada saliente y se hace cargo del canal para hacer llamadas a nombre del usuario.

- **Eavesdropping**

Este ataque es difícil aún cuando el nivel de cifrado de la red es deshabilitado, ya que, el canal de aire desempeña obligatoriamente revolver los datos del usuario como parte del proceso de la señal de radio.

- **Ataques de DoS**

Existen muchas maneras en las cuales se podría intentar un ataque de este tipo. Algunas de estas formas pueden frustrarse por el esquema de seguridad de 3G, mientras que otras no. Se pueden agrupar en dos grandes categorías. (Salkintzis, 2004)

1. DoS a la capa de red.

a) El primer método de ataque es a través de la supuesta petición de des-registro del usuario. Aquí el agresor engaña con un mensaje de des-registro desde un dispositivo móvil a la red, causando que la red termine su sesión con el dispositivo.

b) El segundo método es a través de una falsa petición de actualización de la localización. Es similar al ataque anterior, excepto que en vez de enviar una petición de des-registro, se envía una de actualización de localización y el usuario no puede alcanzar la red debido a que ésta cree que el usuario está en una localización incorrecta.

c) El tercer método implica "establecerse" en una falsa estación base. En este caso el atacante imita una estación base y el usuario se asocia con ella y por lo tanto pierde conectividad con la red real.

d) El cuarto ataque involucra "establecerse" en una estación base (BS por sus siglas en inglés) o en un sistema móvil (MS por sus siglas en inglés). En este caso la BS/MS actúa como un repetidor de mensajes entre la red real y el usuario. La estación falsa puede permitir pasar algunos mensajes, mientras filtra otros.

2. DoS en la capa física.

El control de poder es una parte importante de la operación de sistemas en 3G. El apropiado incremento o decremento del poder de la señal transmitida permite las ventajas de mejora de la calidad de la señal de frecuencia de radio, el tiempo de vida de la batería, reduce interferencia, y la ganancia de la capacidad del sistema.

Por lo tanto el control de poder puede ser usado para el ataque de DoS. Por ejemplo, un nodo puede pedirle artificialmente a la estación base mantener incrementando el poder de las señales transmitidas aunque la señal recibida tiene una un alto SINR (Signal to Interferente Noise Ratio).

- **Ataque de Identidad (Identity Caching Attacks).**

Hay al menos dos maneras de realizar este tipo de ataques.

1. El primer método es una pasiva identity caching attack. En este caso, el atacante monitorea la red de comunicación en espera que la red pida que el usuario envíe su identidad a la estación base.

2. El segundo método es un ataque activo. En este caso, un agresor con una falsa estación base, pide al usuario que envíe su identidad permanente en un plano sencillo. (Salkintzis, 2004)

- **Ataques sobre el flujo de información.**

  - **Interrupción:** Un recurso del sistema es destruido o se vuelve no disponible, por lo tanto este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros. (Delitos informáticos, 2001)

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

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

  - **Fabricación:** Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo. Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

- **Ataques a sistemas**

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

    - Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante. (Delitos informáticos, 2001)

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

  - **Suplantación de identidad:** El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

  - **Reactuación:** Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada. (Delitos informáticos, 2001)

  - **Modificación de mensajes:** Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

  - **Degradación fraudulenta del servicio:** Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes falsificados. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, etc. (Delitos informáticos, 2001)

Capítulo 5. Análisis

Como se observó en la sección 4.1 referente a la Arquitectura y dimensiones básicas de la seguridad, existen diversas capas y planos sobre las cuales se trabaja la seguridad de la información.

Para el estudio de la tesis se trabajará sobre la capa de aplicación y el plano de seguridad de usuario final, ya que, para analizar la seguridad de toda una tecnología como tercera generación, desde el punto de vista de todas las capas y planos, se requiere una investigación mucho más rigurosa sobre todo en los aspectos técnicos, de acceso, protocolos y de cifrado entre otros, para lo cual se necesita un período de tiempo mucho más prolongado que el disponible.

Por otro lado, en 3G se tiene mayor conciencia de la seguridad respectiva a las capas inferiores de infraestructura y servicio, aumentando considerablemente el grado de dificultad en los ataques a estos niveles.

La metodología utilizada en este análisis existe en la literatura referente a la seguridad de la información (ISO 17799), sin embargo, para poder ser aplicada a esta tesis es necesaria la modificación y adaptación de la mayor parte de las métricas, así como los criterios aplicados, debido a que no se cuenta con la información que normalmente se requiere para este tipo de estudios, procesos, financieros y legales entre otras.

Tomando en cuenta además, que resulta difícil encontrar documentación de seguridad cuyas políticas y controles se apliquen específicamente a tecnología inalámbrica, se puede afirmar que la técnica aplicada es una importante aportación en el género de la seguridad para aplicaciones de tercera generación ya que ofrece a los operadores una guía particularizada para la administración de esta tecnología.

5.1 Análisis del flujo de información

En todas las aplicaciones en las cuales intervenga el envío de información, se genera un flujo entre los diversos componentes tecnológicos que conforman la red. Cuando se entiende bien esta red de información, se puede determinar la importancia de su análisis, el cual permite detectar las vulnerabilidades a las cuales la información se somete.

Aplicación	Sistema Origen	Sistema Destino	Razón de Flujo
E-mail	Móvil	Servidor de e-mail	Envío información diversa al servidor (Buzón) donde se almacena, para ser accesada mediante la interfaz de usuario por medio de la red de Internet.
Localización	Móvil	Servidor de Localización	Información que se envía desde el móvil (no es generada por el usuario), utilizada por el operador para ofrecer diversos servicios como la publicidad personalizada
M-Health	Móvil	Servidor externo	Envío de información desde el usuario hasta el servidor de la aplicación, el cual no es dominio del operador.

Tabla 3. Flujo de información entre aplicaciones

La tabla 3 ayuda a entender de forma general los flujos de información de los servicios que están siendo analizados, sin embargo, la visualización del flujo particular entre los activos que interactúan en estas aplicaciones, permite identificar de mejor forma la información importante y clasificarla de acuerdo a su valor en la organización.

La figura 12 muestra la arquitectura del servicio de e-mail de forma mucho más detallada.

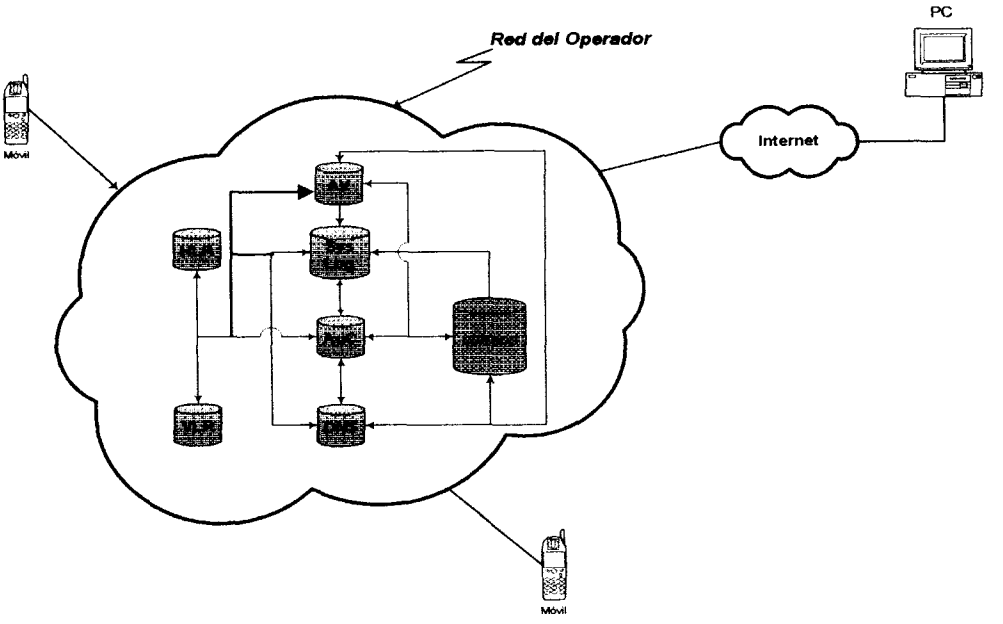

Figura 12. Interacción de activos en la arquitectura de E-mail

El activo de antivirus debe estar interconectado con todos los servidores para asegurar que todos estén protegidos en contra de cualquier clase de software malicioso. Así mismo el Syslog recibe información de todos los eventos ocurridos en cada uno de los servidores para poder realizar los historiales con fallas en los equipos, accesos no autorizados o bien modificación de la información sin permiso.

El HLR y VLR contienen información (IMSI, TMSI y derechos de servicio del usuario, por mencionar algunos) que complementan el servicio que ofrece autenticación para proveer los accesos correspondientes a cada petición de servicio de los usuarios, es decir que si ocurre un ataque a estos activos y quedan no disponibles, como consecuencia el servidor de autenticación queda inservible también. El DNS interactúa con el servidor de correos y, obviamente debe estar interconectado al antivirus y al Syslog para control de fallas y ataques. Este servicio se usa principalmente para establecer los vínculos con los destinatarios de los correos.

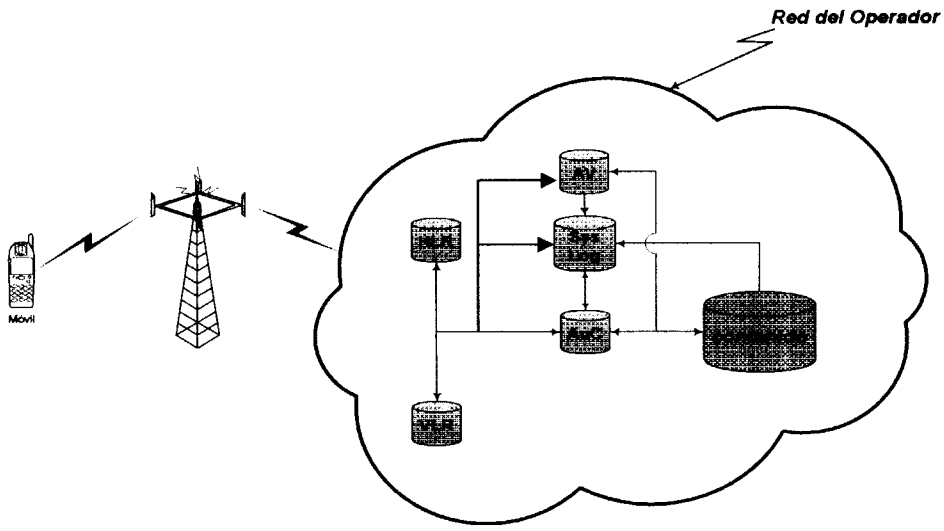

Figura 13. Interacción de activos en la arquitectura de Localización

Como se puede observar en la figura de arriba la interconexión de activos en el servicio de localización es muy similar a la de E-mail. El antivirus se interconecta a todos los activos por razones de protección contra software malicioso, el Syslog registra eventos anormales en los activos. El HLR y VLR interactúan con el servidor de autenticación, sin embargo, en este servicio la autenticación sirve no sólo para conceder accesos a los servicios del operador, también se usa para establecer la localización física del equipo móvil. El servidor de contenidos guarda la información propia para ofrecer el servicio (publicidad, clima, logística, etc.).

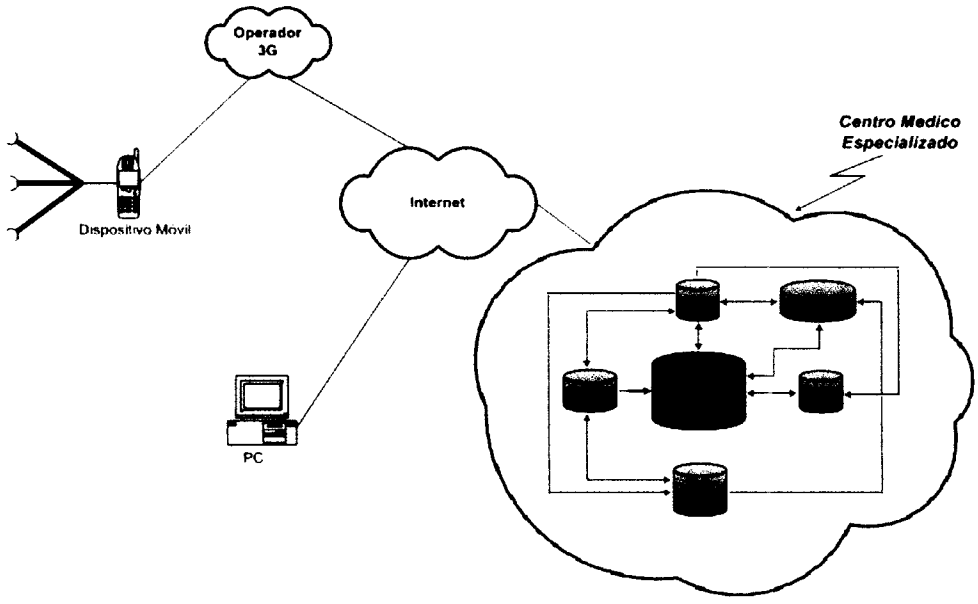

Figura 14. Interacción de activos en la arquitectura de M-Health

En el servicio de M-Health, como en las aplicaciones de E-mail y localización el servidor de antivirus y el Syslog, son indispensables en cualquier estructura de red, para proteger los activos de software malicioso y registrar las fallas para futuros incidentes similares. El servidor de autenticación proporciona los niveles de permisos a los usuarios para accesar a la información del Back-end. El activo de alarmas requiere información del servidor Back-end para poder establecer los avisos de acuerdo a la información de los usuarios (historiales, análisis, recetas médicas, etc.). El servidor web se utiliza en caso de acceso desde internet e interactúa con todos los activos restantes (ver figura 14).

5.2 Clasificación de la información

La información puede ser clasificada por su importancia, esta clasificación permite establecer medidas de seguridad para evitar que sea corrompida o comprometida causando daños.

La categorización más comúnmente utilizada está dividida en:

Pública: Es la información que es expresamente autorizada para su divulgación pública. Puede ser distribuida vía canales autorizados como: páginas web, artículos, etc.

Interna: Esta clase de información es clasificada de acuerdo a la sensibilidad del material que contiene y se autoriza su divulgación internamente.

Confidencial: Esta clase de información puede tener efectos adversos para la corporación en caso de ser comprometida.

Restringida: Si es comprometida, esta información, puede causar severos daños financieros, legales, regulatorios y de reputación.

En la siguiente tabla se clasifica la información de los activos a proteger en la aplicación de E-mail.

E-mail													
Información													
DNS		Autenticación		Correos		HLR		VLR		Syslog		Antivirus	
Nombres de Internet	P	Nombres de usuarios	C	Nombres de usuarios de correo	C	Información de la estación móvil (IMSI, MSISDN)	C	Información de la estación móvil (IMSI, MSISDN, TMSI)	C	Registros de eventos de los operadores	C	Bases de datos de equipos en el dominio	C
Nombres de dominio	I	Contraseñas de cuentas de usuario	R	Correos de los usuarios	C	Información de localización (ISDN del HLR y VLR)	C	Información de localización (MSC, LAI)	C	Registros de eventos de la infraestructura	C	Versión del antivirus instalado en cada equipo	C
Nombres de servidores de correo	I	Perfiles de usuario	C	Web-mail	P	Información de servicios (suscripción, restricciones, servicios suplementarios)	C	Información de servicios (subgrupo de servicios del HLR)	C			Versión de S.O. de cada equipo	C
						Identificadores Internacionales de Equipos Móviles (IMEI)	I						

Donde: P = pública, I = Interna, C = confidencial, R = restringida

Tabla 4. Clasificación de la información de E-mail

Los nombres de Internet se relacionan con una dirección IP que corresponde a la página que se quiere accesar, estos nombres sirven únicamente para hacer el acceso más fácil, ya que es más sencillo recordar nombres que números, por lo tanto su dominio es público y se clasifican como tal. En este caso no es el nombre lo que le interesa proteger al operador sino el vínculo con la dirección IP correspondiente, el cual, en caso de perderse si podría ocasionar el enrutamiento incorrecto de los e-mail provocando su pérdida.

El servicio de Web-mail, se refiere a poder accesar a los correos almacenados en el servidor de e-mail perteneciente al operador, desde cualquier otro dispositivo que no sea el móvil. La información que este activo almacena es únicamente la necesaria para poder desplegar en lenguaje HTML la información requerida por el usuario. Debido a esto se integra al servidor de correos y se clasifica como pública.

El servidor DNS sirve para poder accesar a un dominio específico entre los millones existentes asegurando su visibilidad. Cuando un servicio requiere el uso del DNS, la información ahí almacenada es accesada de forma transparente, el usuario no se entera o no debe enterarse de esta información, para asegurar esto se clasifica de Interna.

La etiqueta de confidencial se otorga a la información que en caso de ser corrompida representa situaciones de peligro tanto para el operador, como para el usuario, comprometiendo sus operaciones y servicios ofrecidos entre otros. Los perfiles de usuario (que se usa para una administración adecuada de los permisos entre otras funciones), son un ejemplo de información confidencial ya que si son cambiados o eliminados sin autorización ocasionan la pérdida de control del operador sobre los servicios ofrecidos a cada cliente.

Como restringida, se clasifica la información que en caso de ser comprometida de alguna manera, ocasionen al operador pérdidas financieras, daño de imagen y problemas legales por mencionar algunos. Las contraseñas de cuentas son de vital importancia para la aplicación de E-mail. Si, por ejemplo, un software malicioso atacase el activo que guarda esta información ocasionando su pérdida, los usuarios no podrían accesar a este servicio, provocando posibles pérdidas de clientes, financieras y la decepción por parte del usuario.

En la tabla 5 se clasifica la información de los activos a proteger en la aplicación de Localización.

Localización											
Información											
Autenticación		Contenido		HLR		VLR		Syslog		Antivirus	
Nombres de usuarios	C	Información para el usuario (publicidad, clima, mapas)	P	Información de la estación móvil (IMSI, MSISDN)	C	Información de la estación móvil (IMSI, MSISDN, TMSI)	C	Registros de eventos de los operadores	C	Bases de datos de equipos en el dominio	C
Contraseñas de cuentas de usuario	R			Información de localización (ISDN del HLR y VLR)	C	Información de localización (MSC, LAI)	C	Registros de eventos de la infraestructura	C	Versión del antivirus instalado en cada equipo	C
Perfiles de usuario	C			Información de servicios (suscripción, restricciones, servicios suplementarios)	C	Información de servicios (subgrupo de servicios del HLR)	C			Versión de S.O. de cada equipo	C
				Identificadores Internacionales de Equipos Móviles (IMEI)	I						

Donde: P = pública, I = Interna, C = confidencial, R = restringida, IMSI = International Mobile Suscriber Identity, TMSI = Temporary Mobile Suscriber Identity, MSISDN = Mobile Station Internacional Service Digital Network, ISDN = Integrated Services Digital Network, HLR = Home Location Register, VLR = Visitor Location Register, MSC = Mobile Switching Center, LAI = Location Area Identity

Tabla 5. Clasificación de la información de Localización

La aplicación de localización ofrece gran valor agregado a los usuarios, sin embargo, la información requerida para soportar éste servicio es delicada y requiere una clasificación muy cuidadosa para evitar la invasión a la privacidad de los clientes. Por esta razón la mayoría de ella es clasificada como confidencial.

La información contenida en los activos de HLR y VLR correspondiente a la información de la localización, es información vital que soporta el servicio, sin embargo se considera confidencial únicamente, en lugar de restringida, debido a que la información almacenada ya se encuentra cifrada, por lo tanto, aún cuando algún atacante accesara a ella sería complicado poder descifrarla.

Como pública se puede considerar la información para el usuario almacenada en el servidor de contenido, y se considera de ésta clasificación, ya que aún siendo personalizada, su acceso es del dominio público.

El IMEI, que sirve para identificar como única una terminal móvil, debe estar restringido al uso interno de la organización, debido a que en caso de ser divulgada esta información, se podrían deducir datos privados, como por ejemplo, la cantidad de móviles e incluso qué móviles específicamente pertenecen al operador y esta información podría ser usada por los competidores.

En la siguiente tabla se clasifica la información de los activos a proteger en la aplicación de M-Health.

M-Health											
Información											
Autenticación		Back-end		Alarmas		Web		Syslog		Antivirus	
Nombres de usuarios	C	Información del usuario (recetas, análisis, historiales médicos)	R	Archivos de configuración	I	Cuentas con nombre y contraseña de usuarios	R	Registros de eventos de los operadores	C	Bases de datos de equipos en el dominio	C
Contraseñas de cuentas de usuario	R			Perfil de los usuarios	C	Archivos de acceso	C	Registros de eventos de la infraestructura	C	Versión del antivirus instalado en cada equipo	C
Perfiles de usuario	C					Niveles de permiso	R			Versión de S.O. de cada equipo	C

Donde: P = pública, I = Interna, C = confidencial, R = restringida

Tabla 6. Clasificación de la información de M-Health

En el caso de M-Health, tercera generación es una plataforma para el soporte de la aplicación, por lo tanto los activos a proteger no son propiedad del operador. El hospital o centro especializado de la salud, es el responsable de la seguridad de la información, sin embargo, su clasificación se debe hacer tomando en cuenta de igual modo de acuerdo al valor de la información.

La información crítica a proteger en este servicio corresponde a la información del usuario, las contraseñas para el servicio de autenticación y los niveles de permiso. Esta información es indispensable para la aplicación de M-Health y en caso de ser corrompida generan conflictos que comprometen seriamente a la corporación pudiendo provocar incluso su desintegración, ya que la índole de la información resulta demasiado significativa.

Como se menciona en los servicios anteriores la información clasificada como confidencial es aquella que genera problemas graves para la empresa sin llegar a significar su quiebre.

Los archivos de configuración se clasifican internos ya que son un recurso importante para poder administrar las alarmas adecuadamente. El sistema de alarmas consiste en avisar al usuario de las diversas actividades que deben llevarse a cabo (análisis, chequeos, historiales, citas, etc.) para controlar mejor el cuidado de su salud. Como se puede notar estos archivos resultan importantes más no imprescindibles para la subsistencia de la organización.

5.3 Análisis de Riesgo

Un riesgo puede verse como una proximidad de peligro, evaluarlos y determinar la mejor forma de administrarlos representa un gran desafío. Tratar de cubrir todos los riesgos posibles y prever todas sus consecuencias es complejo, debido a que es imposible eliminar la incertidumbre de un evento al cien por ciento. Sin embargo el análisis de riesgo representa una forma sistemática de evaluar mejor los riesgos, simplificarlos y resolver gran parte de las dudas con respecto a ellos.

Probabilidad	Impacto	Nivel de Riesgo
Alto	Alto	Muy Alto
Alto	Medio	Alto
Alto	Bajo	Medio
Medio	Alto	Alto
Medio	Medio	Medio
Medio	Bajo	Bajo
Bajo	Alto	Medio
Bajo	Medio	Bajo
Bajo	Bajo	Muy bajo

Tabla 7. Métrica para determinar el nivel de riesgo

No existe una única forma de realizar el análisis de riesgos, el que se emplea en esta tesis es el ISO 17799 y el nivel de riesgo se lleva acabo de acuerdo a la tabla 7.

El nivel de subjetividad aplicado en el análisis de esta tesis es alto, debido a la falta de información legal financiera y de procesos, como resultado de analizar una tecnología genérica y no una organización en particular. Este nivel reduce a medida que se cuente con mayor cantidad de datos de la organización y tomando en cuenta el criterio de los expertos responsables de la información.

En la siguiente tabla se lleva a cabo la definición de las amenazas bajo las cuales se define el nivel de riesgo más adelante.

Amenaza	Descripción
Acceso no Autorizado	Un usuario con permiso restringido a cierta información, accesa a ella deliberadamente o bien por accidente pero decide obtenerla.
Negación de Servicio	El activo recibe una desmesurada solicitud de peticiones, y al no ser capaz de responderlas todas, disminuye paulatinamente su rendimiento.
Software Malicioso	Cualquier programa malicioso o código móvil inesperado, ya sea virus, troyanos, gusanos o programas "broma", es decir, que simulan ser virus sin serlo.
Repudiación	La negación de información que ha sido enviada o recibida.
Brechas de seguridad debido a debilidades de la misma (controles incorrectos o no implementados)	La implementación de controles es incorrecta o peor aún no existe ninguno.
Brechas de seguridad debido a la incorrecta clasificación o manejo de información	No se da el valor apropiado a la información, por lo que el nivel de protección no es suficiente.
Uso indebido	La utilización incorrecta de la información, por ejemplo el chantaje.
Incidentes y fallas	Fallas o incidentes relacionados con la infraestructura física de la red, por ejemplo, el robo de un servidor. En el caso de la negación de servicio, no ocurre debido a una falla técnica o física de hardware, como en este caso, más bien es por software.
Seguridad física	Desastres naturales, incendios accidentales, tormentas, inundaciones, amenazas ocasionadas por el hombre, disturbios, sabotajes deliberados internos y externos.
Modificación no autorizada de la información.	Cambios o pérdida de información por personas no capacitadas para hacerlo.
Divulgación de información confidencial	Ventilación pública de información privilegiada.

Tabla 8. Descripción de amenazas.

La tabla 9 presenta el análisis de riesgo de las aplicaciones con la justificación del análisis.

Amenaza	P	I	NR	Aplicación	Justificación
Acceso no Autorizado	M	A	A	E-mail Localización M-Health	El acceso no autorizado, es un recurso no tan fácil para los atacantes, por lo tanto, aunque resulta atractivo para ellos fisgonear o burlar la seguridad de las redes, prefieren orientarse a otro tipo de ataques más sencillos que causan mayor daño. El impacto es alto, porque si ocurre deja vulnerable cualquier información del operador a cualquier tipo de ataque que el infiltrado desee.
Negación de Servicio	A	A	MA	E-mail Localización M-Health	La probabilidad es alta, debido a que este tipo de ataques no es complicado y es común. El impacto se considera alto debido a que el resultado de este ataque resulta en el descenso de la calidad de servicio o bien en la terminación del servicio.
Software Malicioso	A	A	MA	E-mail Localización M-Health	Es de los ataques más comunes actualmente, con gran número de herramientas (gusanos, troyanos, bromas, etc.) y con mayor impacto en el negocio, ya que tiene la capacidad de causar daños graves, como por ejemplo, pérdida de información y daños lógicos.
Brechas de seguridad debido a debilidades de la misma (controles incorrectos o no implementados)	A	A	MA	E-Mail Localización M-Health	La probabilidad de esta amenaza es alta debido a que por lo general no se tiene la cultura en cuanto a la seguridad de la información en las organizaciones y como consecuencia se crean huecos permitiendo la corrupción de a información, generando alto impacto en el negocio.
Brechas de seguridad debido a la incorrecta clasificación o manejo de información	M	A	A	E-Mail Localización M-Health	La información por lo general no se clasifica adecuadamente, no se le da el valor necesario, sin embargo hoy en día se toma más en cuenta, por lo que la probabilidad disminuye un poco, aún así en caso de ocurrir, información importante corre el riesgo a quedar vulnerable ante diversos ataques.
Repudiación	B	B	MB	M-Health	Tanto la probabilidad como el impacto de que este ataque suceda, es muy bajo, debido a que la relación entre médico-paciente se basa principalmente en la confianza.
Uso indebido	B	M	B	E-mail Localización	En el caso del e-mail y localización es difícil que el atacante encuentre información para usar inadecuadamente, aún en el caso de las contraseñas, estas pueden ser cambiadas en cualquier momento por los propietarios de las mismas, sin embargo el tiempo que transcurre mientras el problema es solucionado puede causar problemas al operador, es por esto que su nivel de impacto es medio.
	A	A	MA	M-Health	La información de los usuarios en M-Health se presta a su uso indebido ya que es tan importante que puede ser utilizada para chantajes, por poner un ejemplo. El impacto si esto ocurre es de alto nivel para la organización, debido a que puede representar incluso su fracaso.

Amenaza	P	I	NR	Aplicación	Justificación
Incidentes y fallas	A	A	MA	E-Mail Localización M-Health	La probabilidad de que la infraestructura física de la red falle es alta, por lo general siempre existen problemas de hardware en los equipos, como por ejemplo que el disco duro de un servidor se queme. El impacto por supuesto es alto para el operador ya que además de la pérdida de información representa una pérdida financiera.
Seguridad física	B	A	M	E-Mail Localización M-Health	La probabilidad de un desastre natural es remota, sin embargo cuando esto ocurre, por lo general, deja una organización inactiva, ocasionando pérdidas financieras altas, de información y de equipo.
Modificación no autorizada de la información.	B	M	B	E-mail Localización	Es poco probable que el atacante se interese en modificar los correos, el contenido de los servicios de localización (publicidad, clima, etc.) o las claves de los usuarios, recurren más a otro tipo de ataques como negación de servicio. El impacto es de nivel medio ya que, para los operadores, si esto ocurre puede crear un problema de administración de correos o bien el descontento de los usuarios.
	M	A	A	M-Health	La probabilidad es media, ya que no se trata de una amenaza tan fácil de realizar, sin embargo la modificación de la información en esta aplicación, puede causar desprestigio de los especialistas, del hospital y por supuesto daños irreparables al usuario. Un ejemplo sería que alguien modificara el historial clínico de un paciente.
Divulgación de información confidencial	B	M	B	E-mail localización	Por lo general en estos servicios es poco probable que se envíe información demasiado confidencial, y los activos de contraseñas, por lo general contienen información cifrada por lo que la probabilidad de divulgarla disminuye. Aunque la probabilidad es baja el riesgo se considera medio ya que, el operador tiene la obligación de proteger la información del usuario independientemente de su importancia.
	A	A	MA	M-Health	La información manejada en este servicio es muy importante, por lo que se vuelve foco de atención de los atacantes malintencionados, es por ello que la probabilidad de ocurrencia es alta. El impacto que puede causar divulgar información de los usuarios en este servicio causa problemas legales, financieros y definitivamente de imagen y credibilidad de los usuarios.

Donde: P = probabilidad, I = impacto, NR = nivel de riesgo, A = alto, M = medio, B = bajo, MA = muy bajo, MB = muy bajo

Tabla 9. Análisis de Riesgo de todas las aplicaciones

5.4 BIA (Análisis de Impactos en el Negocio)

Este tipo de análisis se debe realizar para entender el impacto de una pérdida o de una reducción en las actividades críticas de la funcionalidad del negocio. El BIA permite clasificar, establecer prioridades y orden de restablecimiento de los procesos que soportan a la organización, para asegurar su pronta recuperación para que la productividad no se vea afectada.

El impacto en el negocio se puede realizar mediante la formulación de diversas preguntas que permitan visualizar el impacto en caso de que algún riesgo llegue q materializarse.

- **¿Cuál es la información más importante a proteger?**

E-mail. La información más crítica en este servicio es aquella almacenada en el activo de autenticación, ya que, amenaza la administración de los usuarios y como consecuencia la disponibilidad de la información. El servidor de antivirus también pone en riesgo esta característica de la información, ya que si algún software malicioso atacase este activo, podría provocar incluso la destrucción de los correos de los usuarios impidiendo al operador proporcionar el servicio.

Localización. En el servicio de localización lo más importante es la privacidad del usuario, por lo tanto la información crítica a proteger es aquella que mediante algún tipo de ataque, amenace la confidencialidad de la localización o identidad del usuario. El activo de autenticación es una amenaza potencial a estos aspectos.

M-Health. En esta aplicación la mayoría de la información resulta crítica, sin embargo aquella que amenace fuertemente su integridad, es la que requiere mayor protección. Los activos de autenticación, Back-end y web, son los que exigen mayor nivel de seguridad.

- **¿De quién se desea proteger esta información?**

En general toda la información de las diferentes aplicaciones se desea proteger de personas malintencionadas cuya finalidad es hacer daño, robar información privada, dañar bases de datos, fisgonear, usar el correo electrónico ajeno y hasta hurtar valores.

Sin embargo, también se desea establecer medidas de control para hacer frente a los ataques accidentales, en los que la información resulta dañada, debido a la falta de conocimiento en materia de seguridad por parte de los propietarios de la información, En este caso los operadores y los centros especializados en la salud.

- **¿Cuál es la probabilidad de amenaza y la vulnerabilidad de la Organización?**

Por lo general, cuando se habla de una tecnología como en este caso, tercera generación, el tema de seguridad tiende a ligarse a la automatización de procesos y requerimientos tecnológicos, por ejemplo, firewalls, antivirus y sistemas de respaldos. Como consecuencia se da poca importancia a otro tipo de herramientas como el establecimiento de políticas y la documentación de las mismas, para mejorar en mayor grado la administración de la seguridad de los activos.

Y si bien ninguno de los puntos es determinante por sí mismo en conjunto e interacción, proponen una buena solución a los problemas de seguridad.

De este modo, se puede deducir que la probabilidad de amenaza y vulnerabilidad de los propietarios de la información representa un problema fuerte en la actualidad, debido a la falta de integridad de esos factores. Además se puede agregar que el grado de sofisticación de los atacantes crece con la misma velocidad con que la tecnología avanza.

- **¿Qué tan importante es el recurso (costo estimado de perdidas, si algunas de las amenazas fuesen realizadas)?**

Es difícil determinar las pérdidas exactas en costo ya que el análisis se refiere a una tecnología y no a una organización en particular. Debido a esto el costo estimado de pérdidas varía dependiendo de los servicios que un operador en particular ofrece, y cuál representa mayores ganancias.

Para poder establecer cuál es el impacto en el negocio de cada aplicación es necesario priorizar las características de la información por su importancia.

E-mail: En esta aplicación la cualidad más importante es la disponibilidad de la información, ya que en caso contrario causa el descontento de los usuarios. La siguiente característica es la Integridad de la información, debido a que en caso de que cierta información llegara a ser modificada, puede causar que los correos no lleguen a su destino originando la no disponibilidad de la información. En último caso se encuentra la confidencialidad, puesto que, aunque sí resulta importante tener cierta protección en contra de la divulgación de la información, cuando esta es accesada por el usuario y sale de los dominios del operador viajando por una red pública, se vuelve vulnerable a las amenazas de la misma, por lo que pierde un poco el sentido de resguardarla bajo demasiada seguridad.

Localización: En este caso la confidencialidad es la característica más importante a tomar en cuenta para establecer las políticas y controles de seguridad en los activos que pertenecen a esta aplicación. La Integridad de la información, es una cualidad importante, ya que si es modificada de algún

modo puede generar errores enviando información equivocada del servicio. Por último se lista la disponibilidad, ya que la información requerida por el usuario no es de vital importancia, es preferible que el servicio no esté disponible determinado tiempo, a poner en riesgo su privacidad o bien otorgarle datos erróneos.

M-Health: La integridad de los datos es la característica más importante debido a que la información que en esta aplicación se maneja es crítica para los usuarios, la modificación de un historial clínico por ejemplo, resulta inaceptable en este servicio. Una vez estableciendo controles para proteger la integridad de los datos, se debe tomar en cuenta la confidencialidad, ya que la divulgación de la información en este servicio puede causar problemas fuertes para el propietario de la misma, tales como legales, financieros o de imagen. La disponibilidad, ciertamente es una característica importante en cualquier servicio, sin embargo en ésta aplicación, no resulta crítica ya que el descontento de los usuarios no es tan prioritario como el cuidado de la salud.

De acuerdo a las siguientes tablas, por cada aplicación se establece la relación entre el tipo de impacto (financiero, legal, de imagen, cambio en las actividades del negocio y desconfianza) que causa la corrupción de cada activo y las características de la información ya mencionadas con anterioridad. Esto permite observar cuáles son los activos más críticos de cada servicio analizado.

Activo	E-mail Aspectos de Impacto al Negocio No disponible (Disponibilidad)					Destrucción (Disponibilidad)					Divulgación (Confidencialidad)					Modificación (Integridad)				
	F	**L**	**I**	**C**	**D**	**F**	**L**	**I**	**C**	**D**	**F**	**L**	**I**	**C**	**D**	**F**	**L**	**I**	**C**	**D**
DNS	X		X	X	X	X		X	X	X			X		X				X	
Autenticación	X	X	X	X	X	X	X	X	X	X	X	X	X		X			X	X	X
Correos	X		X		X	X		X		X			X		X			X		X
HLR					X					X			X		X				X	
VLR					X					X			X		X				X	
Syslog				X					X						X				X	X
Antivirus	X		X	X	X	X		X	X	X					X				X	

Donde: F = financiero, L = legal, I = imagen, C = cambio en las actividades del negocio, D = desconfianza.

Tabla 10: Relación Impacto activo – Característica de la información en el servicio de E-mail

Como se observa en la tabla 10 si el servidor DNS es comprometido, los vínculos establecidos entre los destinatarios y sus correos pueden perderse, en este caso los correos no llegarían al usuario final inutilizando la disponibilidad del servicio. Debido a esto se puede establecer que este activo resulta muy crítico, como se puede observar en la tabla 11.

La corrupción del servidor de autenticación impacta en mayor grado la disponibilidad del servicio, por lo tanto se puede determinar muy crítico.

Aunque en el previo análisis de la información, el contenido se clasificó como confidencial y no restringido, en el análisis de impacto al negocio se toman en cuenta diferentes aspectos a los accesos de datos, es por esto que observando la tabla X, se observa que si el servidor de correos es corrompido, puede incluso perderse la información del usuario impidiendo la disponibilidad del servicio, por lo tanto se considera muy crítico.

El HLR y VLR se analizan igual, debido a que la información contenida en ellos es parecida. En este caso, si la información de estos activos es divulgada causaría desconfianza y cierta pérdida de imagen en cuanto a la seguridad con que el operador protege la información de los usuarios.

El syslog que es el activo en el cual se almacenan los registros de eventos tanto del operador como de la infraestructura, permite llevar un control de las actividades realizadas, los accesos y las fallas de equipo. Si la integridad de estos registros se ve amenazada, puede generar desconfianza y confusión de quienes tuvieron acceso a que tipo de información durante el tiempo en que se repara la falla, dando lugar a un ataque sin poder determinar el responsable. Según el orden de importancia se clasifica como crítico.

El antivirus es un activo muy importante para el mantenimiento de la disponibilidad de la información, ya que en caso de ser corrompido podría ocasionar que los demás activos estén en riesgo y la información sea incluso destruida. Por esto se considera un activo muy crítico.

En la siguiente tabla se resume los activos y su clasificación en muy crítico, crítico y no crítico.

E-mail			
Activo	Muy crítico	Crítico	No crítico
Autenticación	X		
Correos	X		
Antivirus	X		
Syslog		X	
DNS	X		
HLR			X
VLR			X

Tabla 11. Nivel crítico de los activos de la aplicación de E-mail

Activo	Localización Aspectos de Impacto al Negocio No disponible (Disponibilidad)					Destrucción (Disponibilidad)					Divulgación (Confidencialidad)					Modificación (Integridad)				
	F	**L**	**I**	**C**	**D**	**F**	**L**	**I**	**C**	**D**	**F**	**L**	**I**	**C**	**D**	**F**	**L**	**I**	**C**	**D**
Autenticación			X					X			X	X	X	X	X			X		X
Contenido	X		X		X	X		X		X			X					X		X
HLR			X					X					X		X			X	X	X
VLR			X					X					X		X			X	X	X
Syslog					X					X					X					X
Antivirus			X	X	X			X	X	X			X		X					X

Donde: F = financiero, L = legal, I = imagen, C = cambio en las actividades del negocio, D = desconfianza.

Tabla 12: Relación Impacto activo – Característica de la información en el servicio de localización

El servidor de autenticación se considera muy crítico debido a que su corrupción afecta la confidencialidad del usuario, como se puede ver en la tabla 12. El activo de contenido impacta directamente a la disponibilidad, un aspecto que vale la pena mencionar es que algunas compañías establecen contratos de tiempo de reestablecimiento del servicio, ocasionando pérdidas financieras durante el período en el cual el servicio no se encuentre disponible. En este caso se clasifica no crítico, como se muestra en la tabla 13.

El HLR y VLR afectan la integridad de la información, ya que si ésta información es modificada afecta la eficiencia del servicio. Es importante dejar en claro que no afecta directamente la confidencialidad del usuario, porque la información contenida en estos activos se encuentra cifrada, por lo que resulta difícil su divulgación, por lo tanto el atacante se limita a causar mayores daños mediante su modificación o destrucción. Su clasificación es crítica.

De acuerdo a la tabla 13 el antivirus y el syslog se clasifican no críticos debido a que su mayor impacto es en la disponibilidad de los datos.

Localización			
Activo	Muy crítico	Crítico	No crítico
Autenticación	X		
HLR		X	
VLR		X	
Contenido			X
Syslog			X
Antivirus			X

Tabla 13. Nivel crítico de los activos de la aplicación de localización

M-Health Aspectos de Impacto al Negocio																				
Activo	No disponible (Disponibilidad)					Destrucción (Disponibilidad)					Divulgación (Confidencialidad)					Modificación (Integridad)				
	F	L	I	C	D	F	L	I	C	D	F	L	I	C	D	F	L	I	C	D
Autenticación			X		X			X		X	X	X	X	X	X	X	X	X	X	X
Back-end			X		X			X		X	X	X	X	X	X	X	X	X	X	X
Alarmas			X					X					X	X	X			X		X
Web			X		X			X		X	X	X	X		X	X	X	X	X	X
Syslog					X					X	X		X		X					X
Antivirus					X					X	X		X		X					X

Donde: F = financiero, L = legal, I = imagen, C = cambio en las actividades del negocio, D = desconfianza.

Tabla 14: Relación Impacto activo – Característica de la información en el servicio de M-Health

Como se observa en la tabla 14, el servidor de autenticación impacta en la integridad de la información en mayor medida, y dado que es la característica más importante en la aplicación de M-Health, se considera muy crítica.

El servidor de Back-end contiene la información del usuario y como se puede observar impacta, de igual modo que el activo de autenticación, en la Integridad de la información, por lo tanto se considera muy crítica, como se muestra en la tabla 15.

Las alarmas son un servicio importante para esta aplicación, y en caso de comprometerse la información ahí contenida se pone en riesgo la confidencialidad del usuario, su clasificación es crítica.

El servidor web, contiene niveles de permiso y cuentas de usuario entre otros, y si esta información es corrompida, impacta en mayor grado la integridad de la información del usuario, por lo tanto se clasifica como muy crítica.

El servidor de syslog y antivirus amenazan la característica de confidencialidad en la información, debido a esto se considera información crítica, como se muestra en la tabla de abajo.

M-Health			
Activo	Muy crítico	Crítico	No crítico
Autenticación	X		
Back-end	X		
Web	X		
Alarmas		X	
Syslog		X	
Antivirus		X	

Tabla 15. Nivel crítico de los activos de la aplicación de localización

- **¿Qué medidas se pueden implementar?, ¿Son efectivas en costo y tiempo?**

Los controles necesarios para gestionar la seguridad de la información se establecen de acuerdo a las amenazas establecidas anteriormente y al ISO 17799, como se muestra en la tabla 16.

El ISO 17799 es una norma internacional que ofrece recomendaciones para proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización

Amenaza	Controles
Acceso no Autorizado	5.2.1 Clasificación de directrices 5.2.2 Clasificación y manejo de la información 6.1.4 Términos y condiciones de empleados 8.3.1 Controles en contra de SW malicioso 8.5.1 Controles de red 8.6.3 Manejo de procedimientos de información 9.1.1 Política de control de acceso 9.2.1 Registro de usuarios 9.2.2 Administración de privilegios 9.2.3 Administración de contraseñas de usuarios 9.2.4 Revisión de derechos de acceso de usuario 9.3.1 Uso de contraseñas 9.4.1 Política de uso de servicios de la red 9.4.3 Autenticación de usuarios de conexiones externas 9.4.5 Segregación de la red 9.4.7 Controles de conexión de red 9.4.9 Servicios de seguridad de red 9.5.1 Autenticación de terminales 9.5.2 Procedimientos Log-on de terminales 9.5.3 Identificación y autenticación de usuarios 9.5.4 Sistema administrador de contraseñas 9.6.1 Restricción de acceso a la información 9.7.1 Registro de eventos 9.7.2 Monitoreo de uso del sistema 10.2.3 Autenticación de mensajes 10.2.4 Validación de datos de salida 12.1.3 Guardar los registros de la organización
Negación de Servicio	8.5.1 Controles de red 8.7.6 Política de sistemas disponibles 8.7.7 Otras formas de intercambio de información
Código Malicioso	8.1.5 Separación del desarrollo y las instalaciones operacionales 8.3.1 Controles en contra de software malicioso 8.4.1 Información de respaldo 8.7.4 Seguridad en el correo electrónico
Repudiación	8.7.6 Política de sistemas disponibles 10.3.2 Servicios de no repudiación
Brechas de seguridad debido a debilidades de la misma (controles incorrectos o no implementados)	4.2.1.7 Revisión independiente de la seguridad de la información 4.4.3.2 Reporte de las debilidades de la seguridad 4.6.2.2 Sistemas de aceptación 4.6.4.3 Reporte de faltas 4.10.2.1 Conformidad con las políticas de seguridad 4.10.2.2 Comprobación de la conformidad técnica
Brechas de seguridad debido a la incorrecta clasificación o manejo de información	4.3.2.1 Directrices de clasificación 4.3.2.2 Clasificación y manejo de la información
Uso indebido	4.6.1.4 Segregación de funciones 4.10.1.5 Prevención del uso indebido de las instalaciones del procesamiento de información 7.3.2 Retiro de la propiedad 8.6.1 Disposición del medio

Amenaza	Controles
Incidentes y fallas	4.1.1.1 Documento de la política de seguridad de la información 4.1.1.2 Revisión y evaluación 4.2.1.5 Aviso de los especialistas en la seguridad de la información 4.2.1.6 Cooperación entre organizaciones 4.4.3.1 Reporte de incidentes de seguridad 4.4.3.4 Aprendizaje de incidentes 4.6.1.3 Procedimientos de gestión de incidentes 4.2.1.4 Procesos de autorización para las instalaciones de procesamiento de información. 4.6.1.5 Separación del desarrollo y de instalaciones operacionales 4.6.2.1 Planeación de capacidad 4.6.2.2 Aceptación del sistema 4.6.4.1 Respaldo de la información 4.7.7.2 Uso de sistemas de monitoreo 4.8.2.1 Validación de la entrada de datos 4.8.5.1 Procedimientos de control de cambios
Seguridad física	7.1.1 Perímetro de seguridad física 7.1.2 Controles de acceso físicos 7.1.3 Seguridad en oficinas, cuartos e instalaciones. 7.2.1 Protección y ubicación de equipo 8.4.1 Información de respaldo 6.1.2 Investigación y política del personal 7.2.4 mantenimiento de equipo 7.2.2 Suministros de poder

Tabla 16. Controles de acuerdo al ISO 17799

5.5 Arquitecturas

En base a los estudios realizados se puede diseñar una arquitectura con los elementos de seguridad necesarios para minimizar los riesgos de un ataque.

Hasta ahora las aplicaciones de E-mail y Localización se han trabajado de forma independiente con el fin de llevar a cabo un análisis confiable y objetivo de cada activo involucrado en las aplicaciones. Sin embargo para poder proponer una arquitectura a nivel operador, es necesario tomarlas en cuenta al mismo tiempo, ya que, el operador establece una sola red para ofrecer todos sus servicios y sería muy costoso y complicado establecer una arquitectura de red diferente para cada aplicación.

Como se puede observar en la figura 15 se propone una arquitectura con activos separados.

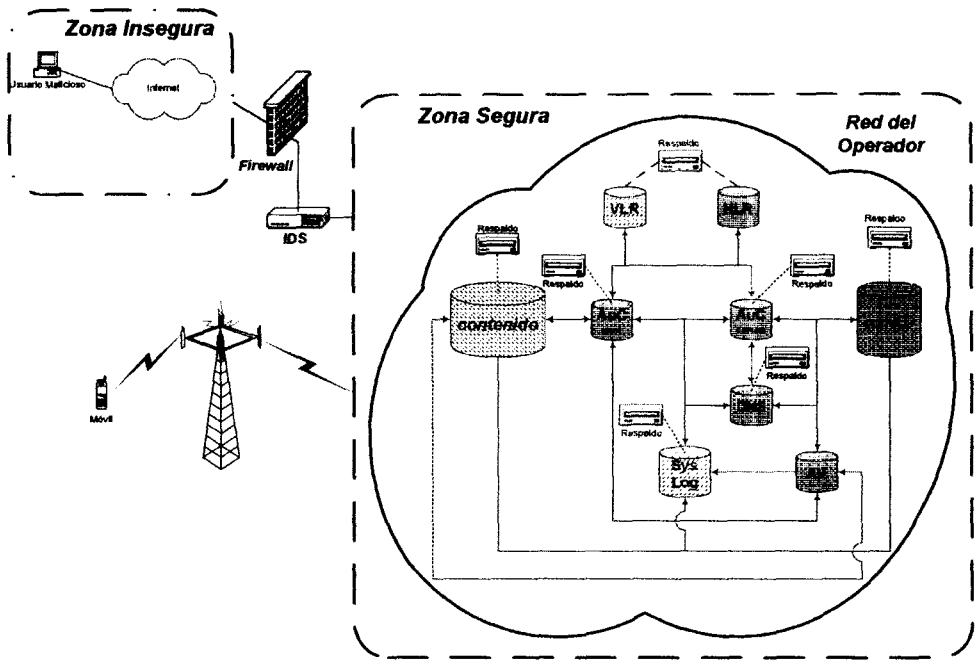

Figura 15. Arquitectura de seguridad propuesta para las aplicaciones de E-mail y localización.

La arquitectura se divide en dos grandes zonas, la insegura, sobre la cual no se tiene algún tipo de control y la zona segura la cual pertenece al operador. Entre estas dos zonas se sugiere implementar un firewall para filtrar tráfico sospechoso e inmediatamente se implementa un IDS (Intrusion Detection System), para detectar posibles ataques a los componentes de la red interna (activos) que no han sido detectados por el firewall.

El servidor de contenido y de correos que contienen la información que es enviada al usuario cuando realiza una petición de servicio de E-mail o de Localización respectivamente, se almacenan en activos diferentes, ya que en caso de ataque sólo se afecta a una aplicación al mismo tiempo, minimizando el impacto al negocio.

Los activos que como consecuencia de sufrir daño originen la pérdida del servicio se manejan también de forma independiente, estos activos son el de autenticación correspondiente al correo y al de contenido. El servidor de antivirus es único para todos los servicios y hay que asegurar su utilización y actualización constante para evitar el ataque de software malicioso. El Syslog se maneja de igual forma, ya que, guarda los registros de todos los demás activos en caso de falla y resultaría un gasto innecesario poner uno para cada aplicación. El HIR y VLR por cuestiones de diseño no pueden ser más de uno por cada operador. Por último el DNS es único, ya que sólo se utiliza para la aplicación de E-mail.

A pesar de la segregación de activos y la utilización adecuada del antivirus, sería tonto confiar en los sistemas de almacenamiento, los cuales no están exentos de fallas de infraestructura. Por este motivo se propone un sistema de respaldo para los activos resguardando la información que almacenan, generando copias de seguridad para poder restaurar la información en casos de emergencia.

Los sistemas de respaldo se proponen de forma independiente para todos los activos excepto el antivirus, HLR y VLR. En el caso del antivirus no tiene caso establecer el respaldo, debido a que en caso de falla se instala nuevamente y se actualiza con una velocidad de respuesta aceptable. Para salvaguardar la información del HLR y VLR se propone un sistema de respaldo único ya que su información es similar.

El DNS requiere también sistema de respaldo para que en caso de emergencia, pueda ser restaurado lo antes posible evitando que peligre la disponibilidad del servicio debido a la carencia de vínculos para el direccionamiento de los correos.

El Syslog no contiene información propiamente indispensable para los servicios que ofrece el operador, sin embargo la velocidad de restauración de la información en casos de desastre es muy importante y los respaldos aumentan esta velocidad considerablemente. Además cierta información ahí almacenada está configurada de acuerdo a las necesidades del operador y en muchos casos no es sencillo obtener de nuevo esa personalización, en cuyo caso los respaldos aportan una valiosa ayuda.

La arquitectura propuesta para la aplicación de M-Health se ilustra en la siguiente figura.

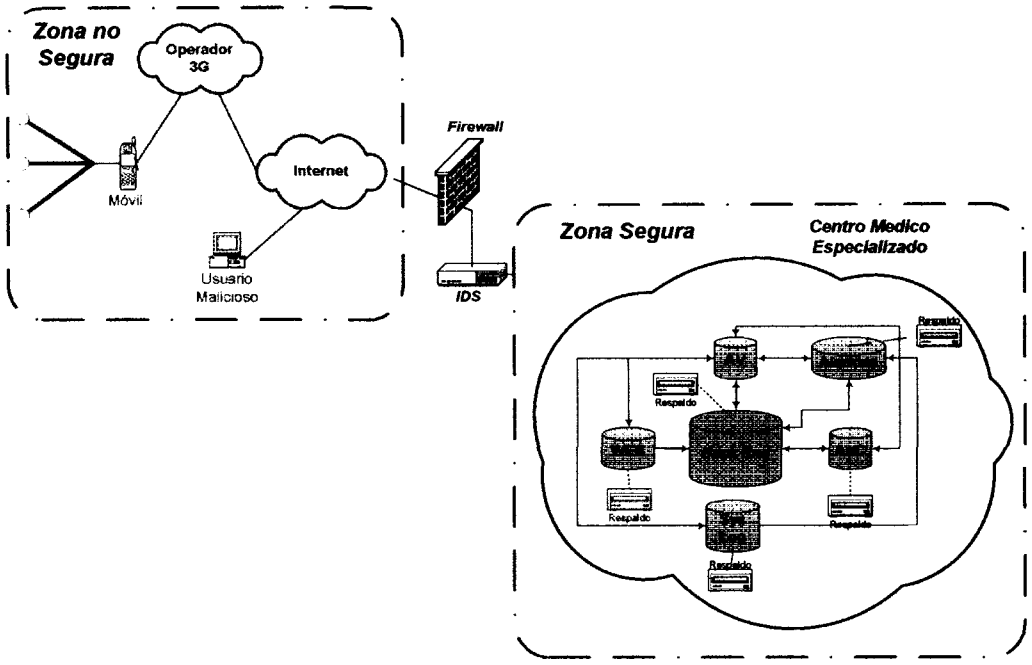

Figura 16. Arquitectura de seguridad propuesta para la aplicación de M-Health

En este caso la propuesta se realiza de forma independiente a las aplicaciones anteriores, debido a que el propietario de la información, no es el operador, sino el centro médico especializado de la salud.

De igual forma se pueden distinguir dos zonas (insegura y segura) dividida por un firewall seguido de un IDS, para evitar lo más posible la intrusión de usuarios maliciosos a la red interna de la organización.

El antivirus no cuenta con sistema de respaldo por el mismo motivo que en el servicio de localización. El resto de los activos cuentan cada uno con su sistema de respaldo para minimizar el daño en caso de ataque o desastre y establecer tiempos de restauración del servicio con velocidades óptimas.

5.6 Políticas

La falta de políticas de seguridad en la información es uno de los mayores problemas que las organizaciones enfrentan actualmente. Por lo general las corporaciones consideran que la compra de nuevos productos de hardware, software o contratación de servicios, son suficiente para proteger sus activos ignorando el hecho de que los usuarios son la principal causa de ataques, daños y fallas a las tecnologías de información.

Las políticas permiten establecer controles y procedimientos para saber manejar asuntos de seguridad y proteger los activos estableciendo medidas de protección como puede ser el uso de contraseñas, el antivirus y el registro de eventos entre otros.

En general las políticas establecen metas y objetivos generales de los usuarios en relación a las violaciones de la seguridad, y si bien estas varían considerablemente según el tipo de organización, es posible establecer medidas genéricas aplicables a los servicios particulares analizados en ésta tesis.

Por ejemplo el 11 de Agosto de 2003 se propagó el gusano informático conocido como Blaster, el cual atacó máquinas con sistema operativo Microsoft Windows 2000, Windows XP y NT, explotando una vulnerabilidad del tipo "Buffer Overflow". El gusano tenía como objetivo además de propagarse, realizar un ataque de negación de servicio distribuido al sitio windowsupdate.com y utilizaba diversos puertos de protocolos TCP y UDP para ello, por lo que la actividad generada hacia estos puertos identificados indicaba la infección a nivel red. Además el gusano estaba diseñado para propagarse en máquinas en la misma red y aleatoriamente. (Morales, 2004)

En este caso algunas de las políticas y controles establecidos en la tesis como aquellas referentes a software malicioso (antivirus), acceso remoto, respaldo de información y monitoreo de eventos pueden minimizar enormemente los daños e incluso evitar el ataque.

Por lo tanto, resulta evidente que, a pesar de que la implementación de políticas tiene cierto costo para la organización, el riesgo de asumir las consecuencias si un ataque importante se lleva a cabo, es mucho mayor, ya que los daños no se limitan únicamente a pérdidas financieras, también pueden implicar daño de equipo, pérdida de información importante, del servicio, de imagen e incluso generar demandas y desconfianza por parte del usuario.

5.6.1 Contraseñas

Las contraseñas son un aspecto importante para la seguridad de las organizaciones, pues son la primera frontera de protección de las cuentas de los usuarios. Una contraseña insegura puede resultar un alto riesgo para la red del propietario de la información, ya sea el operador o el centro especialista de la salud. Todos los usuarios que utilicen los sistemas de la compañía son responsables seguir los lineamientos adecuados para asegurar sus contraseñas.

- **Propósito**

El propósito de esta política es establecer un estándar para la creación, fortalecimiento y protección de las contraseñas.

- **Alcance**

El alcance de esta política incluye a todo usuario que tiene o es responsable de una cuenta o acceso que requiera el uso de contraseña, o

quien tenga acceso a la red y a los sistemas que residen dentro de la organización.

- **Política**

Para mantener la confidencialidad de la información cualquier personal que labore en estas organizaciones o que cuente con algún acceso a los sistemas, grupos de trabajo, redes y aplicaciones, deberá tener una contraseña segura, única y diferente a otros usuarios.

- **Directrices**

1) Las contraseñas, para almacenarse en algún sistema de cómputo, deberán mantenerse cifradas, si esta condición no se cumple ninguna contraseña podrá ser almacenada en algún archivo.
2) Las contraseñas no serán compartidas con nadie, incluyendo personal administrativo, secretarias, compañeros de trabajo, jefes directos, familiares, otros usuarios, administradores de red, etc.
3) Las contraseñas no deberán ser reveladas por teléfono, e-mail o cualquier otro medio electrónico.
4) Si alguien requiere de una contraseña, hacer referencia a este documento para elaborarlo y dirigirse con el personal correcto.
5) No escribir ni almacenar las contraseñas (oficinas, o cualquier otro sitio público).
6) Las contraseñas serán renovadas al menos una vez cada 4 meses.
7) Cualquier anomalía o situación sospechosa con su contraseña se deberá reportar con el personal adecuado.
8) Evitar crear contraseñas con alguna de las siguientes características:

    - Palabras encontradas en un diccionario.
    - Palabras de uso común como: Nombres de familia, mascotas, amigos, compañeros de trabajo.
    - Nombre de computadora, comandos, hardware, software.
    - Palabras derivados del nombre de la compañía.
    - Cumpleaños o información personal de teléfonos, direcciones.
    - Palabras o números con patrones como 12345, abcd, xxxyyy

9) Procurar crear contraseñas que puedan ser fácilmente recordadas.
10) Para fortalecer las contraseñas se pueden utilizar:

    - Contener la combinación de mayúsculas y minúsculas
    - Tener caracteres y letras
    - Tener por lo menos una longitud de 8 caracteres alfanuméricos.

5.6.2 Acceso Remoto

El acceso remoto para el caso particular de las aplicaciones analizadas en esta tesis es la capacidad de acceder a la red de la organización desde cualquier teléfono móvil, para obtener los beneficios de los servicios ofrecidos

por los operadores y centros médicos especializados de la salud. En casos particulares como el acceso al e-mail, se puede acceder desde otro tipo de dispositivos como computadoras personales o portátiles.

Debido a que una gran mayoría de ataques son realizados remotamente, resulta imprescindible para las organizaciones establecer procesos que le permitan administrar y controlar efectivamente este tipo de accesos para evitar pérdidas importantes.

- **Propósito**

El propósito de esta política es definir los estándares y lineamientos para una conexión remota a la red de la organización desde cualquier punto. El objetivo es minimizar cualquier exposición y daño a los datos, sistemas o aplicaciones de la compañía por cualquier acceso no autorizado.

- **Alcance**

Esta política se aplica a cualquier usuario que se conecte desde cualquier dispositivo móvil a la red de la empresa. La política aplica a cualquier acceso remoto a la compañía incluyendo conexión a las bases de datos, correos, sistemas, aplicaciones y redes.

- **Política**

Es responsabilidad de los usuarios que cuenten un privilegio de conexión remota a la red del operador de asegurarse que dicha conexión sea establecida por un servicio definido por la organización.

Es responsabilidad de los usuarios con acceso remoto y acceso a Internet de no realizar actividades ilegales y ajenas a los intereses del negocio.

- **Directrices**

1) Un acceso remoto seguro debe estar estrictamente controlado. Los controles se establecen con una autenticación de usuario y contraseña única. (Ver Política de contraseñas).
2) Estarán prohibidos los accesos remotos fuera de los horarios establecidos por el personal de sistemas.
3) Las conexiones a la red de la organización pueden ser únicamente con equipo registrado en la compañía. Cualquier equipo no propiedad de la compañía que requiera acceso a la red, deberá cumplir con los estándares de seguridad y autenticación previamente establecidos y autorizados por el personal de la organización.
4) Únicamente usuarios con contrato o pertenecientes a la organización podrá estar conectado vía remota a la red de la compañía y no podrá estar conectado simultáneamente a otra red.
5) No están permitidos los cambios importantes de configuración de conexión sin autorización.

5.6.3 Servidores

Los servidores son un activo importante que se encuentra presente en todas las organizaciones y su función varía de acuerdo a las necesidades de las mismas.

En muchos de los casos los servidores soportan las aplicaciones y servicios que una corporación ofrece, es por esto, que se necesita establecer políticas que protejan estos activos de ataques, daños y fallas.

- **Propósito**

El propósito de ésta política es establecer estándares para la configuración base del equipo de servidor interno que es propiedad del operador o bien del centro médico especializado y es operado por ellos mismos. La implementación efectiva de ésta política minimizará el acceso no autorizado para los propietarios de la información y tecnología

- **Alcance**

Esta política se aplica a todo el equipo de servidores manejados por el operador o centro médico especializado, y para servidores registrados bajo cualquier dominio de red que sea de propiedad interna.

- **Políticas**

Todos los servidores internos implementado deben ser manejados por un grupo operacional el cual es responsable de la administración del sistema.

La aprobación de las directrices de configuración de los servidores debe ser establecida y mantenida por cada grupo operacional, basándose en las necesidades del negocio. Los grupos operacionales deben supervisar la conformidad de la configuración y poner una política de excepción en ejecución adaptada a su ambiente.

- **Directrices**

1) Los servidores deben ser registrados dentro del sistema de gerencia corporativo de la empresa. Como mínimo la siguiente información es requerida para identificar el punto de contacto:

    - Contactos y localización de los servidores, y un contacto de respaldo
    - Hardware y sistemas operativos
    - Principales funciones y aplicaciones, si es aplicable.

2) La información en el sistema de gerencia corporativo de la empresa debe ser mantenida actualizada.

3) Los cambios de configuración para los servidores deben seguir los apropiados procedimientos de administración del cambio.
4) La configuración de los sistemas operativos debería estar de acuerdo con las directrices aprobadas de la organización.
5) Los servicios y aplicaciones que no serán usadas deben ser deshabilitadas.
6) El acceso a servicios debería ser registrado y/o protegido a través de métodos de control de acceso.
7) Los parches de seguridad más recientes deben ser instalados en el sistema tan pronto como se pueda, siendo una excepción cuando la aplicación interfiera con los requerimientos del negocio.
8) Las relaciones de confianza entre sistemas son un riesgo de seguridad, y su uso debería ser evitado. No usar relaciones de confianza cuando otro método de comunicación lo hará.
9) Utilizar siempre los estándares de seguridad de menor acceso para realizar una función.
10) Los servidores deben estar físicamente localizados en un ambiente de acceso controlado.
11) Los servidores están específicamente prohibidos del funcionamiento desde áreas incontroladas del cubículo
12) Las auditorias serán desempeñadas en una base regular por organizaciones autorizadas.
13) Todo esfuerzo será hecho para prevenir que las intervenciones causen faltas o interrupciones operacionales.

5.6.4 Análisis de Riesgos

El análisis de riesgos es una práctica fundamental en el proceso de establecimiento de políticas de seguridad dentro de una organización, ya que permite observar los puntos débiles donde se puede producir mayor daño en caso de un ataque.

La ejecución regular de esta práctica permite fortalecer los procesos de la organización disminuyendo su vulnerabilidad ante diversos peligros informáticos y establecer medidas de seguridad de acuerdo a los lineamientos corporativos de la empresa.

- **Propósito**

El propósito de esta política es fortalecer la seguridad de la compañía con una revisión periódica, por medio un análisis de riesgos para determinar las áreas vulnerables y así minimizar los riesgos.

- **Alcance**

El análisis de riesgos puede ser manejado por personal de la organización o por alguna compañía externa y debe de cubrir cualquier sistema de información incluyendo servidores, aplicaciones, redes y procesos.

- **Política**

Es responsabilidad de la organización la correcta ejecución, desarrollo e implementación de programas que evalúen los riesgos dentro de la misma. La cooperación de los empleados con el equipo del análisis de riesgos es importante para el desarrollo de un plan de contingencia.

- **Directrices**

1) Clasificar la información que se maneja dentro de la organización para evaluar el contenido, quien y como puede tener acceso a ella.
2) Detectar las vulnerabilidades y revisar periódicamente cualquier nueva vulnerabilidad de los sistemas, aplicaciones, servidores o redes de la compañía.
3) Analizar y listar todas las amenazas posibles a las que los sistemas, aplicaciones, servidores o redes de la organización pueden ser expuestos.
4) Evaluar cada vulnerabilidad y amenaza y definir controles para mantener un menor riesgo de incidencia.
5) De ser necesario ajustar o crear las políticas de seguridad y los procesos.

5.6.5 Antivirus

El antivirus es una herramienta poderosa que le permite a las organizaciones protegerse en contra de cualquier tipo de software malicioso.

La implementación física de la herramienta no es suficiente para asegurar una buena protección en contra de ataques, es necesario proporcionar el mantenimiento adecuado, con las actualizaciones y licencias necesarias para asegurar la efectividad de su función.

- **Propósito**

El propósito de esta política es implementar controles de seguridad que protejan a la organización contra cualquier tipo de software malicioso. De igual forma es necesario hacer conciente a los usuarios de la utilización apropiada de las tecnologías de información.

- **Alcance**

La política se aplica a todos los usuarios que tienen acceso a la red del operador.

- **Política**

Es de carácter obligatorio para la organización poseer un antivirus actualizado que asegure la protección de los activos donde se almacena la

información, contra cualquier tipo de software malicioso. Así mismo asegurar que los usuarios entiendan la importancia de respetar y aplicar esta política.

- **Directrices**

1) Evitar el uso de software pirata, adquiriendo las licencias y actualizaciones apropiadas.
2) Utilizar siempre el antivirus estándar de la organización, descargar e instalar las actualizaciones conforme estén disponibles.
3) Evitar siempre la descarga de archivos desde fuentes no fiables.
4) Almacenar los datos en un lugar seguro y respaldar la información crítica y configuraciones del sistema en una base de datos regular.
5) Actualizar periódicamente el antivirus debido a que nuevos virus son descubiertos cada día.
6) Realizar revisiones regulares del software y de la información crítica que soportan el negocio.
7) Investigar cualquier archivo sospechoso o no aprobado, incluyendo los provenientes de medios electrónicos y de redes no confiables.
8) Desarrollar procedimientos de capacitación de usuarios, responsabilidades y reportes en caso de ataques.
9) Implementar un plan de recuperación de la información, software necesario para la continuidad de servicios de la organización.
10) Manejar diversos niveles de alarma para determinar el grado de daño y urgencia del ataque.
11) La organización es responsable de adquirir las últimas noticias referentes a nuevos virus, analizarlas y desarrollar planes de ataque. Se bebe asegurar que las fuentes de información sean confiables.
12) Verificar si existen servicios obsoletos o innecesarios y removerlos.
13) En caso de haber activos infectados aislarlos hasta su recuperación para evitar comprometer a toda la organización.

5.6.6 Respaldo de información

Confiar ciegamente en los sistemas de almacenamiento implementados es un error que puede resultar muy costoso a la organización. La información no está exenta de ataques y en un caso extremo incluso podría darse su pérdida total. El caos que puede causar la pérdida de información valiosa va desde meses de documentación de procesos hasta cuentas de usuarios, contraseñas, perfiles de usuario e incluso información financiera crítica de la organización.

El respaldo de la información crítica minimiza el impacto de los ataques a la integridad de la información, mediante copias de seguridad proporcionando la opción de su recuperación hasta la última actualización almacenada. Por esta razón es de gran importancia establecer políticas que aseguren el respaldo periódico de información evitando daños mayores en caso de ataque.

- **Propósito**

Los mecanismos de respaldo y recuperación de la información son fundamentales para garantizar su restauración en caso de anomalías o daños en los activos y evitar que información crítica para las operaciones de la organización se pierdan indefinidamente.

- **Alcance**

Todo usuario que tenga relación con el almacenamiento, manipulación y procesamiento de la información generada por las diversas actividades de la organización.

- **Política**

Es obligación de la organización respaldar la información crítica que en caso de ser corrompida puede ocasionar daños irreversibles e impactos financieros severos. Además debe establecer los mecanismos de control apropiados para la restauración ordenada de los sistemas de información.

- **Directrices**

1) La organización debe proporcionar la infraestructura necesaria para asegurar que la información puede ser recuperada en caso de falla.
2) Se deben realizar copias periódicas del respaldo de la información.
3) Proporcionar niveles de protección física adecuados para los respaldos de la información.
4) Los sistemas de respaldos requieren su evaluación periódica para asegurar su correcta respuesta en caso de emergencia.
5) Así mismo se deben probar regularmente los procesos de restauración de la información, para asegurar su efectividad de operación y tiempo.
6) Asegurar que la organización cuenta con los procesos de respaldo y recuperación y que cumplen con las políticas relacionadas.
7) Especificar, seleccionar y administrar el uso de herramientas y paquetes de respaldo y recuperación de datos. Así como el uso de dispositivos operacionales de soporte, como cintas y discos.
8) Establecer un sistema de clasificación e identificación eficiente para los dispositivos físicos de almacenamiento.
9) Asegurar que los medios de almacenamiento sean resguardados en un ambiente seguro.
10) Determinar los requerimientos de hardware y software para los procedimientos de respaldo y recuperación.

5.6.7 Registro de usuarios y administración de privilegios

Para poder administrar eficientemente la red es importante mantener el control efectivo de los usuarios. La política de registro de usuarios y administración de privilegios permite a la organización establecer jerarquías de acceso a la información, protegiéndola contra los accesos no autorizados.

- **Propósito**

Para evitar daños en la información a través del acceso no autorizado, es necesario establecer una adecuada gestión de los usuarios. Esta política debe permitir el acceso correcto en el tiempo correcto.

- **Alcance**

Esta política está dirigida a todos los usuarios directos o indirectos de la red corporativa.

- **Política**

La organización debe contar con la administración adecuada de permisos de usuarios, permitiendo el control de los accesos a la información crítica, para evitar daños, modificaciones o pérdidas de la misma a través del acceso no autorizado.

- **Directrices**

1) Cada usuario debe ser asociado con un identificador único para responsabilizarlo de sus acciones.
2) La organización debe verificar que las autorizaciones vayan de acuerdo a sus necesidades.
3) Asegurar que el nivel de acceso concedido es el adecuado para ese usuario en particular y para el propósito del negocio.
4) Verificar que los privilegios cumplan con la política de seguridad de la organización.
5) Establecer por escrito los derechos de los usuarios de acuerdo a sus niveles de acceso y asegurar que dicho documento sea asimilado.
6) Pedir a los usuarios firmar un documento donde se haga explícito que están enterados de sus derechos y que los aceptan.
7) Llevar a cabo registros de los eventos de acceso de los usuarios.
8) Remover los derechos de los usuarios que abandonen la organización o bien pierdan el privilegio actual.
9) Evaluar periódicamente las cuentas de usuarios y eliminar aquellos identificadores que resulten redundantes.
10) Evitar que los identificadores redundantes sean usados por otros usuarios.
11) Asegurar control efectivo en los usuarios de acceso externo como Internet.

5.6.8 Monitoreo y registro de eventos

Cuando se detecta una falla en el sistema de la organización, es importante registrarla e implantar un historial de eventos al que se pueda recurrir en caso de incidentes similares.

El establecimiento de políticas de monitoreo y registro de eventos aseguran mayor control de los daños y permiten establecer procedimientos de recuperación del sistema basados en el historial de eventos.

- **Propósito**

Registrar las actividades de la organización para permitir un control efectivo recolectando información que permita observar los eventos de la misma y detectar actividades que vayan en contra de las políticas de la corporación. Además esta política permite optimizar procesos, reducir fallas y realizar diagnósticos de acuerdo a los eventos registrados.

- **Alcance**

Esta política aplica a todo usuario dentro de la organización que esté relacionado directa o indirectamente con el proceso de monitoreo y registro de eventos.

- **Política**

Es obligación de la organización investigar, desarrollar e implementar técnicas de monitoreo y registro de eventos para reducir fallas, optimizar procesos y aumentar la efectividad en el control de actividades.

- **Directrices**

1) Asegurar la optimización del uso de software y hardware mediante el monitoreo y registro de los recursos de la red de la organización.
2) Se deben establecer las reglas específicas de monitoreo dependiendo de los diferentes sistemas operativos, hardware, aplicaciones, etc.
3) Establecer variables claras de monitoreo como por ejemplo:

    - Utilización del CPU
    - Utilización de memoria
    - Tasa de entrada/salida de datos
    - Archivos de usuarios
    - Número de registros de usuarios
    - Tiempos de respuesta

4) Establecer límites de operación normales de las variables de monitoreo.
5) Observar si existen recursos sobre-utilizados, o por debajo del nivel establecido.
6) Monitorear los tiempos de respuesta de las tecnologías de información y servicios de la organización.
7) Establecer métricas de monitoreo específicas y efectivas.
8) Las técnicas de monitoreo y registro deben facilitar el procesamiento de la información, para asegurar que los usuarios realicen actividades para las cuales tienen autorización.

9) Se debe establecer el nivel de monitoreo individual de acuerdo al análisis de riesgos.
10) Establecer las áreas que deben ser consideradas para el monitoreo y registro de eventos, algunas pueden ser:

- Acceso autorizado
- Operaciones privilegiadas
- Intentos de acceso no autorizados
- Sistemas de alerta o fallas.

11) Dependiendo del riesgo, los registros arrojados por el monitoreo de eventos deben ser revisado periódicamente.
12) Se necesita la elaboración de bitácoras de los eventos relevantes para facilitar las investigaciones futuras.
13) Revisión periódica de las bitácoras.

Capítulo 6. Conclusiones

Debido a que tercera generación es una tecnología cuyos protocolos son más seguros que generaciones anteriores, la información resulta más difícil de corromper mientras se encuentra viajando en el canal. Basándose en este hecho, el análisis se centro únicamente en la zona referente a los propietarios de los activos y en capas y planos superiores.

Bajo este mismo supuesto y los estudios realizados en el desarrollo de la tesis, la hipótesis referente a la seguridad en las aplicaciones de tercera generación, fue comprobada.

En el caso del análisis de la información, los flujos y las arquitecturas fueron diseñados de forma general. El BIA y el análisis de riesgo se realizaron a criterio del investigador de acuerdo a las vulnerabilidades propias de tercera generación. Debido a que la investigación no se centró en una organización en particular, fue difícil identificar los riesgos y los impactos, ya que no se contó con información financiera, legal y de procesos, en consecuencia fue necesario establecer supuestos, que en casos reales deben ser analizados y modificados de acuerdo a la información proporcionada por la empresa. Sin embargo, la metodología seguida es un marco de referencia efectivo que los administradores de la seguridad en las organizaciones pueden utilizar confiadamente, para llevar a cabo la elaboración de controles que ayuden a gestionar la seguridad de la información.

Las arquitecturas propuestas en la tesis son totalmente factibles tanto en costo como en requerimientos tecnológicos, sin embargo, ya que la mayoría de las organizaciones establecen su propio esquema de red y segregan los activos dependiendo de sus necesidades, para poder aplicar este esquema a es conveniente rediseñar su arquitectura dependiendo de los resultados arrojados por el análisis de la información que debe ser realizado antes de diseñar las arquitecturas.

En cuanto a las políticas elaboradas se establecieron las directrices dirigidas de forma general a las aplicaciones de tercera generación analizadas en el trabajo. Un ejemplo claro de las limitantes que presentan las políticas establecidas en este trabajo, es que todos los análisis base se realizaron únicamente en las capas y planos de gestión de la seguridad superiores, por lo tanto todas las políticas y directrices referentes al canal de transmisión, de criptografía y aspectos que hacían referencia a áreas físicas particulares de la organización, entre otros, fueron omitidos implementando aquellos controles que hacían referencia únicamente a los riesgos de las aplicaciones estudiadas en la tesis.

Aún así, las políticas y controles establecidos son seguros y pueden ser aplicados en casos reales particulares, haciendo modificaciones de acuerdo a las necesidades de la organización y tomando en cuenta los riesgos y controles establecidos en el ISO 17799, que no fueron requeridos en esta investigación. Este documento, es indispensable para la gestión de la seguridad ya que

establece los riesgos principales que pueden existir dentro de una organización y establece los controles aplicables a esos riesgos. Por esta razón el apoyo del ISO 17799 fue indispensable para el desarrollo de políticas válidas y efectivas aplicables a los servicios analizados tesis.

En caso de que algún operador de la seguridad requiera aplicar este estudio a un caso real, es indispensable que cuente con el soporte del ISO 17799 para poder hacer los ajustes correctos de acuerdo a sus necesidades.

Una de las mayores dificultades a enfrentar en la aplicación de éste documento es el entorno demasiado general que se ofrece en la estructura, lo que genera varios cambios en casos reales, sin embargo es una guía útil para que los operadores se introduzcan al mundo de la seguridad ofreciendo a los usuarios soluciones más confiables.

Se hizo mucho hincapié en la importancia de establecer estándares de seguridad para proteger la información en la organización, sin embargo, el trabajo no termina ahí, ya que la implementación no es una tarea fácil, se deben desarrollar estrategias efectivas de comunicación a todos los niveles de usuarios, haciendo conciencia de las responsabilidades y privilegios que posee cada uno con respecto a la información que maneja. Este paso no es referido en este trabajo, sin embargo, es muy importante ya que establece las pautas para implementar las medidas de seguridad como una cultura dentro de la organización, lo cual es uno de los retos principales actualmente en materia de seguridad.

Para poder continuar con esta investigación ya sea aplicándola a caso reales o bien aumentando el número de aplicaciones analizadas, se sugiere seguir con algunas recomendaciones aprendidas de los tres servicios estudiados en este trabajo.

- Se recomienda analizar los flujos de información tanto de forma general como detallada para poder determinar de forma correcta los activos que intervienen en la red estudiada.
- Recopilar la mayor cantidad de información posible sobre las aplicaciones y servicios que la organización ofrece.
- La información recopilada no se debe limitar únicamente a aspectos tecnológicos, si es posible obtener información financiera, legal y de procesos. Esto facilitará enormemente el análisis de riesgos y de impacto en el negocio.
- Para llevar a cabo los estudios de la información de forma objetiva y confiable, se recomienda analizar cada aplicación por separado, sin importar que tan parecidas sean o cuantos activos en común intervengan en cada servicio. Esto es debido a que aún teniendo ciertos elementos en común por lo general difieren en función o en grado de importancia de acuerdo al tipo de aplicación que se analiza.
- Para proponer la arquitectura se recomienda tomar en cuenta todos los activos en conjunto identificando aquellos elementos

que pueden ser comunes y segregando aquellos que representen mayor riesgo para la organización.

- Los requerimientos tecnológicos propuestos para la arquitectura deben ser factibles en costo y su implementación debe ser justificable a las necesidades de la organización.
- Las políticas de seguridad deben ser coherentes con los resultados obtenidos en el análisis de la información y deben estar alineadas a las necesidades de la organización.
- Se recomienda establecer controles claros no dejando lugar a malas interpretaciones. Estos controles deben estar relacionados con los riesgos y las necesidades de la empresa.

A pesar de las recomendaciones presentadas resulta lógico concluir que se pueden enfrentar otro tipo de barreras no presentadas en este documento, por lo tanto, es importante buscar apoyo en el ISO 17799 y otra bibliografía especializada en la materia de gestión de la información.

Por último es importante resaltar que esta tesis marca la pauta para el análisis más profundo y de mayor amplitud, abarcando más aplicaciones de tercera generación y atacando otros planos y capas de gestión de la seguridad como el de control y de infraestructura respectivamente. Este tipo de estudios complementará la guía ofreciendo al operador mayores opciones en la implementación de medidas de seguridad a todos los niveles de la organización.

Bibliografía

A. B. García, M. Alvarez-Campana, E. Vázquez, J. Berrocal, J. Vinyes, "Dimensionando Eficiente de la Red de Acceso UMTS en Presencia de Múltiples Clases de Tráfico", 15 de Marzo de 2004, Depto. De Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid.

Alan Clapto, "Future mobile networks: 3G and beyond", 2001, London: Institution of Electrical Engineers.

Ana Bernardos, "Tecnologías de localización", Diciembre de 2003, Centro de Difusión de Tecnologías ETSIT-UPM, http://www.ceditec.etsit.upm.es/localizacion.php.

Apostolis k. Salkintzis, "MOBILE INTERNET Enabling Technologies and Services", 2004, CRC PRESS.

Baluma Networks, "Lenguaje de Internet", 2001, http://www.baluma.com/internet1al10/lenguaje.asp

Benyi Arregocés, "Sistemas de localización móviles: Proporcionan servicios útiles, pero son un riesgo para la intimidad de las personas", Consumer.es EROSKI Diciembre de 2003, http://www.consumer.es/web/es/tecnologia/hardware/2003/12/26/93204.php?page=3

Centro de Predicción Económica, CEPREDE, 2004, http://www.n-economia.com/fichas_neconomia/pdf/gr6/6_8.pdf

César Colorado, "Selección y control de calidad en pruebas de intrusión", Septiembre 2004, Auditorias de seguridad, e-security.

Chamero, J. "Historia de Internet y El Internet Histórico", 1999 http://www.aunmas.com/future/internet_historia/

Dan Steinbock, Eli M. Noam, "COMPETITION FOR THE MOBILE INTERNET", 2003, Editorial Kluner Academic Publishers.

Delitos Informáticos, "Clasificación y tipos de ataques contra sistemas de información", 25 de Marzo de 2001, http://www.delitosinformaticos.com/seguridad/clasificacion.shtml.

Dr. Enrique V. Carrera, "Seguridad Informática", 22 de Febrero de 2005, Colegio Politécnico, Universidad San Francisco de Quinto.

E-salud. "Programa de Acción E-Salud", 2004, http://www.e-mexico.gob.mx/wb2/eMex/eMex_Acerca_del_programa_eSalud

Ernesto Aranda Almansa, Antonio de la Paz Rincón, Ignacio Berberana Fernández-Murias, Héctor Gonzáles Sanchís. "Sistemas de localización en redes móviles: el servicio de emergencias 112", junio 2001, Comunicaciones de Telefónica I+D.

Ernesto Collado Rodríguez, "Evolución Histórica de Internet", 02 de Septiembre 2003,
http://www.maxitrucos.com/articulos/ernesto/evolucion_historica_internet.htm

Francisco Javier Chamorro Pérez, Antonio Alberto de Mercado Cristóbal, José Luis Núñez Díaz, Alberto Gómez Vicente "Arquitectura de Internet Móvil", Marzo 2001, Comunicaciones de Telefónica Investigación y Desarrollo.

Gabriel Chova, "Una breve historia de Internet", 2004, http://www.articulos.astalaweb.com/Internet%20-%20Historia/Una%20breve%20historia%20de%20Internet%20(I).asp

Hernández Campos Omar, "INTERNET MÓVIL una herramienta para reducir la brecha digital", Foro Internet AHCIET, 13 y 14 de Septiembre del 2004

Hernandez, Rafael, "Principios Para La Explotación En México De Las Redes Híbridas" WLANG-3G, 2003

Hispamedia Network, S.A., "Mercadeo en Internet", 2003, http://www.hispamedia.biz/servicios/marketing.asp

Ing. Lagerloef Torrealba Figueira, "aplicaciones futuras 3g en venezuela y la migracion de la tecnología siemens 2g hacia 3g", Diciembre de 2000, http://neutron.ing.ucv.ve/revista-e/No8/Lagerloff%5Ctrabajo2.htm

José Juan Jiménez, "Evolución e historia de la telefonía celular", 28 de Septiembre de 2003, http://www.ilustrados.com/publicaciones/EpyuZyllpytCnsdaDd.php

José Luis Saavedra Romero, "Análisis Del Espectro Radioeléctrico Para La Implementación De Las Tecnologías De Tercera Generación En México", Abril de 2004

Juan C. S´anchez, Xavier Perramon, Ramon Mart´ı, Jaime Delgado "Implementation and Performance Evaluation of Communications Security in a Mobile E-health Service", 2004 Universitat Pompeu Fabra (UPF), Barcelona Spain.

María Almudena González Pérez, "MODELOS DE SEGURIDAD PARA MÓVILES", Julio de 2001, Universidad Politécnica de Cataluña.

MasterMagazine, "Telefonía Móvil de última generación", 2004, http://www.mastermagazine.info/catalog/news/news_detail.php?ID=610

Miguel Alejandro Soto, "Protocolos TCP/IP", SF, http://usuarios.lycos.es/janjo/janjo1.html

Miguel Ángel Álvarez, Manual "Publicar en Internet", SF, http://www.desarrolloweb.com/articulos/188.php?manual=3

Nokia, "Mobile email", SF, http://www.nokia.com/nokia/0,8764,63942,00.html.

Paola Iza Martínez, "La mejor manera de mantenernos en contacto", 2000, Microasist, http://microasist.com.mx/noticias/tp/paotp170303.shtml

Publicaciones EMB, "Promesas y Desafíos de la Internet Móvil", 2003, http://www.gerencia.cl/articulo.mv?sec=3&num=2

Revista del Consumidor No. 288, "Estudio de mercado: Servicio de Internet móvil", Febrero de 2001, http://www.profeco.gob.mx/html/revista%5Cpdf%5Cmovil.pdf

Ricardo Morales, "Administración de Riesgos de Seguridad de Información", Octubre de 2004, ITESM.

Roberto Corona Copado, "INTERNET: Atrapados en la red", 28 de Enero del 2003, http://www.claves.udg.mx/pdf28-internet/internet.pdf

Sapal Tachakra, X.H. Wang, Robert S.H. Istepanian, Y.H. Song, "Mobile e-Health: The Unwired Evolution of Telemedicine", Telemedicine Journal and E-Health, 2003, Mary Ann Liebert, Inc.

Sony Ericsson Mobile Communications, 2004, http://www.ericsson.com.mx/soluciones/mobil/internetmovil/

Susana Voces Gómez, "¿Cómo los operadores de telefonía móvil pueden convertir un requerimiento en una oportunidad?", 28 de Octubre de 2003, Product Marketing Manager, Ericsson, http://www.icemd.com/area-entrada/articulos/consulta-art.asp?id=137.

Telefónica, "Las telecomunicaciones y la Movilidad en la Sociedad de la Información", S.F http://www.telefonica.es/sociedaddelainformacionok/pdf/publicaciones/movilidad/capitulo_13.pdf

Tendencias Digitales, "Internet móvil marcará el rumbo de las comunicaciones y la nueva forma de hacer negocios", Febrero del 2004, http://www.tendenciasdigitales.com/td/mundo9.htm

Unión Internacional de Telecomunicaciones, "La seguridad de las telecomunicaciones y las tecnologías de información, Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT-T existentes", Diciembre 2003.

VADEMECUM REMER, "Fundamentos de Internet", 2002, http://www.proteccioncivil.org/vademecum/vdm032.htm

Vinton G Cerf, "Gobierno de Internet", 28 de Octubre del 2004, http://www.icann.org/presentations/cerf-internet-publication-spanish-28oct04.pdf

Waymovil, "En cualquier momento y lugar", 2002, grupo J. Venture & Partner Spa, http://www.waymovil.net/root/debate_2915.htm#bottom.

3G americas, "ESTADISTICAS: La familia de tecnologías GSM", junio 2004, http://www.3gamericas.org/PDFs/media_kit/esp/tech_stats_june2004_span.pdf