INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS MONTERREY
PROGRAMA DE GRADUADOS EN ELECTRONICA, COMPUTACION, INFORMACION Y COMUNICACIONES

MODELO DE ADMINISTRACION DE SEGURIDAD DE INFORMACION PARA REDES INALAMBRICAS MOVILES BASADO EN EL ESTANDAR BRITANICO BS-7799

TESIS
MAESTRIA EN ADMINISTRACION DE LAS TELECOMUNICACIONES

POR
LIC. JORGE ALBERTO BLANCO CRUZ

ABRIL 2004

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS DE LA DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

MODELO DE ADMINISTRACIÓN DE SEGURIDAD DE INFORMACIÓN PARA REDES INALÁMBRICAS MOVILES BASADO EN EL ESTANDAR BRITÁNICO BS-7799

TESIS

MAESTRIA EN ADMINISTRACIÓN DE LAS TELECOMUNICACIONES

POR

LIC. JORGE ALBERTO BLANCO CRUZ

ABRIL 2004

MODELO DE ADMINISTRACIÓN DE SEGURIDAD DE INFORMACIÓN PARA REDES INALÁMBRICAS MOVILES BASADO EN EL ESTANDAR BRITÁNICO BS-7799

POR

LIC. JORGE ALBERTO BLANCO CRUZ

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 de las Telecomunicaciones

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

ABRIL 2004

Al Instituto Tecnológico y de Estudios Superiores de Monterrey por haber abierto sus puertas a través de la Escuela de Graduados (EGADE), brindándome la oportunidad de adquirir los conocimientos que me han formado, a través del mundo de las telecomunicaciones.

Reconocimiento especial al Dr. Ricardo Pineda Serna, PhD, al Dr. Jorge Carlos Mex Perera, PhD y al Dr. Jose Ramón Rodríguez Cruz, PhD, que me brindaron su apoyo para la realización de este trabajo, y que con su orientación me condujeron a obtener los mejores resultados.

A mis profesores y a todos aquellos que con su vocación de servicio me dedicaron parte de su tiempo y me transmitieron sus experiencias.

A mis padres:

Jose Angel Blanco Fernandez
Maria Elena Cruz de Blanco
Porque con su esfuerzo y apoyo logré alcanzar una de mis más grandes metas. ¡¡¡ Gracias !!!

A mis compañeros y amigos que en su momento me respaldaron de alguna forma.

Jorge Alberto Blanco Cruz

MODELO DE ADMINISTRACIÓN DE SEGURIDAD DE INFORMACIÓN PARA REDES INALÁMBRICAS MOVILES BASADO EN EL ESTANDAR BRITÁNICO BS-7799

Lic. Jorge Alberto Blanco Cruz

Instituto de Tecnológico y de Estudios Superiores de Monterrey, 2004

La tecnología inalámbrica gana más adeptos día con día gracias a la variedad de servicios y dispositivos que es capaz de ofrecer, su evolución se ha presentado como una de las más rápidas en la historia de la tecnología. Wi-Fi, GSM, GPRS, WAP, Bluetooth han permitido en un periodo corto de tiempo grandes avances en el mundo de las telecomunicaciones.

En Monterrey por su geografía, resulta muy atractiva la adopción de este tipo de tecnología, ya que esta favorece a su implementación. Los administradores de TIC en las empresas entrevistadas en esta investigación, han optado por adoptarla, debido a su fácil y rápida instalación, permitiendo velocidades de transmisión de 11 mbps en la banda de 2.4 Ghz hasta 54 mbps en la banda de los 5 Ghz. El acceso a Internet a partir de a partir de dispositivos inalámbricos plantea mayores desafíos en cuestiones de seguridad para las empresas, los dispositivos inalámbricos (smart phones o PCs portátiles) tienen ciertas vulnerabilidades y no ofrecen altos niveles de confianza, a pesar de que los propios usuarios sean confiados al respecto.

La gran variedad de servicios y dispositivos utilizados por la tecnología inalámbrica es un factor que incrementa el nivel de riesgo, permitiendo el surgimiento de nuevos ataques de información a través del uso de nuevas amenazas para explotar nuevas vulnerabilidades encontradas. Garantizar la privacidad, confidencialidad y disponibilidad de la información en las redes inalámbricas móviles de las empresas en Monterrey es una de las metas más importantes de los administradores de TI, ya que en la actualidad se maneja información con un mayor grado de confidencialidad. A pesar de que muchas organizaciones consideran el gasto en seguridad como un costo negativo que debe soportarse, el hecho es que en el negocio de las telecomunicaciones la inversión en seguridad puede representar una ventaja competitiva. Cabe mencionar que en términos financieros es un poco complejo determinar el costo, pero de acuerdo con la información obtenida de la investigación realizada, se pudo conocer que del presupuesto destinado a la adquisición y administración de la tecnología aproximadamente el 10% es para la seguridad de información.

Una buena seguridad permite construir relaciones de confianza con socios y clientes, puesto que protege la confidencialidad de los datos compartidos. Las empresas que han construido una infraestructura informática tienen más oportunidades de cumplir con las necesidades de seguridad, mientras que las empresas tradicionales deben llevar a cabo, en la mayoría de los casos, grandes inversiones para reestructurar sus políticas e infraestructuras.

De ahí la importancia del uso de modelos de seguridad que nos puedan garantizar el nivel de seguridad adecuado y que nos permita ofrecer a los usuarios de las redes inalámbricas servicios de calidad necesarios para satisfacer las demandas del mercado.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

CAPITULO 1

INTRODUCCIÓN

1.1.- SITUACION PROBLEMÁTICA

A consecuencia de la gran diversidad de sectores en donde puede implementarse la tecnología de redes inalámbricas móviles y de sus múltiples servicios y aplicaciones que ofrece, existe un riesgo grande de seguridad. (Muller, 2000).

La seguridad se está convirtiendo en una prioridad porque la comunicación y la información se han convertido en un factor dominante en el desarrollo económico y social. Como todos, los negocios, individuos privados, las administraciones públicas desean explotar las posibilidades de las redes de comunicaciones, la seguridad de estos sistemas se está convirtiendo en un requisito previo para el progreso.

En México, aun falta mucho por hacer en cuanto a cultura de seguridad de información y de telecomunicaciones se refiere. (Ruíz, 2002). Esta falta de cultura en seguridad de información, crea una gran desventaja en las empresas, por lo que tienen que pagar el precio al tener problemas con sus sistemas de información y de telecomunicaciones, los cuales tienen una gran probabilidad de ser vulnerados.

Casos actuales registrados en los primeros meses del 2004, como el gusano Beagle.Q, el cual explota una vulnerabilidad reciente en el Internet Explorer, o la variante del Virus Netsky denominada Netsky.Q el cual utiliza su propio motor de SNMP para enviarse por si mismo a otras direcciones de correo, o uno de los últimos casos correspondiente al gusano Witty en el mes de Marzo, el cual aprovecha vulnerabilidades en los productos de ISS. (UNAM-CERT, 2004).

Estos sucesos se consideran un grave problema ya que al no tener implementados procesos o metodologías de seguridad, las empresas se encuentran expuestas a constantes ataques los cuales pueden ser minimizados a través de modelos de seguridad que puedan adecuarse a las necesidades de las empresas de este país. (Ruíz, 2002).

En la siguiente gráfica, la cual es resultado de las investigaciones realizadas por el FBI, se muestra el número de ataques registrados en las organizaciones en el año de 2003, de acuerdo con 530 especialistas de seguridad encuestados.

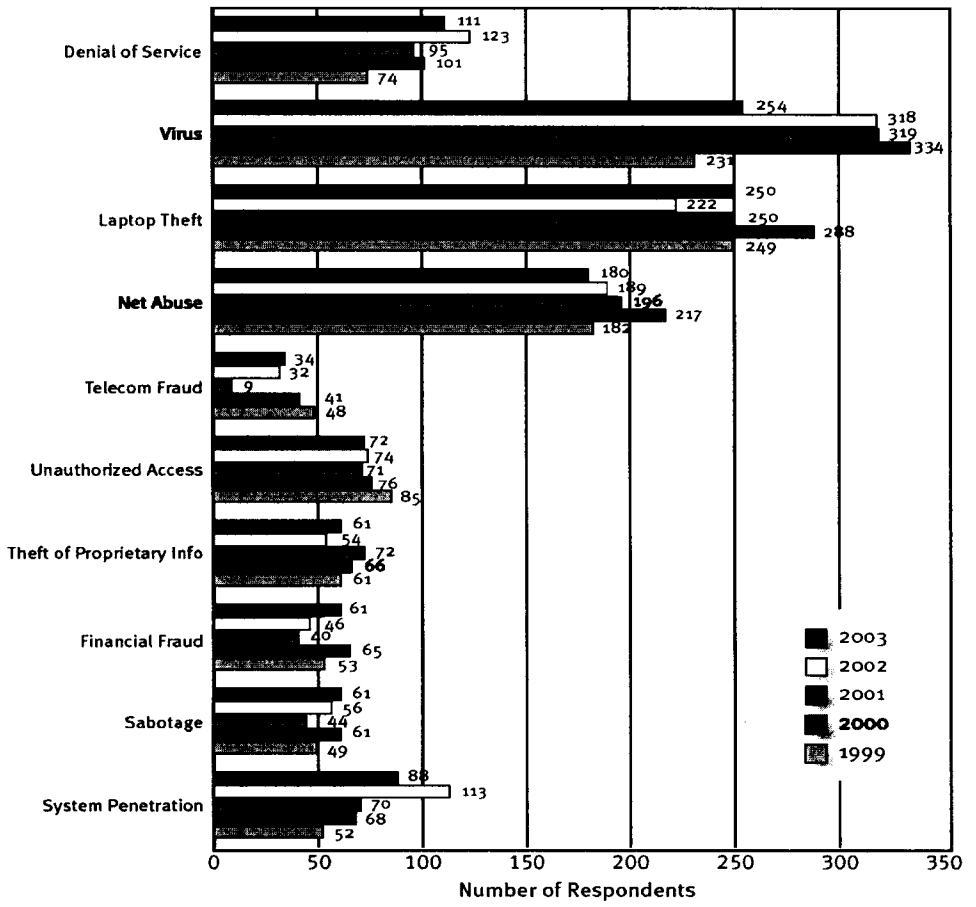

Figure 1.- (CSI/FBI, 2003) Tipos de Ataque en las Organizaciones

Con estos resultados nos podremos dar cuenta del grado de exposición que tienen la mayoría de las empresas actualmente ante un evento adverso de seguridad de información.

Para poder tener un nivel alto de seguridad en las redes inalámbricas móviles existentes o en construcción en una organización, es necesario conocer las ventajas y desventajas que ofrece la tecnología que se desea usar, los riesgos y vulnerabilidades que la información tendrá al viajar de un lugar a otro a través de los enlaces inalámbricos. (Solarte, 1999).

La materialización de los incidentes de seguridad de información implica la generación de grandes pérdidas monetarias a causa del impacto generado, como podemos ver en la figura 2.

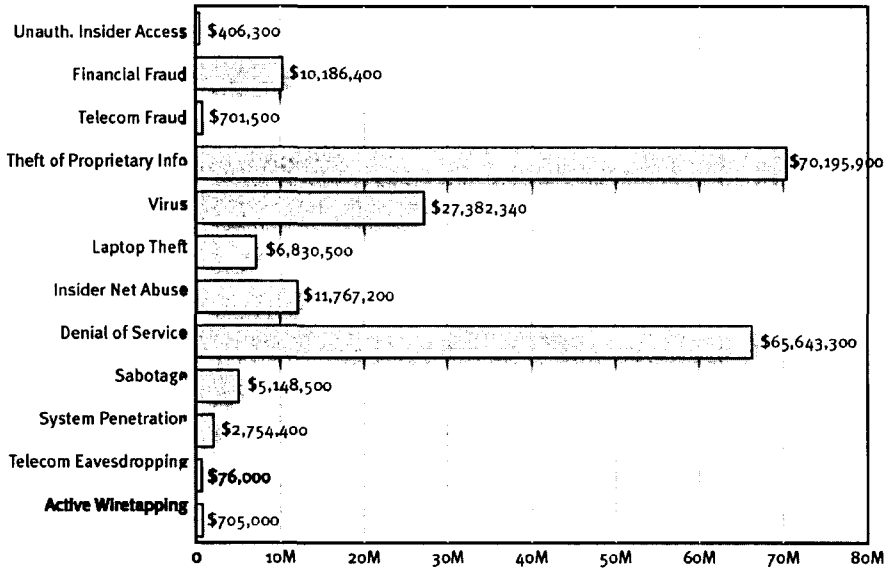

Figure 2.- (CSI/FBI, 2003) Perdidas en Miles de Dólares por Tipo de Ataque

Las empresas buscan reducir los costos de operación y de procesos, buscando siempre la automatización de sus actividades, eligiendo la solución de menor costo que les garantice calidad en los servicios que requieren. (Tss, 2002).

Lo más importante de la automatización de las actividades en una empresa, es el análisis de los procesos de información que se realizan, con el objetivo de encontrar la solución más adecuada a la problemática que se presenta, algo que se conoce en el ambiente de seguridad como 80-20, en la cual el 80% corresponde al análisis de los procesos de información y el 20% restante corresponde a la implementación de la tecnología adecuada para garantizar la seguridad de esos procesos. (Tss, 2002).

La propiedad intelectual y la información sensible o crítica de negocios es lo más valioso de las compañías de hoy. Con el incremento del numero de aberturas de TI que son divulgadas, las compañías necesitan protegerse así mismas y a sus clientes. (Sapphire, 2003).

La seguridad de la información almacenada o en transito, es de vital importancia para los negocios modernos. Los socios de negocios, clientes y proveedores quieren asegurarse de que la información esté disponible y sea completamente confiable, protegida contra intrusos. Los medios de proporcionar tal aseguramiento a los socios presentes y futuros son obtener un certificado de conformidad con un estándar de seguridad. El BS7799 es el estándar de seguridad más extenso reconocido en el mundo. (Hefferan, 2003).

El estándar de seguridad de información BS7799 es de reciente creación, y su adopción por parte de las empresas a nivel mundial está en proceso. La implementación de modelos de seguridad basados en este estándar aun está en etapas de desarrollo e implementación. (Bsi, 2003).

Por lo cual su adopción en las diferentes áreas de los sistemas de información y de telecomunicaciones, debe realizarse de la mejor forma para garantizar que la información que viaja a través de las redes de las empresas cuente con los más altos niveles de seguridad de información, y por lo tanto existirá un alto grado de confidencialidad, integridad y disponibilidad.

1.2.- OBJETIVOS

1. Proponer un modelo de administración de seguridad de información para redes inalámbricas móviles basado en el Estándar Británico de Seguridad BS7799, que ayude a determinar el grado de riesgo que enfrentan las tecnologías de información y los servicios de comunicaciones inalámbricas en el sector empresarial.

2. Evaluar y/o validar el modelo a través de expertos o profesionales en el área de seguridad de información y telecomunicaciones, para establecer las mejores reglas y normas que se deben seguir para el adecuado aseguramiento de la información en la utilización de las tecnologías de comunicación inalámbricas.

CAPITULO 2

MARCO TEÓRICO

2.1.- INTRODUCCIÓN

La evolución de la tecnología en los últimos años ha sido impredecible, el mundo esta siendo testigo del tremendo crecimiento en la disponibilidad y funcionalidad de una amplia variedad de tecnologías personales. La creación de nuevas tecnologías para poder transmitir información ha transformado nuestras vidas, satisfaciendo nuestras necesidades de comunicación, desde la creación del cable coaxial, hasta la utilización de la fibra óptica, las videoconferencias, la creación de microcomputadoras, los celulares, las redes inalámbricas y muchos dispositivos y tecnologías han transformado los entornos laborales en todo el mundo, facilitando la realización de nuestras actividades diarias.

Las empresas están adoptando la fidelidad inalámbrica por muchas razones, en especial por lo conveniente que resulta. El hecho de no tener cables da libertad a los empleados para trabajar en áreas comunes o desde el disco duro para llegar a todas partes. Un número cada vez mayor de empresas se están olvidando de las infraestructuras totalmente conectadas y están adoptando las conexiones inalámbricas. Sin embargo, la tecnología inalámbrica es más que un asunto de seguridad, y demasiadas empresas se precipitan a implementar la fidelidad inalámbrica (Wi-Fi) antes de entender la tecnología y todos los riesgos que implica.

Para satisfacer la demanda creciente de datos en equipos móviles y servicios de telefonía mejorados, los operadores de tecnologías inalámbricas requerirán realizar convergencia con el crecimiento de Internet. Se ha proyectado que 540 millones de personas a nivel mundial usarán Internet para el año 2005. (Revista RED, 2003).

Muchas personas tienen diferentes puntos de acceso hacia Internet, incluyendo sus casas, trabajo, escuela y lugares públicos. Los mismos usuarios de Internet también cuentan con equipos de comunicación personal, tales como teléfonos celulares y computadoras de bolsillo. La tercera generación de redes inalámbricas (3G) está ofreciendo la convergencia de Internet a través de los sistemas inalámbricos. Los equipos personales de bolsillo están convirtiéndose en el punto de acceso a Internet de mayor demanda.

A nivel internacional, las telecomunicaciones son el mercado de mayor crecimiento global, tanto en ventas como en inversión y en asociaciones estratégicas. A pesar de que México ha iniciado su lucha por la competitividad de este importante sector, hay que apuntar que el desarrollo moderno de las telecomunicaciones se encuentra aun muy concentrado en los países desarrollados. (Revista RED, 2003).

En los últimos tres años, una tecnología inalámbrica ha arribado con el poder para cambiar totalmente el juego. Es una forma de dar a Internet alas sin licencias o permisos. En un mundo donde hemos sido condicionados a esperar por los carriers de teléfonos celulares para traernos el futuro, esta anarquía de las ondas aéreas esta tan liberada como el primer PCS con el poder para cambiar cualquier cosa. La tecnología es Wi-Fi, y es el primer golpe en una revolución, llamada open spectrum, que llevara a internet a la siguiente era en esta colonización del globo. Como la red misma, Wi-Fi fue confinada a círculos técnicos antes de explotar dentro del marco principal. Los dos años pasados, llego a ser una de las tecnologías de mas rápido crecimiento en la historia. (Revista RED, 2003).

Gartner calcula que el número de usuarios móviles de redes WLAN (de área local inalámbricas) a nivel mundial crecerá de 4.2 millones en 2003 a más de 31 millones hacia 2007, lo que beneficiará de manera importante a la industria de dispositivos móviles. (Revista RED, 2003).

Un factor clave para el éxito de esta nueva tecnología es el desarrollo de puntos públicos de conexión inalámbrica, conocidos como Hot Spots, los cuales estarán inundando los centros comerciales, hoteles, aeropuertos, restaurantes, cafés, bibliotecas, parques y todos los sitios públicos que se pueda imaginar. Y México no es la excepción. En la actualidad existen en el país más de 100 sitios públicos habilitados con conexión inalámbrica a Internet, y este número seguirá en aumento. (Revista RED, 2003).

2.2.- CONVERGENCIA

En un intento por hacer Internet más fácil, las compañías tecnológicas están enlazando Wi-Fi y tecnologías celulares. Wi-Fi envía páginas Web a través de ondas de radio. Esto esta ganando rápidamente usuarios de laptops porque permite acceso rápido a internet sin tener que hacer uso de una línea telefónica. Pero esto solo funciona si el usuario se encuentra en un radio de 1000 pies de una antena Wi-Fi. Conectando a internet vía celular o a través de una laptop con antena celular, es lento, pero la cobertura de la célula telefónica es mucho más grande que la cobertura de Wi-Fi.

Un dispositivo con ambas tecnologías, tendrá las ventajas de ambas. Una laptop, por ejemplo, deberá usar Wi-Fi cuando se encuentre en el rango de Wi-Fi y utilizara la tecnología celular cuando este fuera del rango de Wi-Fi. El servicio celular sería lento, pero por lo menos habría una conexión.

Un obstáculo para la combinación Wi-Fi/Teléfono Celular es ¿quien seguirá pagando?. Las redes Wi-Fi están corriendo por una mezcolanza de compañías, agencias y personas. Las redes telefónicas celulares usualmente corren a través de compañías telefónicas. Para permitir el switching de una red a otra, las compañías deberán trabajar fuera de facturación y mantener los servicios.

2.3.- TECNOLOGIAS INALAMBRICAS

2.3.1.- SISTEMAS CELULARES

GSM

Cuando comenzó a andar el mundo de la telefonía móvil, éste se soportaba sobre un canal de comunicaciones analógico, lo que hacía que las comunicaciones fuesen demasiado lentas y poco fiables para pensar en proporcionar sobre ellas servicios de datos que pudiesen ser atractivos para los usuarios. Así llegó al mundo de la telefonía móvil el sistema GSM, ya de tecnología digital, que ofrece un enlace a 9600 bps, suficiente para ofrecer servicios con una mínima calidad.

La llegada de GSM ha dado lugar a la aparición de servicios para móviles, donde los proveedores proporcionan a sus clientes mensajes cortos con información sobre el tráfico, noticias, gasto mensual acumulado, etc.

El sistema GSM está basado en técnicas de conmutación de circuitos, de modo que al efectuar una llamada se reserva un canal de comunicación entre origen y destino. Una vez realizada la reserva de un canal, éste permanecerá ocupado durante todo el tiempo que dure la conversación. Este sistema está pensado para llamadas de voz, ya que en una conversación telefónica el canal está casi siempre ocupado (es raro que ambos interlocutores permanezcan callados).

Dos ejemplos de aplicaciones que podrían soportarse con una tasa de transmisión de 9600 bps podrían ser los siguientes:

- Podría registrarse en una web dedicada a informar de forma dinámica los cambios en valores de bolsa y así saber cuando sus acciones han bajado de un cierto umbral.

- Desde su teléfono móvil, utilizando un buscador de productos, podría saber si existe alguna tienda virtual donde, por ejemplo, el precio de un determinado televisor está por debajo de un umbral, obteniendo información de cuánto le costaría (incluyendo incluso los gastos de envío) y en qué tienda podría adquirirlo.

Pero también es cierto que hay muchas aplicaciones que no podrían soportarse bajo dicha tasa de transmisión. Por ejemplo:

- Navegar un corto período de tiempo por Internet mientras estamos esperando a que llegue el tren, ya que iría bastante lento en cuanto nos saliésemos de los sitios especialmente diseñados para móviles, y ya no digamos si pretendemos bajar gráficos.
- Ver el gol que marcó nuestro jugador favorito en la última jornada de liga, ya que 9600 bps está muy por debajo del ancho de banda mínimo necesario para vídeo.

Por tanto, se deduce que aunque con GSM se presentan algunos servicios bastante atractivos, es obvio también hay bastantes limitaciones.

Es posible aumentar la tasa de 9600 bps sin salirnos de la banda estrecha, introduciendo la conmutación de paquetes en las comunicaciones móviles. De esto se encargará el estándar GPRS ("General Packet Radio Service").

Tres trayectorias diferentes de actualización han sido desarrolladas para GSM, y dos de las soluciones soportan IS-136. Las tres opciones de actualización de TDMA incluyen: (a) High Speed Circuit Switched Data (HSCSD); (b) General Packet Radio Service (GPRS); y (c) Enhanced Data Rates for GSM Evolution (EDGE). Esto es para que

WAP Y GSM

El Protocolo de Aplicaciones Inalámbricas (Wireless Application Protocol) apareció en 1999 como un estándar internacional que permitía por primera vez el acceso desde dispositivos móviles a contenidos y servicios de Internet a través de conexiones inalámbricas.

El desarrollo de este protocolo fue promovido por empresas líderes del sector de las comunicaciones como Nokia, Ericsson, Motorola y Unwired Planet a los que se unieron más de 200 empresas de todo el mundo. WAP es un protocolo que permite a los móviles con tecnología GSM tener acceso a Internet y utilizar la red. Debido a la velocidad de transmisión (9,6 Kbps) y al interfaz del GSM la navegación no se realiza a través de las páginas HTML, sino que se utiliza el formato WML, lenguaje de marcas basado en XML y que está diseñado exclusivamente para esta tecnología.

Este formato permite optimizar los ficheros de datos para poder ser transmitidos por redes GSM. Cuando WAP apareció en 1999 todos los actores del sector de las comunicaciones inalámbricas profetizaron la explosión del acceso a Internet a través de teléfonos móviles GSM dotados de tecnología WAP, pero hasta el momento las tasas de penetración de esta tecnología no están teniendo los resultados esperados.

Su salida al mercado supuso los siguientes retos para fabricantes y operadoras:

- Crear un nicho de mercado partiendo de cero.
- Cambiar los hábitos de navegación de los internautas, ya que la navegación con WAP no permitía la inclusión de gráficos, animaciones, efectos multimedia ni grandes volúmenes de datos.
- Ofrecer unos servicios útiles y adaptados a las peculiaridades y limitaciones de los dispositivos.

Estos retos iniciales no se han llegado a alcanzar ya que pese a ofrecer una forma sencilla y práctica de acceso a Internet, existen una serie de limitaciones cuando hablamos de WAP bajo GSM:

a) Tiempo de acceso real a la información muy elevado.
b) Alto coste de utilización.
c) No admite elementos gráficos de calidad.
d) Aplicaciones limitadas y de escaso valor añadido para el usuario.

Conscientes de estas limitaciones, encontramos una característica fundamental que supone la mayor ventaja de WAP y un cambio en las hábitos de navegación tradicionales: la información a la que se accede es información en estado puro.

El usuario accede a un sitio WAP con un propósito determinado, buscando información puntual y desaparecen todos aquellos aspectos que no son relevantes para el usuario (presentaciones flash, banners publicitarios, etc.). Por tanto, el eje fundamental del acceso a contenidos WAP desde los dispositivos móviles deben ser la utilidad de la información contenida en dichos sitios.

Este concepto no consiguió transmitirse correctamente, lo que ha llevado a afirmar que WAP es un protocolo que no tiene cabida dentro de los nuevos sistemas de transmisión emergentes. Sin embargo, es innegable que la aparición de WAP fue el primer paso para acceder a servicios de datos avanzados y que supuso una nueva vía para acceder a la información y recuperarla a través del móvil. Una vía que como hemos visto posee sus limitaciones pero también enormes posibilidades.

De todo lo dicho anteriormente se pueden extraer tres conclusiones:

- El concepto de WAP es válido y su aparente fracaso se debe sobre todo a las bajas velocidades de acceso. Pero una de las características determinantes de WAP es su capacidad para adaptarse a los nuevos estándares de transmisión de datos que van surgiendo, en concreto GPRS.

- Por otro lado, el éxito de GSM jugará un papel relevante en el futuro desarrollo de servicios móviles de datos, como cimiento para la construcción de infraestructura y la generación de ingresos a partir de los existentes servicios de Internet móvil mediante WAP y SMS. Su capacidad de itinerancia junto a una infraestructura abierta, convierten a GSM en la plataforma óptima sobre la que construir las futuras estrategias móviles.

- Aumentar la velocidad de 9,6 Kbps adaptando la tecnología GSM a las limitaciones de la banda estrecha, introduciendo la conmutación de paquetes en las comunicaciones móviles. Esto lleva a hablar de GPRS, una evolución del sistema GSM y que permitirá desarrollar nuevos servicios más avanzados y atractivos para el usuario y mejorar los ya existentes.

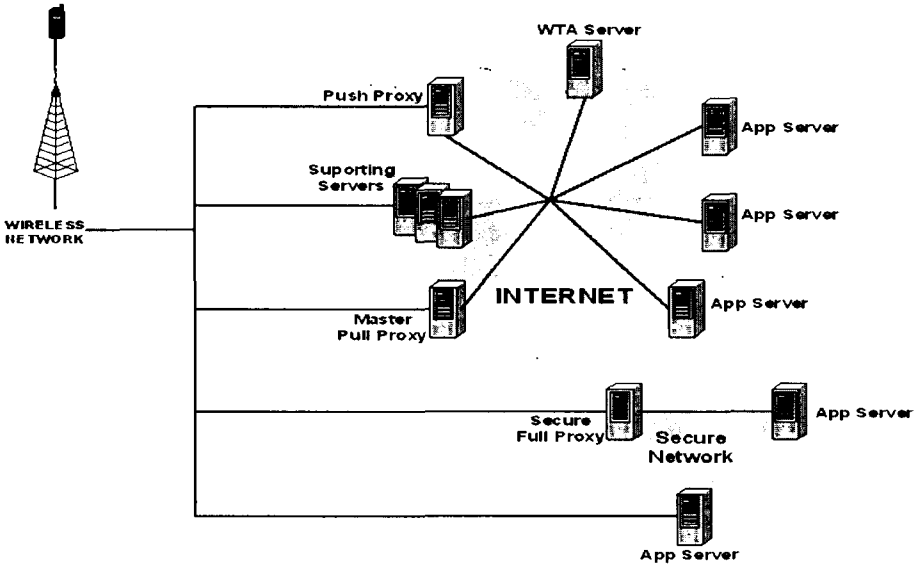

Figura 3.- Arquitectura de Red WAP

GPRS

En las comunicaciones de datos, como ocurre en Internet, el tráfico es "a ráfagas", de modo que el envío de los mismos se concentra en instantes determinados, mientras que durante la mayor parte del tiempo el canal permanece vacío. Luego parece claro que en una comunicación móvil-servidor web la tecnología de conmutación de circuitos es claramente ineficiente.

De este modo, podríamos aumentar la velocidad de transmisión en una comunicación móvil-ordenador utilizando otras técnicas, como por ejemplo la conmutación de paquetes (empleada en las redes de datos fijas, como Internet).

En esta técnica no hay reserva previa de canales de comunicación, con lo cual cuando un canal no está transmitiendo datos puede ser usado por otra terminal. Bajo esta nueva técnica es como se ha construido GPRS ("General Packet Radio Service"), gracias al cual será posible alcanzar velocidades de transmisión entre el móvil y el ordenador de hasta 164 Kbps. Esta tasa de transmisión es incluso superior a la de los modems actuales y por tanto cualquier cosa que puede hacerse desde un ordenador conectado a Internet, podría también llevarse a cabo desde el teléfono móvil.

Actualmente los servicios GPRS tienen una gran variedad y las soluciones que utilizan esta tecnología van en aumento, algunos de los de estos proporciona velocidades de hasta 50 kbits por segundo, en función del tipo de terminal con el que se haga la transmisión.

Algunos ejemplos de servicios GPRS ofrecidos por algunas compañías de telecomunicaciones son los siguientes:

- Acceso a canales propios, públicos y conversaciones privadas vía SMS, llamada a un 900 a través de e-mocion WAP.
- Comunicación con varias personas a la vez, SMS y web también multiconferencia de voz y mensajería instantánea.
- Descarga de juegos a nuestro móvil.
- Regalar canciones tanto a móvil como a fijo.
- A través de WAP acceso a servicios financieros de bancos y cajas.

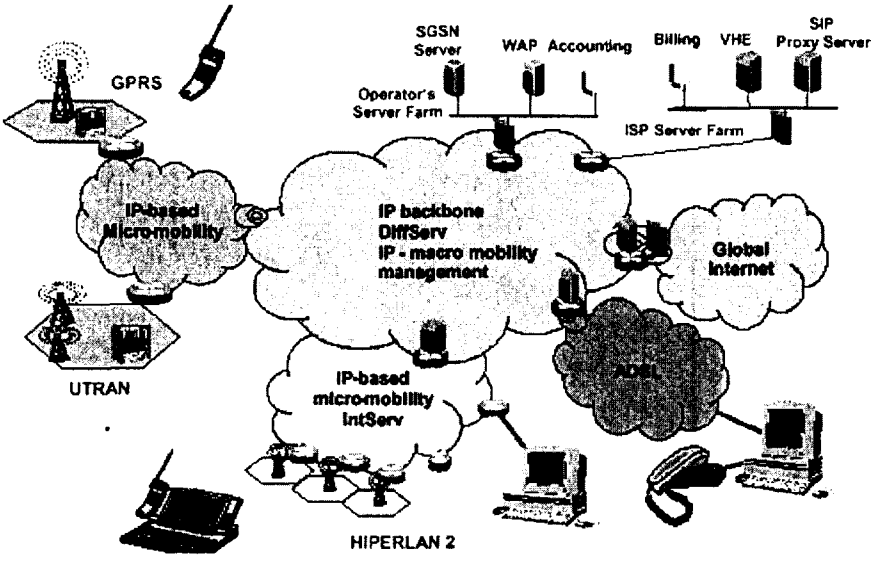

Figura 4 .- Arquitectura de Red Celular

WAP Y GPRS

En un corto periodo de tiempo, WAP se ha convertido en la norma de uso común para llevar contenidos de Internet y servicios técnicos avanzados a todas las redes y dispositivos inalámbricos. WAP posibilita la aparición de una completa gama de nuevos e innovadores servicios de valor agregado.

WAP está dirigido por una asociación industrial denominada Foro WAP. En la actualidad el foro reúne a más de 600 fabricantes de teléfonos y redes, operadores, empresas del sector de la tecnología de la información y proveedores de contenidos.

El Foro WAP respalda a un número de fabricantes de microteléfonos que representa el 99% del mercado mundial, cubriendo a más de 300 millones de usuarios de teléfonos móviles de todo el mundo.

GPRS es un excelente portador para distintos tipos de aplicaciones inalámbricas de datos con transmisiones de datos de carácter esporádico, en especial para la recuperación de información y el acceso a bases de datos basados en WAP.

WAP está diseñado para transmitir información en un formato óptimo para su visualización en dispositivos de cliente ligero. Además, los servicios y aplicaciones que admiten WAP funcionan en todo tipo de redes, tanto actuales como futuras. No obstante, los servicios óptimos para el usuario se disfrutan mediante el envío de los contenidos WAP a través de un servicio de conmutación de paquetes, como GPRS. En este entorno, los abonados pueden seleccionar el acceso instantáneo a servicios WAP.

Los contenidos WAP se optimizan para dispositivos de cliente ligero, como teléfonos móviles, y además son avanzados, haciendo posible su utilización con 2.5G, 3G y otras redes. Entre las funciones GPRS se incluye el uso eficaz de recursos, acceso online instantáneo, entrega rápida de la información e innovadores modelos de cobro. Juntos, WAP y GPRS no sólo mejoran la experiencia del usuario con las aplicaciones ya existentes, sino que también permiten nuevos servicios, por ejemplo, el nuevo soporte es idóneo para juegos interactivos para dos o más participantes. Estos juegos pueden ser de tipo respuesta rápida, que tanto gustan a niños y adolescentes, o juegos de un ritmo más lento, como el ajedrez, y que precisan más tiempo para su finalización. Cada jugador puede hacer su elección con su móvil y los movimientos se pueden realizar de forma inalámbrica.

Estas ventajas también se encuentran en otras aplicaciones que conlleven la interacción en tiempo real o sesiones de larga duración, como subastas online, chat, grupos de noticias y casinos online. La rapidez en los tiempos de respuesta, junto con unos precios razonablemente bajos, impulsara a un mayor uso de los servicios móviles.

Otra herramienta útil es la posibilidad de conexión a numerosos servicios de información. Imagínate a un grupo de amigos que, mientras toman una copa, deciden ir al cine. Sin levantarse del asiento, pueden consultar las películas en cartel, realizar su elección y, a continuación, seleccionar un enlace para reservar entradas y pagar los boletos. La transacción se puede registrar en el teléfono y se puede mostrar al llegar al cine para poder entrar.

Juntos, WAP y GPRS representan un sistema altamente eficaz para usuarios finales de móviles, operadores, proveedores de servicios, empresas y realizadores de aplicaciones.

2.3.2.- SYSTEMAS DE CÓMPUTO MÓVIL

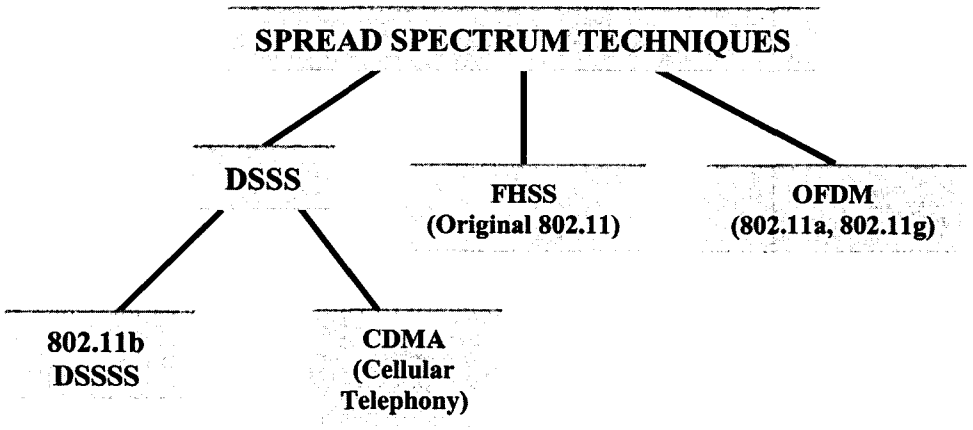

Figura 5.- Métodos Spread Spectrum

WI-FI

Wireless Local Area Network (WLAN) fue diseñada originalmente para redes empresariales internas. Entretanto, el incremento de nuevos usos está empezando a divisarse. En el ambiente residencial, por ejemplo, un servicio ADSL puede correr en cualquier lugar del hogar, con múltiples usuarios conectados a la WLAN. En el ambiente publico, los puntos de acceso WLAN están empezando a desplegarse en supuestos "hot spots" como en aeropuertos, hoteles, restaurantes, centros de conferencias, etc. Son especialmente atractivos para las personas de negocios que están en movimiento, al permitir a sus laptops equipadas con una tarjeta WLAN conectarse a internet, a sitios web corporativos, o a sitios web locales. (Aguirre, José Eduardo, 2002).

Wireless LANs (WLANs) están basadas en el estándar IEEE 802.11 que puede proveer movilidad para usuarios de redes corporativas mientras mantienen los requisitos de los recursos de conectividad. Una laptop y una PDS son los dispositivos más usados en el ámbito laboral, los usuarios tenderán a usar estos dispositivos como sus principales herramientas, el conducir con una mayor portabilidad para las reuniones, conferencias y durante los viajes de negocios. WLANs ofrece a las organizaciones gran productividad por parte de los empleados por proveer una conectividad constante a las redes tradicionales en lugares donde anteriormente no estaba disponible.

De acuerdo a Allied Business Intelligence, el envío de paquetes WLAN a crecido alrededor de 7.6 millones de unidades totales enviadas en 2001 a 23 millones en 2002. Esto es considerable sobre el pronóstico inicial de 15 millones de paquetes de todo el mercado WLAN. El mercado WLAN abarca varias tecnologías, cada una caracterizada por sus ventajas específicas y contrastantes, las cuales ayudaran a que el operador haga sus elecciones.

PROTOCOLOS UTILIZADOS EN WIFI

Protocol	Bandwidth	Frequency	Distance Range
802.11	2 Mbps	2.4 Ghz	160 feet (50 meters)
802.11a	6, 12, 24, and up to 54 Mbps	5-6 Ghz	50-90 feet (15-30 meters)
802.11b	1, 2, 5.5, 11, and up to 20 Mbps	2.4 Ghz	300 feet (100 meters)
802.11g	22 Mbps	2.4 Ghz	150-300 feet (50-100 meters)

Tabla 1.- Protocolos de Acceso para Wireless LAN

IEEE 802.11b/g

EEE 802.11b está actualmente en un desarrollo mas extenso. Opera en la banda de 2.4 Ghz y entrega un máximo rendimiento de procesamiento de 11 Mbps. Desde 1999, la alianza Wi-Fi ha publicado el certificado de interoperabilidad entre productos 802.11b de diferentes proveedores. (Aguirre, José Eduardo, 2002).

802.11g es una extensión de 802.11b, la base de la mayoría de las redes inalámbricas de hoy en día. 802.11g logra llegar a transmisiones de, efectivamente, 54Mbps en el entorno de 2,4 GHz utilizando la tecnología OFDM (Orthogonal Frequency División Multiplexing). Debido a su compatibilidad con soluciones anteriores en 2,4 GHz, un entorno 802.11b es directamente compatible con 802.11g.

IEEE 802.11a/h

IEEE 802.11a es una evolución de IEEE 802.11b que ofrece mayor ancho de banda. Opera en la banda de los 5 Ghz, con un máximo rendimiento de procesamiento de 54 Mbps. Un nuevo estándar, IEEE 802.11h, agregara las funciones de Transmit Power Control (TPC) y Dynamic Frecuency Selección (DFS) para el estándar 802.11a. (Aguirre, José Eduardo, 2002).

IEEE 802.11d/e/f/i

En adición a la definición de la capa física, otro grupo está trabajando en ediciones como QoS y seguridad.

Muchas de esas actividades aún están en proceso. 802.11d (Regulatorio) define como el punto de acceso comunica información a los dispositivos de los usuarios sobre el canal de radio y los niveles de poder permitidos.

Este trabajo esta siendo completado y es parte del estándar 802.11e (Multimedia y QoS) clases de servicio definidas con niveles de manejo de QoS para aplicaciones de datos, voz y vídeo. 802.11f (Movilidad) recomienda prácticas para un Inter-Access Point Protocol. 802.11i (Seguridad) especifica nuevas funciones de seguridad. (Aguirre, José Eduardo, 2002).

Según el ancho de banda requerido se tienen distintas tecnologías aplicables:

Banda estrecha: Se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada. (Pesoa, 2002).

En el caso norteamericano, una vez que una cierta banda de frecuencias es asignada a un determinado usuario, ella no puede ser asignada ningún otro dentro de un radio de aproximadamente 30 Km. (Pesoa, 2002).

Banda ancha: La técnica de espectro disperso es actualmente la más utilizada en las LANs inalámbricas. Inicialmente, las técnicas de espectro esparcido fueron desarrolladas con el propósito de combatir las interferencias en las comunicaciones militares, lo cual se logra esparciendo el espectro de la señal transmitida sobre determinadas bandas de frecuencias. (Pesoa, 2002).

Hay dos tipos de tecnología de espectro disperso:

a) Frecuencia esperada (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración. (Pesoa, 2002).

b) Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado. (Pesoa, 2002).

2.3.3.- CONFIGURACIONES WLAN

Pueden ser simples o complejas. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual.

RED PEER-TO-PEER

Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o pre-configuración. (Pesoa, 2002).

Figura 6.- (Asisa, 2002) Red peer-to-peer

CLIENTE Y PUNTO DE ACCESO

Instalando un Punto de Acceso (APs) se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red alámbrica cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso. (Pesoa, 2002).

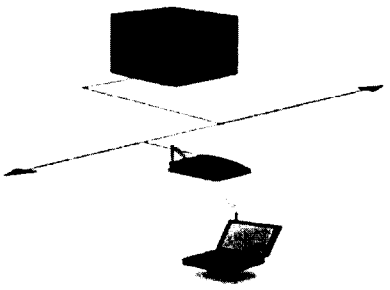

Figura 7.- (Asisa, 2002) Cliente y punto de acceso

MÚLTIPLES PUNTOS DE ACCESO Y "ROAMING"

Los puntos de acceso tienen un rango finito, del orden de 150m en lugares cerrados y 300m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso a esto se le llama "roaming". (Pesoa, 2002).

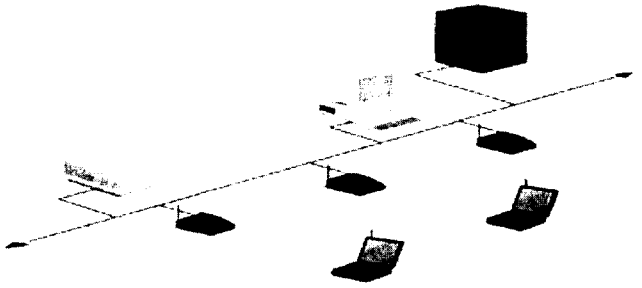

Figura 8.- (Asisa, 2002) Múltiples puntos de acceso y "roaming".

USO DE UN PUNTO DE EXTENSIÓN.

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red alámbrica como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos. (Pesoa, 2002).

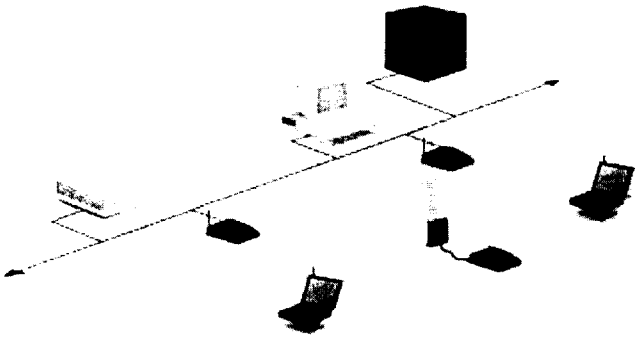

Figura 9.- (Asisa, 2002) Uso de un punto de extensión.

UTILIZACIÓN DE ANTENAS

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: se quiere una LAN sin cable a otro edificio a 1Km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red alámbrica mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación. (Pesoa, 2002).

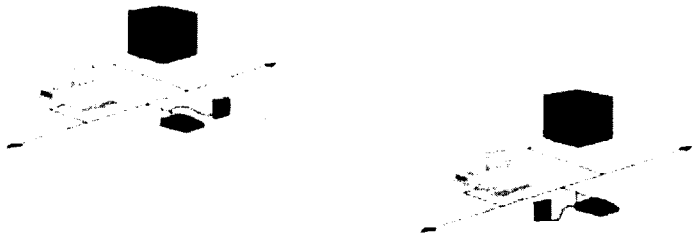

Figura 10.- (Asisa, 2002) Utilización de antenas direccionales.

2.3.4.- MOBILE IP

Con el rápido progreso en el desarrollo de la tecnología inalámbrica, avances recientes en WLANs han demostrado sus promesas para rachas altas en transmisiones inalámbricas de datos. Complementando a los operadores de servicios existentes de GSM y GPRS, la tecnología WLAN provee un significativo costo-efectividad del ancho de banda para acceso a internet. No solo instalado en oficinas interiores, hay también muchas WLANs desplegadas en espacios públicos y campus (Hot Spots). En el presente, WLAN como 802.11b puede transmitir datos a más de 100 metros. Con el incremento de la distancia de transmisión, WLAN quizá también provea una solución económica para transmisión de datos en exteriores, especialmente en áreas regionales como campus o parques. Operando en las bandas industrial, científica y médica (ISM) sin licenciar, una universidad u organización podrá construir una red inalámbrica con WLAN y existiendo un backbone alámbrico para cubrir el campus entero y proveer acceso de banda ancha.

En adición para proveer acceso a Internet, podremos desarrollar un sistema de dirección de campus que provea servicios de multimedia y navegación para cubrir los usuarios móviles en el campus y soportar movilidad IP con WLAN. Ayudado con un sistema de posicionamiento, un visitante puede navegar en un campus con un dispositivo de mano (PDA, Palmtop, etc.) o a bordo de una unidad y viajando alrededor de la estación base usando servicios multimedia a través de WLAN. (Vinay Anand, 2003).

- En internet, más aplicaciones son desarrolladas en modelo cliente-servidor donde la interacción del servicio es iniciada por la petición del cliente. Esto implica que la conexión entre un nodo móvil y un nodo correspondiente es más probable iniciarla por el nodo móvil. (Vinay Anand, 2003).

- Muchos proveedores de contenido construyen grupos de servidores de contenido en la web. Una petición de contenido de usuario para un proveedor en la misma sesión puede conectarse a más de un servidor del proveedor. Esto significa que un nodo móvil accesa a mas de un nodo correspondiente en la misma subred durante una sesión. (Vinay Anand, 2003).

- Específicamente en un sistema de guía regional, los visitantes usualmente están en algún lugar fuera de la región y probablemente están interesados en los servicios de navegación y localización que proveen los servidores internos. Esto sugiere que en un sistema, los agentes locales de los nodos móviles están usualmente fuera de la intranet móvil y muchos nodos correspondientes interesados están fuera. Con la entrega de paquetes se usa un ruteo de triángulo y un tuneleo en reversa para tal sistema. (Vinay Anand, 2003).

- Los vecinos visitantes arriban a la misma célula o acceso. (Vinay Anand, 2003).

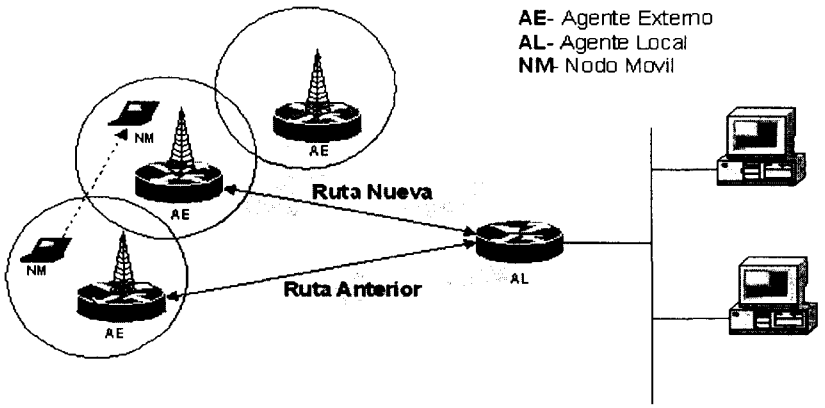

Figura 11.- Diagrama de Red para Roaming con Mobile IP

2.3.5.- DISPOSITIVOS MOVILES

En la actualidad existen una gran variedad de dispositivos inalámbricos que nos permiten realizar actividades diversas, a continuación se mencionan algunos de los más importantes utilizados por usuarios móviles y a los cuales va a estar enfocado el modelo de seguridad.

- Notebook o Laptop

  Este es uno de los elementos de mayor uso en las redes inalámbricas, ya que en los últimos años se ha incrementado su demanda gracias a la disminución de los costos y a la integración de varias tecnologías soportadas en un solo dispositivo.

Figura 12.- Laptop

- Tarjetas de Red Inalámbricas

  Estos dispositivos permiten a los usuarios poder conectarse a la red sin necesidad del uso de cables y ofrecen la funcionalidad de poder ir de un lugar a otro lo que permite tener movilidad. Gracias a los nuevos estándares estas tarjetas de radio multimodo permiten el acceso a redes a través de GPRS, HSCSD o redes LAN inalámbricas, ofreciendo velocidades de hasta 40.2 kbit/s en redes GPRS, hasta 43.2 kbit/s en redes HSCSD y hasta 11 Mbit/s en redes LAN inalámbricas (actualmente hasta 56 Mbps gracias a los nuevos estandares 802.11x).

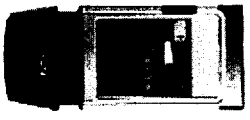

Figura 13.- Tarjeta Wireless compatible con GPRS, HSCSD y WiFi

Existen tres categorías fundamentales cuando se habla de estos organizadores personales (no contando los teléfonos inteligentes y las Pocket PC con Phone Edition): HandHeld, Palmsize y Pocket PC

- *Handheld*

HandHeld es aquel dispositivo que su tamaño es algo más grande que la palma de la mano y posee un teclado. La forma es muy parecida a la de una Laptop pero más pequeña.

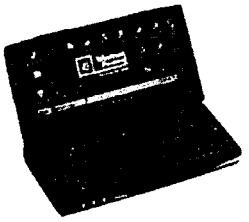

Figura 14.- Handheld

- *Palmsize*

Palmsize son las antecesoras de nuestras Pocket PCs. Al parecer el nombre fue cambiado para evitar equivocaciones con las Palms. Estos dispositivos están ya descontinuados y no hay ninguno en el mercado.

- *Pocket PC*

Pocket PC es aquel dispositivo que cabe en la palma de la mano o mejor aún, en un bolsillo. De ahí el nombre de Pocket PC

Estos dispositivos han presentado una transformación considerable, gracias a la incorporación de tecnologías como Wi-Fi o GSM/GPRS ha tenido un resurgimiento importante, logrando un incremento en su uso y en los diferentes servicios a los cuales se es posible acceder por medio de este dispositivo.

Figura 15.- Pocket PC

- Smart Phone

  Se ha presentado una transformación muy significativa en la tecnología celular, lo que ha permitido incorporar muchos nuevos servicios, la llegada de las tecnologías 2.5G y 3G ofrecen una amplia gama de servicios. Smart Phone es un dispositivo de tecnología celular, el cual puede desempeñar funciones de una Pocket PC.

Figura 16.- Smart Phone

Existen muchos otros dispositivos que tienen la capacidad para operar con tecnologías inalámbricas, pero sería muy extenso mencionar cada una de ellas, por lo que solo se mencionan los dispositivos finales utilizados por los usuarios móviles.

2.3.6.- SERVICIOS MOVILES

Al igual que los dispositivos móviles, existen muchas ofertas en servicios para usuarios móviles, a continuación se mencionan algunas de ellas para poder tener una idea del alcance del modelo de seguridad que se pretende desarrollar.

E-mail: es una herramienta que permite enviar y recibir mensajes, ficheros, documentos, a través de una red de datos a otra persona de esa red y de una manera rápida y eficaz. (Siemens, 2003).

VPN Móviles: Es una forma de conectar una o más redes privadas preexistentes, de tal manera que las redes parezcan una sola para un usuario, es decir, pueden accesar a los servicios que tiene la empresa, a través de cualquiera de sus redes. (Alonso, 2002).

Videoconferencias: Se define como un sistema de comunicación diseñado para llevar a cabo encuentros a distancia en tiempo real que le permite la interacción visual, auditiva y verbal con personas de cualquier parte del mundo.(Comtelca,2001).

Telefonía de VoIP: Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos. (Sánchez, 2002).

Conexiones hacia Internet: Es una forma de conectar a una o más computadoras, independientemente del lugar en que se encuentren, a través de algún dispositivo inalámbrico, como una palm, una NIC inalámbrica, etc, para poder accesar al servicio de internet. (Alonso, 2002).

Transferencia de Archivos: Los usos de la transferencia de archivos abarcan cualquier forma de descargar datos importantes a través de la red móvil. Estos datos podían ser un documento de la presentación para un vendedor que se encontraba viajando, un manual de la aplicación para un servicio de ingeniería o un software de aplicación tal como Adobe Acrobat Reader para leer documentos.

Servicio de Mensajería Multimedia (EMS): Supone la transición desde los SMS hasta los MMS (Multimedia Messaging Service). EMS está basado en los estándares de SMS por lo que su implantación es relativamente fácil, pero permite que los mensajes contengan animaciones, fotos, melodías y texto con formato. Los mensajes EMS pueden suponer la continuación del inmenso éxito que han supuesto los SMS en todo el mundo. Para muchos especialistas serán la clave del éxito de la nueva generación de servicios de datos.

Comercio Electrónico Móvil: M-commerce se refiere al comercio electrónico móvil, es decir, la posibilidad de realizar transacciones comerciales a través de un dispositivo móvil. En este tipo de comercio móvil están incluidos todos los pasos de una transacción comercial. En este proceso, el pago es el que presenta más problemas y el que genera más dolores de cabeza al momento de diseñarlo o administrarlo con el objetivo de garantizar transacciones seguras y fiables.

Aprendizaje On-Line: Requiere de la convergencia de otras aplicaciones como puede ser la transferencia de ficheros, descarga de ficheros de audio, vídeo e imagen e incluso servicios de videoconferencia.

2.4.- TIPOS DE ATAQUE INALÁMBRICO

2.4.1.- LOS HACKERS DE REDES INALÁMBRICAS

Con frecuencia la señal Wi-Fi no se queda entre las cuatro paredes de la oficina, sino que puede ser detectada, utilizada y/o explotada por aquellos atacantes conocidos como hackers de redes inalámbricas (*War Drivers*) y hackers de señales inalámbricas (*War Chalkers*). Con la ayuda de un equipo sencillo y un software "rastreador" de los puntos de acceso inalámbrico que está listo para su descarga de Internet, estos individuos recorrerán ciudades y pueblos en busca de puntos inseguros de acceso inalámbrico.

Los hackers de redes inalámbricas tienen mucha práctica y han dedicado muchos sitios Web y carteleras de anuncios para mejorar sus actividades y compartir sus ideas. Los hackers de redes inalámbricas dedicados consiguen la ayuda del equipo más sofisticado, como antenas que ayudan a recoger las señales y receptores del Sistema de Posicionamiento Global (GPS) que se utilizan para obtener las coordenadas exactas (longitud y latitud) de un punto de acceso inalámbrico detectado con fines de mapeo.

Otro creciente fenómeno es el ataque a señales inalámbricas (*War Chalking*), derivado de la práctica de los vagabundos durante la época de la Depresión que consistía en señalar los hogares y empresas amigables marcando sus andenes y cercas. En el caso del ataque a señales inalámbricas, se pintan los símbolos en el edificio o en el pavimento para indicar que hay un punto de acceso Wi-Fi para que otros puedan aprovechar la señal. Siempre existe el peligro de que estos grupos clandestinos puedan detectar y vulnerar los puntos de acceso desprotegidos de su empresa.

2.4.2.- LAS MOTIVACIONES DEL ATAQUE A LAS REDES INALÁMBRICAS (*WAR DRIVING*)

Para muchos, el ataque a las redes inalámbricas (*War Driving*) es una afición inocua y un juego motivado por su interés en la tecnología. Otros argumentan que están probando que debe haber mayor seguridad inalámbrica al mostrar la gran cantidad de puntos de acceso inalámbrico inseguros que encuentran. Sin importar cómo se analice el asunto, si un hacker de redes inalámbricas (*War Driver*) intercepta la red inalámbrica de una empresa, la pone en grave peligro. Un punto abierto de acceso puede exponer toda la red a la actividad de los hackers. El problema no es únicamente la destrucción que pueden ocasionar a una red empresarial, sino también el gran potencial del robo de información. Con el software adecuado, un hacker sería capaz de ver los contenidos de todo el tráfico de la red incluyendo detalles específicos como los nombres de usuario y de archivo.

2.4.3.- EL PERFIL CAMBIANTE DE LOS ATACANTES

A medida que aumentan las amenazas en cantidad y complejidad, se presenta una evolución en el perfil de los atacantes. Muchos de los ataques recientes de alto perfil han sido lanzados por "aficionados" sin un objetivo o motivación particular. Sin embargo, puesto que las funciones más críticas de las empresas privadas y el gobierno se realizan en línea, esperamos ver una evolución de atacantes más "profesionales" con objetivos y motivaciones más específicos. Estos atacantes con mejores conocimientos y mayor dedicación pueden ser capaces de encontrar y aprovechar las vulnerabilidades mucho más rápido.

2.4.4.- MENOR TIEMPO DE REACCIÓN

Los ataques combinados, los gusanos y hackers con frecuencia aprovechan las vulnerabilidades conocidas del software informático. Por lo general, estos ataques ocurren un tiempo después de descubrir la vulnerabilidad. Me refiero al momento entre el descubrimiento y aprovechamiento de la vulnerabilidad por medio de una amenaza específica como la ventana de amenazas a la vulnerabilidad. Por ejemplo, los gusanos Nimda y Slammer tenían ventanas de amenazas a la vulnerabilidad desde hacía muchos meses lo que le daba mucho tiempo al proveedor de software vulnerable para crear un parche y advertir al público, lo que reducía los daños por amenazas potenciales. En promedio, se crean ataques seis meses después de que la vulnerabilidad se ha revelado públicamente. Así como vemos un aumento de los atacantes profesionales cómo se menciono anteriormente, probablemente veremos menos ventanas de amenazas a la vulnerabilidad. Si un atacante tiene buenos conocimientos, posiblemente tendrá mayores recursos para encontrar nuevas vulnerabilidades y rápidamente crear amenazas asociadas. Esto puede en última instancia ocasionar la emergencia del Día Cero. La amenaza del Día Cero ocurre cuando se crea y libera un ataque tan pronto como se encuentra la vulnerabilidad asociada, lo que no les da tiempo de reacción a los proveedores de software, administradores y usuarios informáticos.

2.4.5.- AMENAZAS ACTUALES Y FUTURAS

Podemos separar las amenazas actuales de las de próxima aparición al asignarles clases generales con base en la rapidez con que se propagan. Cuando se pasa de la clase I a la III, no existen muchas posibilidades de que la respuesta humana pueda contener la amenaza:

- *Amenazas actuales o de clase I*: Las amenazas de clase I se propagan en días u horas. A la fecha, la mayoría de ataques pertenece a esta categoría. Las amenazas de clase I incluyen los gusanos del correo electrónico y muchas amenazas combinadas. Es posible la reacción humana a estas amenazas mediante actualizaciones de antivirus, filtros de enrutadores y reglas de firewall.

- *Amenazas actuales y futuras o de clase II*: Las amenazas de clase II pueden propagarse por Internet en cuestión de horas o minutos. El gusano SQL Slammer que atacó este año nos deja entrever lo que puede hacer una amenaza de clase II puesto que la tasa de infección de Slammer se duplicó cada 8.5 segundos en sus fases iniciales y durante sus primeros cinco días, y produjo pérdidas en la productividad por aproximadamente mil millones de dólares. Las amenazas de clase II de más rápida propagación son muy difíciles o imposibles de contrarrestar a través de mecanismos de respuesta humana y requieren respuestas más automatizadas.

- *Amenazas futuras o de clase III*: Las amenazas futuras de clase III serán capaces de atacar los sistemas de Internet en tan solo segundos y serán una posibilidad muy real debido a la conectividad extendida. La reacción humana a estas amenazas será imposible e incluso la respuesta automatizada más rápida será improbable. Defenderse de las amenazas de clase III requerirá fundamentalmente de nuevas tecnologías proactivas, las cuales deberán ser capaces de bloquear nuevas amenazas a las computadoras host y de redes antes de que se puedan esparcir.

A continuación se mencionan algunas de las amenazas más importantes en el ambiente inalámbrico:

- *Eavesdropping*: Los hackers pueden fácilmente escuchar secretamente el trafico de la red a través del monitoreo de las ondas de radio transmitidas por el access point o el router inalámbrico. Para esto solamente se requiere un receptor de radio con una antena de alta ganancia que pueda interceptar transmisiones de tráfico de red. Este tipo de ataque puede darse sin el conocimiento del administrador o usuario de la red. (Miller, 2003).

- *Breakin In*: Este tipo de ataque se presenta cuando un usuario inalámbrico quiebra la red desde adentro, disfrazado cómo un usuario autorizado. Una vez que el hacker obtiene acceso a los sistemas internos, puede corrumpir, robar, borrar, o destruir datos confidenciales muy valiosos desde cualquier parte de la red. (Miller, 2003).

- *Counterfeiting*: Este ataque consiste en que un hacker instala un access point no autorizado para construir otras estaciones de acceso inalámbricas en lugar de la red autorizada. El counterfeiting access point puede atracar una estación inalámbrica dentro de una red falsa para poder copiar las claves de encripción usadas para registrarse en el access point de la red verdadera. (Miller, 2003).

- *DoS Inalámbrico*: Este tipo de ataque consiste en la compleja creación de un poderoso transmisor, lo suficiente para inundar la banda de 2.4 Ghz (espectro de frecuencia que usa 802.11 para construir conexiones WLAN) con interferencia. Con el poder suficiente, este tipo de ataque puede anular el tráfico de cualquier red inalámbrica. Puede realizarse desde un auto ubicado cerca de las instalaciones de la compañía a atacar. (Miller, 2003).

2.5.- FACTORES DE SEGURIDAD INALÁMBRICOS

Los principales factores que definen la seguridad en un ambiente inalámbrico pueden ser resumidos en cinco elementos; a continuación se explican cada uno de ellos:

1. Robo: Usuarios no autorizados frecuentemente tratan de registrarse a la red para robar la información y utilizarla para beneficio propio. (Miller, 2003).

2. Control de Acceso: Muchas compañías establecen muchos permisos simples de acceso. (Miller, 2003).

3. Autenticación: ¿Conoces si el usuario registrado es quien dice ser?. En muchas redes inalámbricas las empresas configuran una sola cuenta, "usuario inalámbrico", y esa cuenta puede ser usada en muchos dispositivos diferentes. El problema es que un hacker (con su propio dispositivo inalámbrico) puede fácilmente registrarse sobre esta cuenta general y obtener acceso a la red. (Miller, 2003).

4. Encripción: Si un usuario no es capaz de registrarse directamente a la red, quizá este usando un "extractor de paquetes" inalámbrico para espiar el tráfico de la red. De esta forma, incluso si el hacker no puede autenticarse el mismo dentro de la red, puede robarse información sensitiva para monitorear el tráfico y encontrar información útil. (Miller, 2003).

5. Salvaguardas: La mejor salvaguarda es familiarizarse con la propia red WLAN y el router inalámbrico. Deberás conocer los pasos sobre consideraciones serias y establecer llaves de encripción al menos de 64 bits, pero preferentemente de 128 bits. (Miller, 2003).

2.6.- PATRONES DE ATAQUE INALÁMBRICO

Los ataques inalámbricos son activos y pasivos, como se muestra a continuación

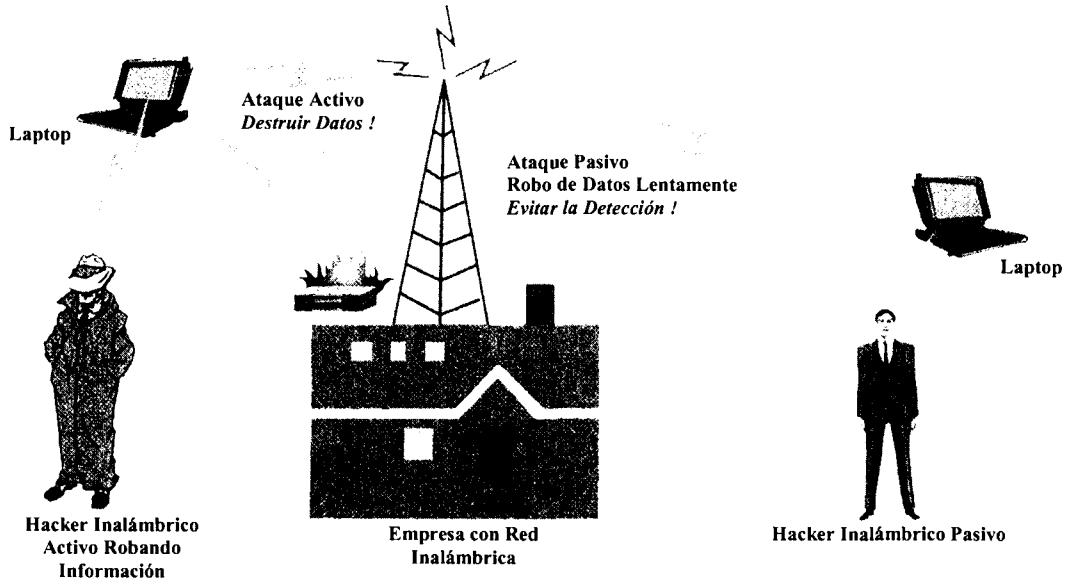

Figura 17.- (Miller, 2003) Patrones de Ataques Pasivos y Activos

PATRONES DE ATAQUE ACTIVOS

Un ataque activo constituye un patrón donde un hacker procura modificar el canal de datos, mensajes o archivos. Mediante una vigilancia constante se deberá tener la capacidad de detectar este tipo de ataque; sin embargo este tipo de ataque es difícil de prevenir sin realmente desconectar tu WLAN.
Los ataques activos incluyen: denegación de servicio (DoS) y alteración de mensajes.

PATRONES DE ATAQUE PASIVOS

En estos ataques, un usuario no autorizado obtiene acceso a los datos fuente de la red. No hay alteración del contenido del mensaje, pero es posible que este espiando la transmisión. Los ataques pasivos se presentan sin provocar interrupciones, pero se utilizan para obtener información que viaja o fluye a través de la red inalámbrica.

2.7.- MODELOS DE SEGURIDAD

La seguridad de información cubre muchas áreas dentro de la empresa. Cada área tiene vulnerabilidades de seguridad, alentadamente, algunas contramedidas para presentar el nivel de seguridad y proveer la mejor protección. Sin entender las diferentes áreas y niveles de seguridad de los dispositivos de red, sistemas operativos, hardware, protocolos, y aplicaciones que pueden causar vulnerabilidades de seguridad que pueden afectar el ambiente en su totalidad. (CISSP, 2003).

Un modelo de seguridad es una metodología que da forma a los requerimientos necesarios para soportar e implementar una cierta política de seguridad, provee una explicación detallada de los pasos a seguir para poder desarrollar apropiadamente políticas y procesos de seguridad específicos. Ayuda a mapear los alcances y metas de las medidas de seguridad que se desean implementar, se puede decir que un modelo proporciona una guía a seguir, la cual provee los pasos o etapas a seguir para hacer una adecuada implementación de las medidas de seguridad en una empresa.

Un modelo de seguridad es la representación simbólica de una o más políticas. Este es un mapa de los desarrolladores de políticas dentro de una serie de reglas que son seguidas por un sistema de cómputo.

Un modelo de seguridad realiza un mapeo de las metas de la política en términos de sistemas de información para especificar estructuras de datos explícitas y técnicas necesarias para impulsar la política de seguridad. (CISSP, 2003).

Algunos modelos de seguridad refuerzan las reglas para proteger la confidencialidad, como es el caso del modelo de Bell-LaPadula. Otros modelos refuerzan las reglas para proteger la integridad, como es el modelo de Biba. Los modelos de seguridad formal, como los de Bell-LaPadula y Biba, son usados para proveer un nivel alto de seguridad. Los modelos informales, como el de Clark-Wilson, son mas usados como un marco para describir como las políticas de seguridad deberán ser expresadas y ejecutadas.

2.5.1.- MODELO DE Bell-LaPadula

En 1970, el ejército de los E.U. usaba sistemas de tiempo compartido y tenia preocupación acerca de la seguridad de estos sistemas y de la salida de información clasificada. El modelo de Bell-LaPadula fue desarrollado para tratar estas preocupaciones. Fue el primer modelo matemático de una política de seguridad multi-nivel usado para definir el concepto de una maquina de estado seguro y modelos de acceso y las reglas externas de acceso. El principal objetivo del modelo es prevenir que la información secreta sea accesada de alguna forma no autorizada.

Un sistema que emplea el modelo de Bell-LaPadula es llamado sistema de seguridad multinivel porque usuarios con obligaciones separadas usan el sistema, y el sistema procesa datos con diferentes clasificaciones. El nivel en el cual la información es clasificada determina la manipulación de procedimientos que deberán ser usados. Estos derechos de acceso juntos forman un enrejado, el cual es un límite superior y limite inferior de acceso autorizado. El nivel ultra secreto es el límite superior y un nivel no clasificado es el límite inferior. El control de acceso mandatario esta basado en un enrejado de etiquetas de seguridad.

2.5.2.- MODELO DE Biba

El modelo de Biba fue desarrollado después del modelo de Bell-LaPadula. Usa un modelo de maquina de estado y es muy similar al modelo de Bell-LaPadula. Biba trata la integridad de los datos que son amenazados cuando sujetos en niveles de prioridad baja son capaces de escribir en los objetos con niveles de integridad alta y cuando sujetos pueden leer datos en niveles bajos. Si se implementa y se refuerza correctamente, el modelo de Biba previene datos de cualquier nivel de integridad para que fluyan a un nivel de integridad alto.

El modelo de Biba dos reglas principales para proveer este tipo de protección. La primera regla, se refiere a "no write up", estados en los cuales un sujeto no puede escribir datos en un objeto en alto nivel de integridad. La segunda regla, se refiere a "no read down", estados en los que un sujeto no puede leer datos de un nivel de integridad baja. Esta segunda regla suena un poco tonta, pero esta regla protege a sujetos y datos en un nivel de alta integridad de la corrupción de datos en un nivel de baja integridad.

2.5.3.- MODELO DE Clark-Wilson

El modelo de Clark-Wilson fue desarrollado después del modelo de Biba y toma algunos acercamientos diferentes para proteger la integridad de la información enfocándose en prevenir que usuarios autorizados no realicen modificaciones no autorizadas de datos, o cometan fraude o errores en aplicaciones comerciales.

Según lo anterior, las instituciones militares están frecuentemente más conscientes de la confidencialidad, y el sector comercial esta usualmente más consciente de la integridad de los datos que procesan. En el modelo Clark-Wilson, los usuarios no pueden acceder y manipular objetos directamente, pero deben tener acceso al objeto a través del programa.

Este modelo también refuerza la separación de responsabilidades, mientras divide una operación en diferentes partes y requiere diferentes usuarios o reglas para realizar cada parte. Esto asegura que una tarea crítica no pueda realizarse por otra entidad. La revisión también es requerida en este modelo para que la información continúe entrando de un sistema externo.

2.6.- ESTANDAR DE SEGURIDAD

2.6.1.- BRITISH STANDARD BS-7799

En la actualidad muchas empresas a nivel mundial, han tomado el estándar británico como referencia para poder crear sus modelos de seguridad, esto es a consecuencia de que el BS-7799, es un estándar muy reconocido a nivel mundial, por su alcance y efectividad. (Bsi, 2003). El British Standard esta compuesto de dos partes BS-7799-1 y BS-7799-2.

BS-7799-1

BS-7799-1:Code of Practice for Information Security Management, Código de Practica para el Manejo de Seguridad de Información. Es una guía de implementación, basada en sugerencias. Es usado como una forma de evaluar y construir una sólida y comprensiva infraestructura de seguridad de información. Detalla los conceptos de Seguridad de Información en la organización "debe hacerse". Da las recomendaciones para el Manejo de Seguridad de Información para ser usadas por quienes son responsables de iniciar, implementar o mantener la seguridad en la organización. Esta destinado a proveer las bases para desarrollar estándares de seguridad organizacional y la practica para el manejo efectivo de seguridad y para proveer confidencialidad en trafico inter-organizacional. (Iso, 2003)

Consta de 10 partes esenciales para el Manejo de Seguridad de Información:

1.- *Políticas de Seguridad de Información*: Proveer dirección de administración y soporte para la seguridad de la información. (Bsi, 2003).

2.- *Seguridad Organizacional*: Para el manejo de iniciativas de seguridad de la información dentro de la organización. (Bsi, 2003).

3.- *Clasificación y Control de Bienes*: Para mantener la protección apropiada de los bienes de la organización. (Bsi, 2003).

4.- *Seguridad Personal*: Para reducir los riesgos de error humano, robo, fraude o el mal uso de los servicios. (Bsi, 2003).

5.- *Seguridad Física y Ambiental*: Para prevenir accesos no autorizados, daño e intromisión a las instalaciones del negocio y a la información. (Bsi, 2003).

6.- *Administración de Comunicaciones y Operaciones*: Para asegurar la correcta y segura operación de los servicios de procesamiento de información. (Bsi, 2003).

7.- *Control de Acceso a los Sistemas*: Para controlar el acceso a la información. El acceso a la información y los procesos de negocios deberán ser controlados con base en los requerimientos del negocio y de la seguridad. (Bsi, 2003).

8.- *Desarrollo y Mantenimiento de Sistemas*: Para asegurar que la seguridad existe dentro de los sistemas de información. (Bsi, 2003).

9.- *Administración de la Continuidad de Negocios*: Para contrarrestar interrupciones a las actividades del negocio y para proteger los procesos de negocio críticos de los efectos de grandes fallas o desastres. (Bsi, 2003).

10.- *Cumplimiento*: Para evitar violaciones de cualquier criminal y ley civil, estatutaria, regulatoria u obligaciones contractuales y de cualquier requerimiento de seguridad. (Bsi, 2003).

BS-7799-2

BS-7799-2: Specification for Information Security Management Systems, Especificaciones para el Sistema de Administración de Seguridad de Información. Es una guía de Auditoria, basada en requerimientos. Para realizar certificaciones de cumplimiento del BS-7799, las organizaciones son auditadas por la parte dos. Detalla los conceptos de Seguridad de Información en la organización "tendrá que hacerse". (Bsi, 2003).

Una organización deberá identificar y manejar muchas actividades en orden para funcionar efectivamente. Cualquier actividad usando recursos y manejada en orden para habilitar la transformación de entradas a salidas, puede ser considerada como un proceso. Frecuentemente la salida de un proceso directamente forma la entrada del siguiente proceso. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacción de estos procesos y su manejo, puede ser referenciado como un "enfoque de procesos". (Bsi, 2003).

Un enfoque de procesos fomenta a los usuarios a enfatizar la importancia de:

a).- Entendimiento de los requerimientos de seguridad de información de negocios y la necesidad de establecer políticas y objetivos para la seguridad de la información.

b).- Implementación y operación de controles en el contexto del manejo de riesgos de negocios en las organizaciones.

c).- Monitoreo y revisión del cumplimiento y eficacia del Sistema de Administración de Seguridad de Información (ISMS).

d).- Mejora continua basada en la medición de objetivos.

El modelo conocido como el "Plan-Do-Check-Act" (PDCA) puede ser aplicado a todos los procesos de ISMS como adopción en este estándar. (Bsi, 2003).

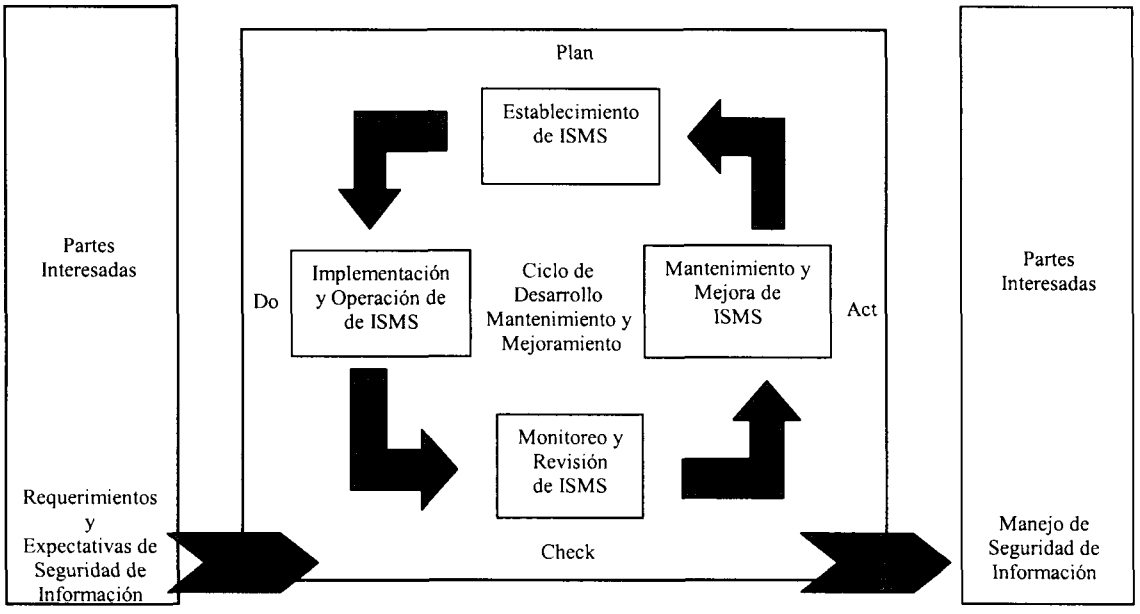

Figura 18.- (Bsi, 2003) Modelo PDCA aplicado a ISMS de procesos

Plan (Establecimiento de ISMS). Establecimiento de políticas de seguridad, objetivos, procesos y procedimientos relevantes para el manejo de riesgos y mejora de la seguridad de información para comunicar resultados acordes con las políticas y objetivos de la organización. (Bsi, 2003).

Do (Implementación y Operación de ISMS). Implementa y opera las políticas de seguridad, controles, procesos y procedimientos. (Bsi, 2003).

Check (Monitoreo y Revisión de ISMS). Valorar y donde aplicar, medir el cumplimiento de los procesos a través de las políticas de seguridad, objetivos y experiencias prácticas y reporte de resultados de administración por revisiones. (Bsi, 2003).

Act (Mantenimiento y mejora de ISMS). Tomar acciones preventivas y correctivas, basadas en los resultados del manejo de revisiones, para lograr mejoras continuas del ISMS. (Bsi, 2003).

Según el Estándar Británico BS7799, los tres aspectos más importantes que la seguridad de información debe tener, son: (Bsi, 2003).

- *Confidencialidad*: Asegurar que la información es accesible solo por personas que tengan acceso autorizado.
- *Integridad*: Salvaguardar la precisión y la totalidad de la información y métodos de procesamiento.
- *Disponibilidad*: Asegurarse que usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.

BS7799-2 es un estándar de administración para la seguridad de los bienes de información de una organización. (Tss, 2002).

En conclusión BS7799 es una guía para cualquier organización que quiera mantener un alto estándar de seguridad en sus procesos de información. (Tss, 2002).

CAPITULO 3

PROPUESTA DE MODELO DE ADMINISTRACIÓN DE SEGURIDAD DE INFORMACIÓN PARA REDES INALAMBRICAS MOVILES BASADO EN EL ESTANDAR DE SEGURIDAD BS7799

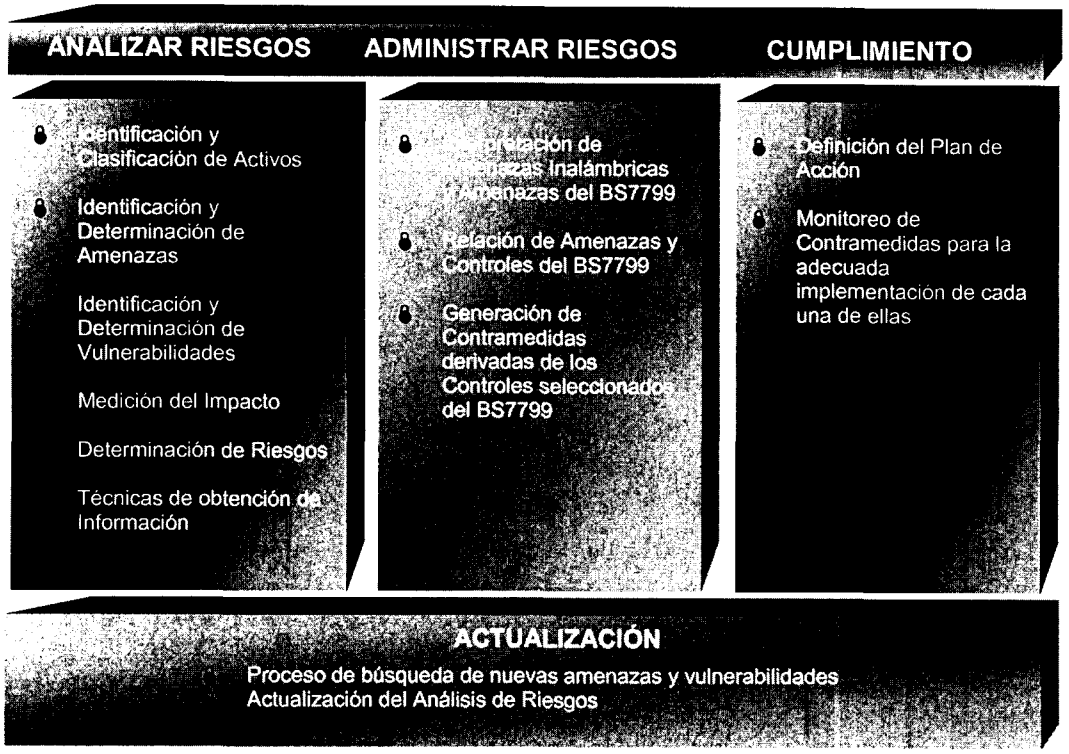

Figura 19.- Modelo de Seguridad para Redes Inalámbricas Móviles

Este modelo provee una guía dirigida a personas conocedoras encargadas de la seguridad de la información en las organizaciones, independientemente si forman parte del sector privado o gubernamental, así como para personas con poca experiencia en el área de seguridad.

Su uso debe en cierta forma motivar a sus destinatarios a involucrarse en la comprensión, implantación o mantenimiento de las condiciones de seguridad de información dentro de sus organizaciones.

A causa de la existencia de una gran cantidad de estándares y tecnologías inalámbricas, se decidió reducir el alcance de este modelo a las tecnologías inalámbricas de Wi-Fi, GSM, WAP, GPRS y MOBILE IP las cuales se encuentran en un proceso de adopción creciente día con día. Considerando también los principales dispositivos móviles de mayor aceptación en la actualidad en las empresas, hogares y en instituciones educativas como son computadoras Laptop, Handheld, Palm/Pocket y Teléfonos Inalámbricos que incluyen el protocolo WAP para poder acceder a Internet.
La Seguridad de Información no es una actividad, es una cultura, por lo cual se convierte en una acción permanente, cíclica y recurrente debido a los cambios del sistema y su entorno.

El modelo propuesto comprende cuatro fases, en las cuales cada una es resultado de la anterior y se considera una entrada de la siguiente, generando así un ciclo constante de regeneración. Estas fases son el producto del estudio del estándar BS7799 y de los principales factores que se deben incluir en un análisis de Seguridad de Información.

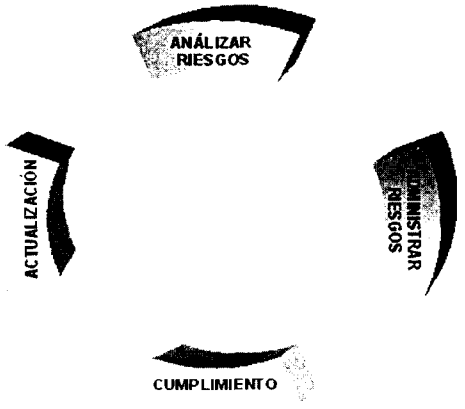

Figura 20.- Fases del Modelo de Administración de Seguridad de Información para Redes Inalámbricas Móviles

Algo que es muy importante mencionar, es la utilización de técnicas matriciales en cada una de las etapas que comprende el modelo de seguridad, esto facilitara su aplicación y contribuirá a una mejor organización de la información generada, facilitando de esta forma su manejo y entendimiento.

3.1.- ANÁLIZAR RIESGOS

El Análisis de Riesgos es la primera fase del modelo propuesto de administración de seguridad, y es definido como la oportunidad o probabilidad de que una amenaza dada haga uso de una vulnerabilidad potencial particular, y el impacto resultante de este evento adverso. Esto es una función de dos componentes separadas, la *probabilidad* de que un incidente no deseado ocurra y el *impacto* resultante del incidente.

La fase propuesta de análisis de riesgos comprende cinco entidades básicas siguientes:

Paso 1 – Identificación y Clasificación de Activos

Paso 2 – Identificación y Determinación de Amenazas

Paso 3 – Identificación y Determinación de Vulnerabilidades

Paso 4 – Medición de Impactos

Paso 5 – Determinación de Riesgos

3.1.1.- IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS

En esta etapa se propone una clasificación de activos en los sistemas de información y/o redes de comunicaciones, la cual consiste en tres categorías, considerando adicionalmente dos factores muy importantes que pueden influir en las medidas de seguridad a tomar:

Activos de Información o Datos: Se consideran como una colección de datos que deberán ser considerados para los propósitos de valuación de datos. La valuación se realiza en términos de impacto de negocios. Son procesados por un activo de aplicación de software y soportados por un activo físico.

Activos de Software: Se definen como una aplicación la cual manipula y/o almacena información. Es usado para cubrir aplicaciones específicas. No hay necesidad de especificar el sistema definido, interconexión o software de BD.

Activos Físicos: Es usado para cubrir todos los componentes de un sistema de información que no pueden ser clasificados como activos de datos, servicio de usuario final o activos de aplicación de software.

Funcionalidades de la Organización: Se consideran los objetivos y misión de la organización, bienes y servicios producidos, personal usuario y/o destinatario de los bienes o servicios producidos.

Identificación de Ubicación: Ciertos tipos de activos físicos pueden ser considerados para residir en una ubicación particular, por ejemplo host servers, gateways, workstations. Esto permite considerar ciertas amenazas contra la localización.

El resultado que se desea obtener de este paso es una caracterización, una fotografía completa y un establecimiento de los límites del sistema, aplicación, solución y/o servicio analizado.

Nombre Activo	Características	Funciones	Tipo	Ubicación	Usuarios
Access Point Aironet CISCO	Aironet 2500 cisco	Proveer de acceso a internet a los clientes	Físico	Sala de Espera	Clientes Usuarios Administradores
Acces Point Orinoco	Orinoco RG-1000	Proveer de acceso a internet a los clientes	Físico	Sala de Restaurante	Clientes Usuarios Administradores
Celular Nokia 6210		Acceso a variedad de servicios móviles a través de internet	Físico	Personal móvil	Cliente

Tabla 2.- Matriz de Activos de Información

3.1.2.- IDENTIFICACIÓN Y DETERMINACIÓN DE AMENAZAS INALÁMBRICAS

Identificación y Determinación de Amenazas: Implica la identificación y determinación del nivel de amenaza para los activos de un sistema. La amenaza es un evento de tipo potencial y puede considerarse como una acción, interrupción o falta de acción situada fuera del control de los actores de seguridad.

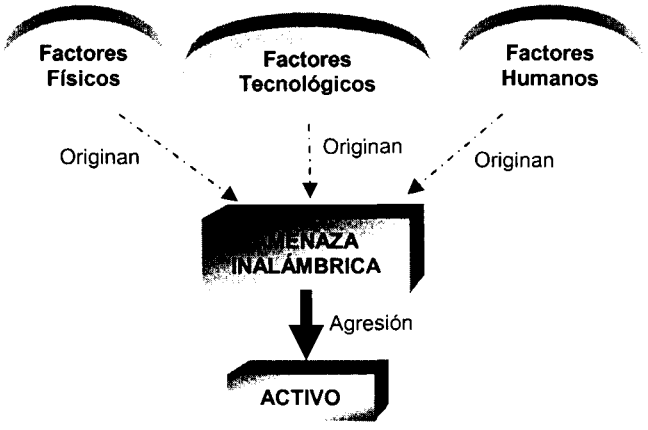

Figura 21.- Interpretación de Generación de Amenazas Inalámbricas

Las amenazas típicas incluyen:

- Ataques deliberados como hacking, spoofing, inserción de mensajes falsos, introducción de software dañino o disruptivo, robo, daño intencionado.
- Desastres como fuego, inundación, etc.
- Errores por personas
- Fallas técnicas

Para poder tener una valoración de cada una de las amenazas y poder así determinar el nivel de riesgo más adelante, es necesario establecer métricas de medición, en la tabla 3 se hace referencia a la siguiente escala:

Periodo de tiempo	Escala de valor de frecuencia
Menor que una vez por semana	Muy alta
Menor que un vez cada cuatro meses	Alta
Menor que un año	Media
Menor que tres años	Baja
Mayor que tres años	Muy baja

Tabla 3.- Métricas de Valuación de Amenazas

Una amenaza no puede hacerse presente cuando no existe alguna vulnerabilidad que la pueda ejercer. El nivel de amenaza es una medida de probabilidad de que un ataque o incidente ocurra.

La matriz de amenazas resultante de esta etapa del modelo se mencionada en la tabla 4 es para poder lograr un mejor entendimiento del proceso:

Activo	Amenaza	Factores de Seguridad			Daños	Nivel de Amenaza
		Disponibilidad	Integridad	Confidencialidad		
Access Point Aironet CISCO	Eavesdropping (Intercepción del tráfico de la red)		X	X		Media
Orinoco RG-1000 Web	Obtención de SSID (captura del SSID para conectarse a un AP)			X		Media
Celular Nokia 6210	Clonación de SIM		X	X		Muy Alta

Tabla 4.- Matriz Resultante de Identificación y Selección de Amenazas

El resultado esperado de este paso es la generación de una lista de amenazas asociadas con las vulnerabilidades del sistema, aplicación, solución y/o servicio analizado que pudieran explotar.

3.1.3.- IDENTIFICACIÓN Y DETERMINACIÓN DE VULNERABILIDADES INALÁMBRICAS

Se requiere de la identificación y determinación de la extensión por la cual los activos son vulnerados para la identificación de amenazas. La vulnerabilidad es una medida de debilidad inherente dentro del sistema o red. Implica considerar cada una en conjunción con la amenaza posible que pueda explotarla.

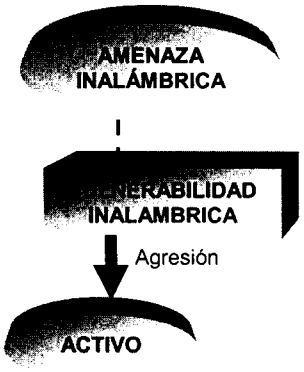

Figura 22.- Interpretación gráfica de una Vulnerabilidad

Algunas fuentes de vulnerabilidades que deben considerarse para un análisis completo y detallado incluyen, pero no se limitan a las siguientes:

- Documentación de Análisis de riesgos previos de sistemas de tecnología de información.
- Listas de vulnerabilidades, como la base de datos del NIST I-CAT, CERT.
- Equipos comerciales de respuesta a incidentes.
- Alertas de Vulnerabilidades para determinada información y boletines de sistemas militares.
- Software de Análisis de seguridad.

Para poder tener una valoración de cada una de las vulnerabilidades y poder así determinar el nivel de riesgo más adelante, es necesario establecer métricas de medición, en este caso se hace referencia a la siguiente escala:

Periodo de tiempo	Escala de valor de frecuencia
Menos de una vez por semana	Muy alta
Menos de un vez cada cuatro meses	Alta
Menor que un año	Media
Menor que tres años	Baja
Mayor que tres años	Muy baja

Tabla 5.- Métricas de valuación de Vulnerabilidades

Tomando en cuenta que una amenaza necesita explotar una vulnerabilidad existente para poder atacar un sistema, es necesario poder identificar las vulnerabilidades que la red, sistema, servicio y/o solución pudiera tener.

La matriz de vulnerabilidades resultante de esta etapa del modelo se menciona a continuación para poder lograr un mejor entendimiento del proceso:

Activo	Amenaza	Vulnerabilidad	Factores de Seguridad			Nivel de Vulnerabilidad
			Disponibilidad	Integridad	Confidencialidad	
Access Point Aironet CISCO	Eavesdropping	Disponibilidad de los paquetes en el medio	X		X	Media
Orinoco RG-1000 Web	Obtención de SSID	El Access Point hace un broadcast del SSID		X		Media
Celular Nokia 6210	Clonación de SIM	Debido a la variedad de usos, el SIM es menos seguro, ya que utiliza el algoritmo COMP128 para A3/A8 el cual tiene defectos		X	X	Alta

Tabla 6.- Matriz Resultante de Identificación y Determinación de Vulnerabilidades

El resultado deseado de este paso es la obtención de una lista de las vulnerabilidades del sistema, aplicación, solución y/o servicio analizado que pudieran ser explotadas por alguna amenaza o grupo de amenazas.

3.1.4.- MEDICIÓN DEL IMPACTO

Todos los activos tienen un valor para la organización y pueden ser medidos en términos del impacto que pueden tener si la confidencialidad, integridad o disponibilidad de los activos fuera comprometida.

El impacto puede ser definido como la consecuencia de la materialización de una amenaza en un activo, es decir, el impacto es la diferencia entre el antes y después de la materialización de una amenaza, como se muestra en la siguiente figura.

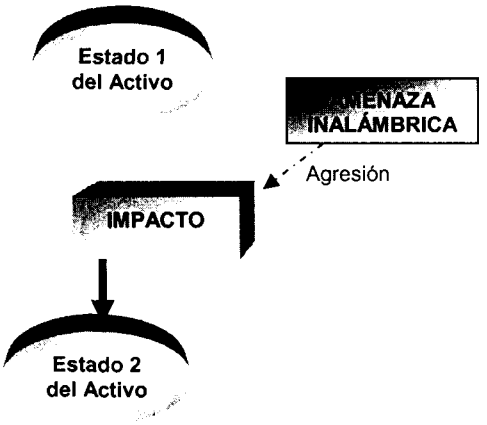

Figura 23.- Interpretación gráfica de un Impacto

El proceso propuesto de valoración de activos mide el impacto que resultara si se presentan algunos de los eventos que a continuación se mencionan sin limitarse a estos:

- Los activos de datos fueran revelados, modificados, destruidos o indisponibles de forma no autorizada o inesperada.
- Los activos físicos fueran dañados o destruidos
- Los activos de software fueran dañados, destruidos, corrompidos o, en el caso de software sensitivo, descubiertos de una forma no autorizada.

La valuación de los diferentes activos que forman parte de la red, sistema, servicio y/o solución a analizar esta relacionada con los factores de *Indisponibilidad, Destrucción, Divulgación y Modificación*. La escala de valuación puede variar de una organización a otra, ya que ninguna maneja el mismo presupuesto y el grado de impacto es variante, por lo cual se tratara de establecer una guía que pueda determinar una escala particular mas apegada a las necesidades de cada organización.

En la siguiente tabla se ilustra un rango de valoración en dólares que determina el nivel de impacto, estos valores están asociados al costo de reposición de la funcionalidad realizada por el activo afectado.

Rango de Valores	Nivel de Impacto
Menor que 1000 dlls	Muy Bajo
Menor que 10,000 dlls	Bajo
Menor que 100,000 dlls	Medio
Menor que 1,000,000 dlls	Alto
Mayor que 1,000,000 dlls	Muy Alto

Tabla 7.- Métricas para la Medición de Impactos

La matriz de impactos resultante de esta etapa del modelo se menciona a continuación para poder lograr un mejor entendimiento del proceso:

Amenaza	Activo	Nivel Activo	Nivel de Vulnerabilidad	Impacto
Eavesdropping (Intercepción del tráfico de la red)	Access Point Aironet CISCO	Alto	Medio	Alto
Obtención de SSID (captura del SSID para conectarse a un AP)	Orinoco RG-1000 Web	Medio	Medio	Medio
Clonación de SIM (Subscriber Identity Module)	Celular Nokia 6210	Medio	Alto	Alto

Tabla 8.- Matriz Resultante de la Medición de Impactos

El resultado esperado es la determinación del nivel de impacto en cada uno de los activos a través de métodos de cuantificación que involucren los principales factores de seguridad.

3.1.5.- DETERMINACIÓN DE RIESGOS

Implica la medición del nivel de riesgo para la red, sistema, servicio y/o solución. El nivel de riesgo es identificado por el valor de los activos, el nivel de amenaza y la extensión de la vulnerabilidad. Si existe una alta valuación de activos, el nivel de amenaza es alto, y significa que existen vulnerabilidades, entonces el riesgo de seguridad para los negocios es considerado por ser alto.

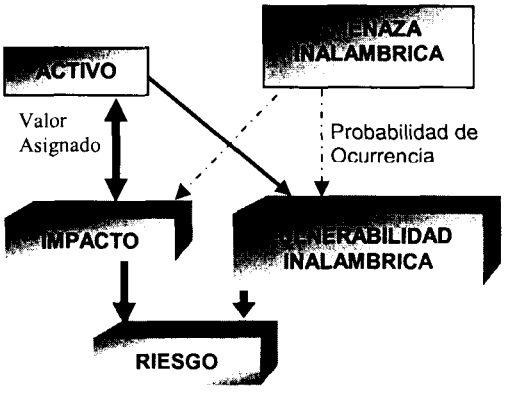

Figura 24.- Proceso de obtención del nivel de Riesgo

Las medidas de riesgo son calculadas en una escala de 1 a 5 usando una matriz de riesgos, donde 1 indica un requerimiento de seguridad de nivel muy bajo y 5 indica un requerimiento de seguridad muy alto.

Para lograr esto es necesario considerar tres factores muy importantes como lo son: impacto, la probabilidad de ocurrencia y el nivel de cada amenaza.

La probabilidad de ocurrencia esta determinado por la vulnerabilidad, el impacto esta relacionado con el valor monetario determinado por la materialización de la amenaza y la valuación del activo realizada anteriormente, y el nivel de amenaza es el determinado en la matriz de amenazas, la combinación de estos tres factores muestran el riesgo de cada una de las amenazas para cada activo.
La matriz de riesgo resultante de esta etapa del modelo se menciona a continuación para poder lograr un mejor entendimiento del proceso:

Activo	Amenaza	Nivel Amenaza	Probabilidad de Ocurrencia	Impacto	Riesgo
Access Point Aironet CISCO	Eavesdropping (Intercepción del tráfico de la red)	Media	Media	Alto	Alto
Orinoco RG-1000 Web	Obtención de SSID (captura del SSID para conectarse a un AP)	Media	Media	Medio	Medio
Celular Nokia 6210	Clonación de SIM (Subscriber Identity Module)	Alta	Muy Alta	Alto	Muy Alto

Tabla 9.- Matriz Resultante de la Determinación de Riesgos

El resultado de esta etapa repercutirá en el proceso de implementación de los controles de seguridad relacionados con las amenazas identificadas, lo cual estará dado por el nivel de riesgo de cada una de ellas.

3.1.6.- TECNICAS DE OBTENCIÓN DE INFORMACIÓN

A continuación se mencionan algunas técnicas importantes que pueden ser utilizadas para obtener información relevante de los sistemas de tecnologías de información:

Cuestionarios: se pueden desarrollar cuestionarios para poder obtener información relevante concerniente a la administración y controles operacionales planeados o usados por los sistemas de tecnologías de información.

Entrevistas en Sitio: las entrevistas con el personal de soporte y administración pueden posibilitar al personal encargado de la determinación de riesgos colectar información útil acerca de los sistemas de tecnologías de información.

Revisión de Documentos: documentos de políticas, documentación de sistemas y documentación relacionada con seguridad pueden proveer buena información acerca de los controles de seguridad usados por y planeados para los sistemas de seguridad de información.

Uso de Herramientas de Escaneo Automático: se pueden usar métodos técnicos proactivos para colectar información eficientemente.

3.2.- ADMINISTRAR RIESGOS

Implica la identificación, selección y adopción justificada de seguridad y las contramedidas de contingencia para mitigar o reducir el riesgo al mínimo nivel de impacto.

Las contramedidas pueden actuar de forma diferente como:

- La reducción de la probabilidad de ataques u ocurrencia de incidentes
- La reducción de las vulnerabilidades de sistemas
- La reducción del impacto de un ataque o incidente debiera ocurrir
- La detección de la ocurrencia de ataques o incidentes
- La facilidad de recuperación de un ataque o incidente.

3.2.1.- INTERPRETACIÓN DE AMENAZAS INALÁMBRICAS A AMENAZAS DEL BS7799

La etapa de interpretación es una de las más importantes en el modelo de seguridad, ya que la correcta definición de las amenazas identificadas y su posterior y correcta relación con las amenazas definidas por el BS7799 es muy importante, porque de este modo se lograra conservar el mapeo o relación con cada uno de los controles de seguridad del estándar británico.

Esta interpretación permitirá seleccionar los controles de seguridad adecuados para poder mitigar los riesgos identificados en los diferentes activos qué conforman la red, sistema, servicio y/o solución inalámbrica que se esta analizando.

Para esta etapa se utiliza un proceso de interpretación de amenazas inalámbricas el cual es uno de los aspectos más importantes del modelo de seguridad propuesto, se describe a continuación:

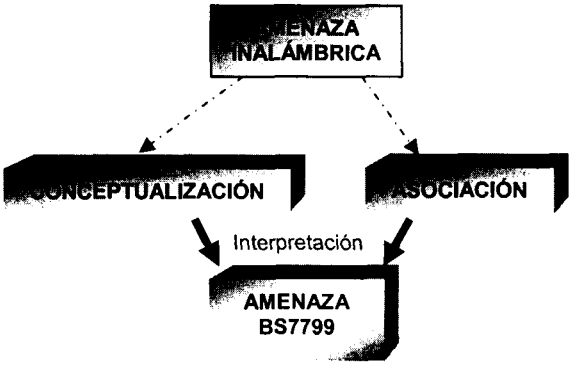

Figura 25.- Proceso de interpretación de amenazas inalámbricas

Conceptualización de Amenazas: Involucra la definición de cada una de las amenazas identificadas relacionadas con tecnología inalámbrica, para poder tener un mejor entendimiento de ellas.

Uno de los puntos muy importantes es lograr un mejor entendimiento de las amenazas y vulnerabilidades identificadas en el análisis de seguridad realizado, por lo cual es fundamental lograr una conceptualización de estas.

Asociación: Cada tecnología tiene características particulares en cuanto a funcionalidad, pero también se encuentran similitudes con otras, tal es el caso de la tecnología inalámbrica. A causa de esto es preciso realizar una asociación adecuada de las amenazas identificadas con factores meramente inalámbricos y las amenazas definidas por el BS7799.

La tecnología inalámbrica a tenido un periodo de vida corto en relación con la tecnología alámbrica, por lo cual la mayoría de las amenazas y vulnerabilidades están dirigidas a las tecnologías utilizadas en redes alámbricas, esto hace necesario la creación de un proceso que garantice una asociación o interpretación adecuada hacia las tecnologías inalámbricas con la finalidad de poder tomar una solución apegada a este tipo de tecnología. Es por esto que esta etapa es una de las más importantes en el modelo de seguridad propuesto.

El resultado de esta etapa es una lista de las amenazas definidas por el BS7799, que posteriormente nos permitirá lograr una correcta relación con los controles de seguridad del estándar británico.

Amenaza Inalámbrica	Amenaza BS7799	Nivel de Impacto
Eavesdropping (Intercepción del tráfico de la red)	3.2.2.- Inability to provide evidence (e.g. due to lack of monitoring) 3.6.3.- Unauthorized modification or destruction of information 3.10.6.- Interception and eavesdropping 3.11.1.- Risk from mobile computing 3.11.2 Risk from teleworking	Medio
Obtención de SSID (captura del SSID para conectarse a un AP)	3.4.2.- Misuse of information processing facilities 3.5.1. –Unauthorized of or changes to software 3.6.2.- Disclosure of confidential information 3.6.8.- Unauthorized access to network and network services 3.9.8.- Denial of Services 3.9.9.- Loss of service 3.11.1.- Risk from mobile computing	Medio
Clonación de SIM (Short Message Service)	3.5.1. –Unauthorized of or changes to software 3.6.2.- Disclosure of confidential information 3.11.1.- Risk from mobile computing	Alto

Tabla 10.- Matriz de Relación de Amenazas Inalámbricas con Amenazas del BS7799

3.2.2.- RELACIÓN ENTRE AMENAZAS Y CONTROLES DEL BS7799

Esta etapa comprende la selección de los controles de seguridad adecuados para poder tomar y/o crear las contramedidas que puedan mitigar o reducir al nivel mínimo el nivel de riesgo de cada una de las amenazas identificadas en etapas anteriores, estos controles de seguridad son tomados del estándar británico BS7799.

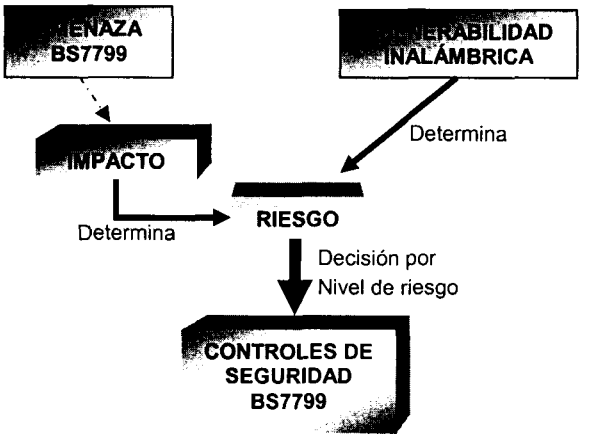

Figura 26.- Proceso de Selección de Controles de Seguridad BS7799

Los controles de seguridad deberán ser seleccionadas de acuerdo al nivel de riesgo calculado y además deben considerarse las diez partes esenciales para el Manejo de Seguridad de Información consideradas en el BS7799:

- *Políticas de Seguridad de Información*
- *Seguridad de Organización*
- *Clasificación y Control de Bienes*
- *Seguridad Personal*
- *Seguridad Física y Ambiental*
- *Administración de Comunicaciones y Operaciones*
- *Control de Acceso a los Sistemas*
- *Desarrollo y Mantenimiento de Sistemas*
- *Administración de la Continuidad de Negocios*
- *Cumplimiento*

El resultado de esta etapa es la generación de una lista de los controles de seguridad adecuados, los cuales deben ser los necesarios para poder generar más adelante las contramedidas que servirán para mitigar o reducir al nivel mas bajo el riesgo identificado.

Amenaza BS7799	Control de Seguridad BS7799	Prioridad
3.2.2.- Inability to provide evidence (e.g. due to lack of monitoring)	8.4.3.- Fault logging 8.1.3.- Incident management procedures 8.3.1.- Controls against malicious software 8.4.1.- Information back-up 9.2.1.- User registration 9.2.2.- Privilege management 9.2.3.- User password management	Media
3.3.2.- Damage from software malfunctions	6.3.3.- Reporting software malfunctions	Muy Alta
3.3.3.- System Failure (e.g. because of insufficient resources, system overload or corruption)	8.2.1.- Capacity planning 8.4.1.- Information back-up	Alta

Tabla 11.- Matriz de Relación de Amenazas y Controles del BS7799

3.2.3.- GENERACIÓN DE LAS CONTRAMEDIDAS DERIVADAS DE LOS CONTROLES SELECCIONADOS DEL BS7799

En esta etapa se materializan los controles seleccionados del BS7799 a través de la definición de las contramedidas a implementar para mitigar o reducir el nivel de riesgo de las amenazas relacionadas con los activos de la red, sistema, servicio y/o solución inalámbrica que se este analizando.

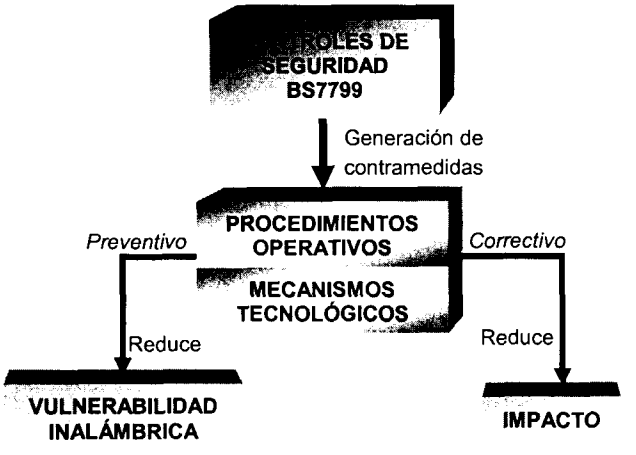

Figura 27.- Proceso de Generación de Contramedidas

Se identifican dos tipos de contramedidas para la mitigación del riesgo identificado, se mencionan a continuación:

- *Preventivas*: se refieren a los procedimientos operativos y/o mecanismos tecnológicos que permitirán actuar sobre las vulnerabilidades identificadas, antes de que se materialice alguna amenaza, reduciendo así su probabilidad de ocurrencia.

- *Correctivas*: se refieren a los procedimientos operativos y/o mecanismos tecnológicos que permitirán actuar sobre las amenazas que ya se materializaron, con la finalidad de reducir el nivel de impacto financiero, legal y/o de imagen provocado por esta materialización.

Se puede presentar el caso en que sin conocimiento alguno o sin tener conocimiento suficiente, se implementen medidas para poder prevenir la materialización de las amenazas, es por eso que se considera importante que en esta etapa se realice una revisión previa, consistente en revisar y/o validar el estatus de los controles (que fueron seleccionados en el proceso de Selección de Controles) para poder determinar si se encuentran implementados, parcialmente implementados o no implementados, lo cual servirá para poder determinar el costo de implementación de las contramedidas generadas.

Los costos generados por las contramedidas a implementar independientemente de que sean preventivas o correctivas, deben ser determinadas mediante un análisis costo-beneficio, ya que estos costos no deben ser muy grandes o mayores al costo de la implantación de la red, sistema, servicio y/o solución inalámbrica, esto es un factor muy importante a considerar en el proceso de análisis y que determinará la viabilidad del proyecto.

Es muy importante también que la implementación de estas contramedidas sea realizada por personal debidamente capacitado, para que de esta forma se garantice una correcta implementación y no generar situaciones adversas.

El resultado de esta etapa es la generación de una lista de contramedidas relacionadas con cada uno de los activos involucrados, estas nos permitirán cumplir con los controles de seguridad del BS7799 seleccionados y de esta forma poder mitigar el riesgo determinado.

Control BS7799	Actividades de Seguridad	Prioridad
6.3.3.- Reporting software malfunctions	Definición de proceso de comunicación entre las áreas involucradas. Definición de contactos hacia el proveedor para reportar falla	Muy Alto
8.1.3.- Incident management procedures	Desarrollar procedimientos de respuesta ante incidentes de seguridad de información más probables en la aplicación	Muy Alto
8.2.1.- Capacity planning	Definición de capacidad que contemple lo siguiente: Pronóstico, Número de clientes, Hits en el servidor, Tiempo de Respuesta, Utilización de Hardware (CPU, Memoria)	Alto
8.3.1.- Controls against malicious software	Desarrollo de procedimientos para prevención, detección y erradicación de programas malicioso que contemple la recepción de notificación de vulnerabilidades Utilización de Niveles recientes de Sistema Operativo, Conjunto de parches actualizado	Muy Alto

Tabla 12.- Matriz de Relación de Controles del BS7799 y Actividades de Seguridad

3.3.- CUMPLIMIENTO

3.3.1.- DEFINICIÓN DEL PLAN DE ACCIÓN

Después de haber clasificado los activos de la red, sistema, servicio y/o solución inalámbrica, después de haber identificado las vulnerabilidades y amenazas de seguridad, de haber realizado la valuación de los activos, determinado el impacto, e identificado el riesgo, después de haber definido todas y cada una de las contramedidas para poder cumplir con los requerimientos de seguridad, hay que realizar el proceso de implantación.

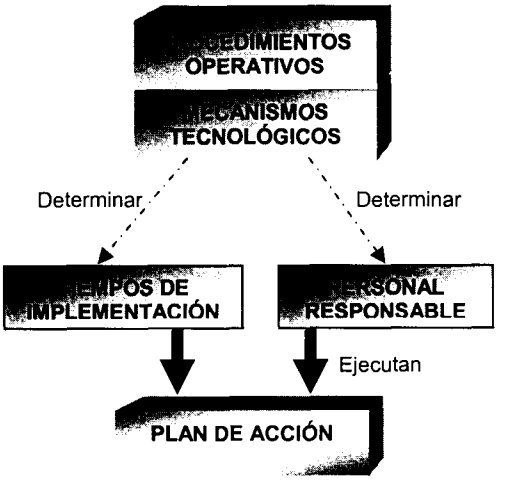

Figura 28.- Generación del Plan de Acción

En este proceso se crea un documento o plan de proyecto (Project Plan) el cual describe las actividades que hay que ejecutar para cumplir con cada uno de los controles de seguridad previamente seleccionados para cada activo de información. Aquí se definen el tiempo y el personal responsable para la implementación de cada una de las contramedidas.

Un punto muy importante que hay que determinar es la prioridad de implementación de las actividades o procesos de seguridad que se identificaron, esto se puede realizar tomando en cuenta el costo determinado en la etapa de *Medición de Impacto* de los activos analizados y el nivel de amenaza determinado en la etapa de *Identificación y Determinación de Amenazas*, con estas dos métricas se podrá decidir el orden de implementación de las contramedidas de seguridad, esto de acuerdo al costo y prioridad asignado.

Se debe contar con la participación del personal de cada una de las áreas involucradas de la compañía para poder garantizar la correcta implantación del modelo de seguridad definido.

Este es el paso mas importante dentro de todo el proceso de análisis del modelo de administración de seguridad para redes inalámbricas móviles, ya que es la culminación de todos los procesos anteriormente descritos, aquí es donde se materializa la solución o soluciones de seguridad construidas a través de este modelo propuesto.

ID	Actividad	Activo	Prioridad	Status	Controles Relacionados	Dueño	Personal de Apoyo	Tiempo	Fecha Inicio
1	Definir proceso de comunicación entre las áreas involucradas	Access Point Aironet CISCO		No implementado	6.3.3.- Reporting software malfunctions	TBD	TBD	4 semanas	TBD
2	Definir contactos hacia el proveedor para reportar falla	Teléfono Celular Nokia 6210		No implementado	6.3.3.- Reporting software malfunctions	TBD	TBD	1 semana	TBD
3	Desarrollar procedimientos de respuesta ante incidentes de seguridad de información más probables en la aplicación	Orinoco RG-1000		No implementado	8.1.3.- Incident management procedures	TBD	TBD	6 semanas	TBD

Tabla 13.- Matriz de Plan de Acción para cada una de las Actividades de Seguridad Definidas

3.3.2.- MONITOREO PARA LA ADECUADA IMPLEMENTACIÓN DE LAS CONTRAMEDIDAS DEFINIDAS

Se debe realizar un proceso de revisión (auditoria) y seguimiento para asegurarse de la implementación y uso adecuado de las contramedidas de seguridad creadas para los activos analizados, para este proceso se debe contar con acuerdos establecidos lo cual garantizara la participación de cada una de las áreas involucradas.

Esta etapa es la aplicación y continuación del Plan de Acción mencionado en la etapa anterior.

Es muy importante contar con un proceso de monitoreo para garantizar el cumplimiento de cada una de las contramedidas de seguridad, ya que no todas las contramedidas son de aplicación única, es decir, su ejecución se convierte en una actividad constante, por lo cual hay que tener un registro de su cumplimiento día a día.

Este proceso de monitoreo puede realizarse a través de la implementación de algún mecanismo tecnológico o de algún proceso manual permanente. Siempre dependiendo del presupuesto y disponibilidad de recursos de la empresa.

3.4.- ACTUALIZACIÓN

3.4.1.- PROCESO DE BUSQUEDA DE NUEVAS VULNERABILIDADES Y AMENAZAS INALÁMBRICAS

Una factor muy importante en el ambiente tecnológico y en la mayoría de las áreas del conocimiento humano es la tendencia a la evolución y mejora continua, entendiendo esto, podemos decir que la tecnología inalámbrica no es la excepción, ya que es una tecnología que actualmente esta pasando por un proceso de adaptación y adopción y aun no se conocen los alcances que tendrá en los próximos años.

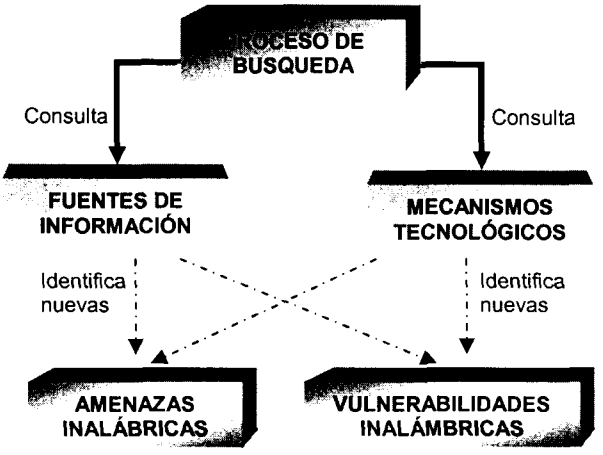

Figura 29.- Proceso de Búsqueda de Nuevas Amenazas y Vulnerabilidades Inalámbricas

Por esto y mas, se identifico la necesidad de crear un proceso de búsqueda enfocado a las vulnerabilidades y amenazas inalámbricas que surgen día a día, lo que permitirá contar con una perspectiva más acorde al comportamiento actual de las comunicaciones inalámbricas y nos permitirá considerar los requerimientos necesarios para poder realizar una actualización constante de nuestros modelos de seguridad, incluidos los mecanismos tecnológicos de seguridad y los procesos de seguridad definidos.

Esta búsqueda de nuevas vulnerabilidades y amenazas inalámbricas puede realizarse a través de:

- La utilización de mecanismos tecnológicos enfocados a la detección de vulnerabilidades
- La generación de convenios con empresas o instituciones dedicadas al área de seguridad informática y tecnológica como pudiese ser (Policía Cibernética, etc.)

- La consulta y utilización de listas generadas por organismos y empresas internacionales como CERT, SANS Institute, Symantec, etc.

- La generación de convenios o acuerdos con los proveedores de tecnología inalámbrica, los cuales deben tener la obligación de mantener una actualización constante de las nuevas vulnerabilidades y amenazas identificadas.

Todas estas fuentes de información nos permitirán conocer el mundo cambiante de la tecnología inalámbrica y poder así mantener en actualización constante nuestras tecnologías y sistemas inalámbricos.

3.4.2.- ACTUALIZACIÓN DEL MODELO DE SEGURIDAD

Como resultado del monitoreo de nuevas vulnerabilidades y amenazas inalámbricas, se produce la activación del proceso de actualización del modelo de seguridad.

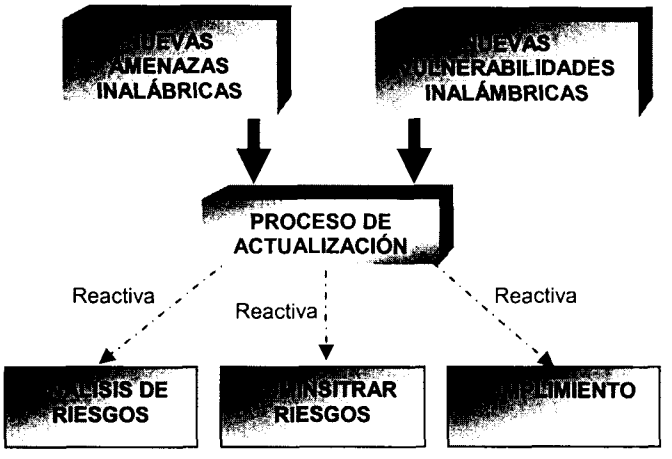

Figura 30.- Proceso de Actualización del Modelo de Seguridad

El objetivo de este proceso o etapa es la realización de las adecuaciones necesarias en las tecnologías inalámbricas implementadas con anterioridad.

Esto repercute en la adopción de nuevos controles de seguridad del BS7799 y la correspondiente generación de nuevas contramedidas o la adaptabilidad de las ya definidas lo que permitirá mantener el valor del análisis de riesgos.

Gracias a este proceso o etapa se lograra considerar las nuevas vulnerabilidades y amenazas inalámbricas identificadas, para poder garantizar la seguridad de la información de las tecnologías inalámbricas. Este proceso permitirá a la empresa mantener sus altos niveles de seguridad de información.

CAPITULO 4

ESTUDIO DE CAMPO

4.1.- MODELO PARTICULAR

Cuando el tamaño de las organizaciones crece, los riesgos de seguridad de las redes se incrementan, ya que cada vez se vuelve más difícil detectar y evitar posibles infiltraciones y detectar ataques que perjudiquen las operaciones del negocio.

¿Como podemos estar seguros de que tenemos cubiertas todas las áreas de seguridad en nuestras redes inalámbricas móviles y que nuestros métodos de seguridad son consistentes?.

Estudios muestran que una de cada cinco compañías de redes ha sido infiltrada por WLAN´s no autorizadas y tres de cada cuatro propietarios de Asistentes Personales Digitales (PDA) utilizan estos dispositivos para actividades de negocios. (BCR, 2003).

De acuerdo a un estudio realizado por TechRepublic, las fallas de sistema, infección de virus y corrupción/daño son las causas mas frecuentes del compromiso en los dispositivos móviles. (BCR, 2003).

La creación, generación y adopción de los procesos adecuados para garantizar la seguridad de la información es lo que hace valiosa la tecnología; una tecnología sin procesos es un simple fierro (router, switch, firewall, etc.) que ocupa espacio en nuestras instalaciones de comunicación.

El propósito de esta investigación es crear o servir de punto de partida para generar un modelo de administración de seguridad de información para redes inalámbricas móviles, dadas las circunstancias que se han presentado en los últimos años y a las tendencias que se esperan de estas tecnologías en los años venideros.

El estándar de seguridad BS7799 es el elegido como la base para este modelo propuesto, por ser uno de los mejores, sino el mejor a nivel mundial, el cual tiene una muy amplia cobertura en el área de seguridad de información.

El proceso de creación del modelo propuesto a desarrollar es el siguiente:

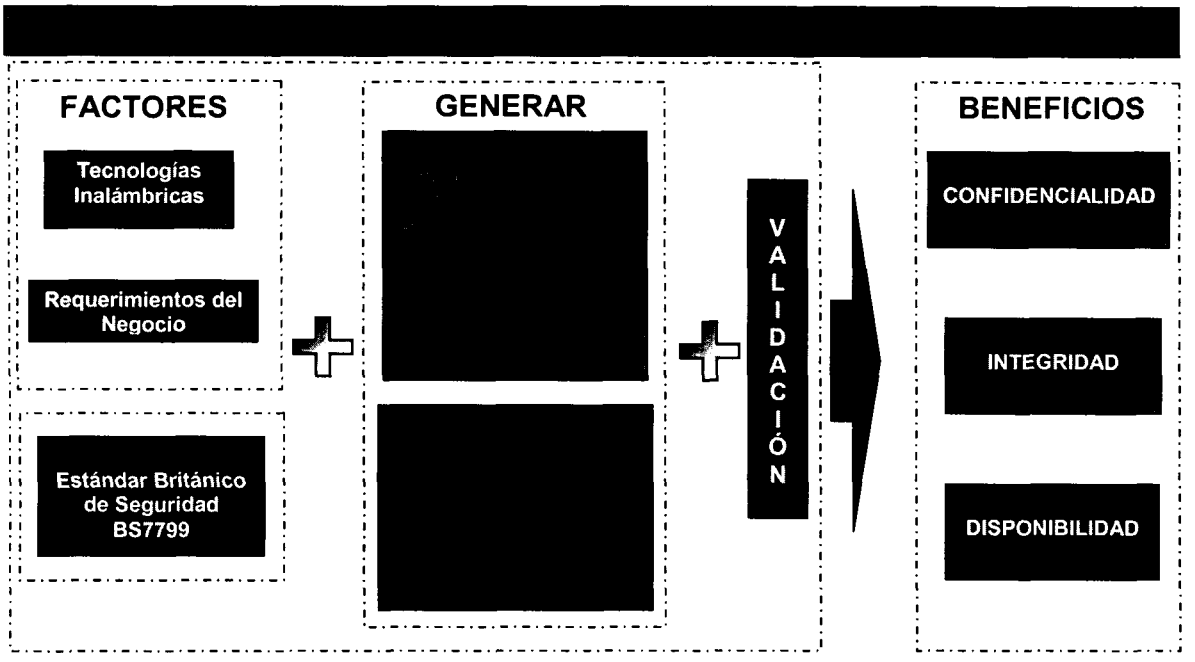

Figura 31.- Proceso de creación del Modelo de Administración de Seguridad de Información

Para poder generar el modelo propuesto de Administración de Seguridad de Información en una Red Inalámbrica Móvil, se tomaran en consideración dos aspectos importantes los cuales son Tecnologías Inalámbricas y los requerimientos del negocio.

Los Factores a considerar en las tecnologías inalámbricas móviles son los siguientes:

1.- Tipo de Tecnología Inalámbrica
- Configuración
- Servicios capaz de proveer
- Rangos de alcance
- Calidad de Servicio
- Costo
- Cumplimiento de los estándares IEEE 802.1x

El estándar de seguridad que servirá como base para generar el modelo es:

2.- British Standard BS-7799

La Generación del Modelo propuesto de Administración de Seguridad de Información para Redes Inalámbricas Móviles basado en BS7799 consiste en:

- *Servicios inalámbricos requeridos por la empresa*: Definir y/o identificar los diferentes servicios para el transporte de información que se desean ofrecer al hacer uso de redes inalámbricas.
- *Rango de Distancia adecuado de los servicios*: Determinar el rango de distancia que abarcara la red inalámbrica para la adecuada operación de sus servicios.
- *Tipo de protocolos de información*: Identificar el o los protocolos utilizados para el transporte y aseguramiento de la información en las redes inalámbricas.
- *Características de configuración de la WLAN*: Definir o Identificar el tipo de topología mas adecuado para la implantación de la red inalámbrica, y la forma de operar en sus diferentes nodos.
- *Riesgos*: Identificar los riesgos más importantes y que pueden afectar de manera trascendental a las empresas que hacen uso de redes inalámbricas.
- *Amenazas y Vulnerabilidades*: Identificar los diferentes tipos de amenazas y vulnerabilidades a las cuales están expuestas las redes inalámbricas, para garantizar su operación y protección adecuada.
- *Clasificación de la información*: Definir el tipo de información que se desea transportar en las redes inalámbricas, para poder determinar el grado de riesgo que la empresa tiene al hacer uso de este tipo de redes y tener un mejor control en el manejo de la información.
- *Identificar Procesos de Información*: Identificar los procesos de información más importantes para poder tener un mejor control del uso de la información en las redes inalámbricas.
- *Políticas y Directrices, para el uso de Información*: Definir Políticas y Directrices para asignar responsabilidades del uso de la información que se considera importante para la empresa, y definir quienes van a ser los responsables de ejecutar esas políticas para asegurar que la información esta debidamente protegida.
- *Concientización, Difusión, Capacitación*: Desarrollar procedimientos para poder lograr involucrar al personal requerido para el cumplimiento de las actividades derivadas de los controles de seguridad identificados. Desarrollar actividades para difundir la importancia que tiene la implementación adecuada de la seguridad de información. Capacitar al personal responsable del cumplimiento de la seguridad de información.

El Proceso de Evaluación y/o Implantación adecuada consiste en:

- Evaluar y/o Implantar el modelo de seguridad en empresas de Telecomunicaciones o en las empresas que requieren este tipo de servicios, para determinar el grado de cumplimiento, determinar el grado de afectación por la falta de modelos de seguridad orientados a tecnologías inalámbricas, para que de esta forma se genere una nueva propuesta de implantación.

El objetivo de este modelo es que exista una guía que aclare las dudas de cualquier empresa de cómo poder implementar las medidas de seguridad de información necesarias en una red inalámbrica móvil, cumpliendo con los más altos niveles de seguridad. Especificando los factores y el estándar necesario, y los riesgos y amenazas que implica el no tener un modelo de seguridad adecuado.

4.2.- HIPÓTESIS

H1. La clasificación de la información basada en BS7799 reduce los riesgos y amenazas que la información tiene en las empresas al hacer uso de las tecnologías de información y telecomunicaciones y mantiene su confidencialidad e integridad.

H2. La identificación de los procesos de información más importantes al aplicar el estándar BS7799 en las empresas que utilizan la tecnología para procesar su información, ayuda a tener un mejor control del uso de la información.

H3. La implementación de Políticas y Directrices basadas en el estándar BS7799, definen el uso adecuado de la información y determina quien tendrá la responsabilidad de la aplicación del modelo de seguridad.

H4. El uso de modelos de seguridad de información para tecnologías inalámbricas basados en el BS7799 garantiza un alto grado de confidencialidad, integridad y disponibilidad de la información en las empresas.

4.3.- MÉTODO DE INVESTIGACIÓN

4.3.1.- TIPO DE INVESTIGACIÓN

La investigación no experimental es la que se realiza sin manipular deliberadamente las variables, observa los fenómenos tal y como se dan en su contexto natural, para después analizarlos. (Hernández, 2003).

Analizar cual es el nivel, estado o la presencia de una o más variables en un momento dado, evaluar una situación, fenómeno o contexto en un punto del tiempo, son características que se apegan al tipo de investigación que se pretende realizar, por lo cual podemos decir que se trata de una investigación de diseño *transeccional*, y también se puede decir que es de tipo *exploratorio*, ya que en este tipo de investigación se comienza a conocer una comunidad, un contexto, un evento, una situación, una variable o un conjunto de variables, por lo general se aplican a problemas de investigación nuevos o poco conocidos.

4.3.2.- POBLACIÓN

La población esta comprendida por ejecutivos o especialistas de informática, telecomunicaciones y redes de empresas que tienen infraestructura inalámbrica y empresas que pretenden implementar este tipo de tecnología en Monterrey, Nuevo León.

Las categorías de computo móvil que se pretende comprenda el modelo de seguridad son computadoras Laptop, Handheld, Palm/Pocket y Teléfonos Inalámbricos que incluyen el protocolo WAP para poder acceder a Internet.

4.3.3.- TAMAÑO Y DISTRIBUCIÓN DE LA MUESTRA

La muestra es no probabilística porque la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace la muestra. (Hernández 2003).

La encuesta se realizo a una total de 32 personas especialistas o relacionadas con el área de seguridad de información en sus empresas, y administración y uso de tecnologías inalámbricas, lo cual permite tener un panorama mas apegado de lo que es el estado de la seguridad en las tecnologías inalámbricas.

No esta de mas mencionar que al ser una encuesta dirigida a personas consideradas con un nivel experiencia alto en la materia, así como a altos directivos, es difícil poder obtener información relacionada con la investigación, la cual al referirse a un tema tan importante como es la seguridad de información se encuentra mucha resistencia a la participación, ya que influye en reflejar el estado de la seguridad de la información en las empresas participantes, por lo cual como petición de los participantes se opto por omitir los nombres y se incluyo la siguiente leyenda:

"La información obtenida en esta encuesta estará dirigida a fines de investigación científica y no con fines de lucro. Con la finalidad de proteger la integridad de las personas participantes."

4.3.4.- VARIABLES

A continuación se describen cada una de las variables

Independiente: La implantación de reglas y normas para garantizar la seguridad de la información, esta conformado por los factores de tecnología inalámbrica que se desea usar, y los aspectos más importantes del estándar británico de seguridad de información BS7799 que garantizan el establecimiento de mecanismos adecuados para lograr un alto grado de seguridad.

Dependiente: Proceso de evaluación y/o implantación adecuado, cuenta con todos los factores, recomendaciones y sugerencias, comparaciones con expertos o profesionales en el área de redes inalámbricas, y la implementación del estándar de seguridad de la información BS7799 haciendo de esta forma que la implantación de redes inalámbricas garantice niveles altos de confidencialidad, integridad y disponibilidad de la información de la empresa.

4.3.5.- ESTRATEGIA DE RECOLECCIÓN DE DATOS

Realizar cuestionarios y entrevistas a expertos en el área, acerca de los factores mas importantes que se deben tomar en cuenta en las empresas, y sobre los métodos y procedimientos de seguridad que se deben considerar para garantizar un alto nivel de seguridad de la información que viaja a través de las redes inalámbricas acorde con los estándares internacionales, en este caso el BS7799.

En las empresas que cuentan con modelos de seguridad enfocados a redes inalámbricas, identificar los aspectos más relevantes que han sido considerados para la identificación de las amenazas y vulnerabilidades mas importantes para que de esta forma se pueda calcular el riego y poder garantizar la seguridad de la información.

Para las empresas que aún no tienen algún modelo de seguridad, establecer los factores más importantes que deben considerar al implantar redes inalámbricas, para poder asegurar un alto nivel de protección de su información, considerando las amenazas y vulnerabilidades que pueden tener un mayor grado de impacto en la empresa.

4.3.6.- TRATAMIENTO DE LA INFORMACIÓN

Identificar los puntos débiles, las amenazas y los riesgos más comunes en las redes inalámbricas móviles de las empresas para poder determinar que tipo de directrices seguir y poder dar la mejor solución en seguridad.

Comparar los resultados obtenidos de empresas que ya cuentan con tecnologías inalámbricas y modelos de seguridad implementados para esas tecnologías. Determinar el grado de beneficio de estos modelos ya usados en caso de existir.

Comparar los resultados obtenidos de empresas que pretenden implantar tecnologías inalámbricas para el manejo de información, y de esta forma identificar los factores de vulnerabilidad y riesgo que van a enfrentar para proponer la implantación de un modelo de seguridad, siempre que sea rentable para la empresa.

4.4.- RESULTADOS

En esta sección se dan a conocer los resultados obtenidos a través de la estrategia de recolección de información descrita anteriormente, la cual pretende dar a conocer una perspectiva actual del estado que guarda la seguridad de información en redes inalámbricas móviles en el área de Monterrey, Nuevo León, y así poder lograr una validación apropiada de la creación de un modelo con las características propuestas anteriormente en los capítulos de esta tesis de maestría.

4.4.1.- ENCUESTA

El cuestionario es el instrumento más utilizado para la recolección de datos. Un cuestionario consiste en un conjunto de preguntas respecto a una o más variables a medir. (Hernandez, 2003).

La encuesta realizada para esta tesis se aplico de una forma auto administrada y enviando por correo electrónico el cuestionario correspondiente. Los respondientes contestan directamente los cuestionarios, ellos marcan las respuestas, no hay intermediario. (Hernandez, 2003).

La encuesta fue diseñada para obtener información relacionada con: el uso redes inalámbricas, métodos de seguridad de información, mecanismos tecnológicos de seguridad, información y servicios utilizados en este tipo de redes, y el factor económico relacionado con la implementación de la seguridad de información en las empresas.

La encuesta se aplicó en Monterrey, Nuevo León, principalmente a personas especialistas en el área de seguridad de información, así como a altos directivos de empresas de telecomunicaciones, consultorías, etc.

A continuación se mencionan los resultados obtenidos de la investigación realizada:

Un factor de mucha importancia es el interés que tienen las personas encargadas de la administración de TIC en las empresas, lo cual permite impulsar la adopción de políticas de seguridad de información y el establecimiento de un ambiente adecuado que permita garantizar la seguridad de la información, esto se puede ilustrar en la figura 30, obtenida de los resultados generados de la encuesta realizada.

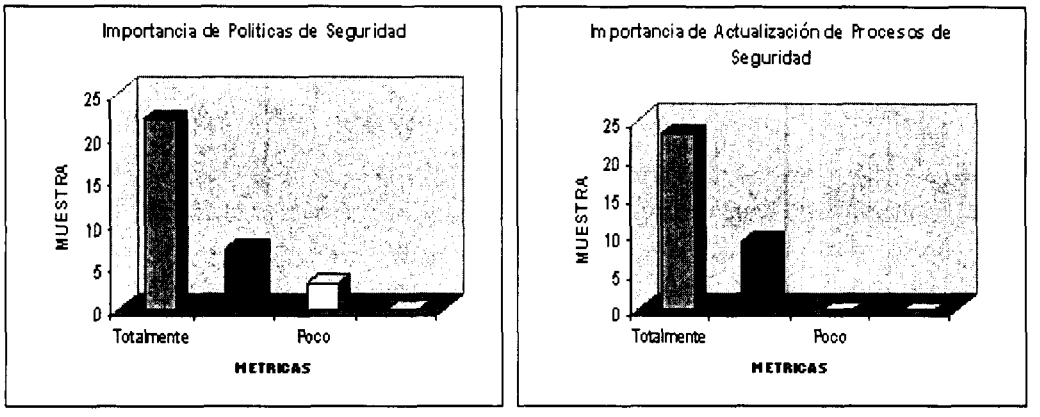

Figura 32.- Importancia de implementar y actualizar políticas y procesos de seguridad de información

En contradicción con el factor anterior se puede identificar la poca o nula adopción de una cultura orientada a la seguridad de información en la empresa, ya que como se menciono en capítulos anteriores en esta tesis, la Seguridad de Información no es una actividad, es una cultura, por lo cual se convierte en una acción permanente, cíclica y recurrente debido a los cambios del sistema y su entorno, así se muestra en la siguiente gráfica.

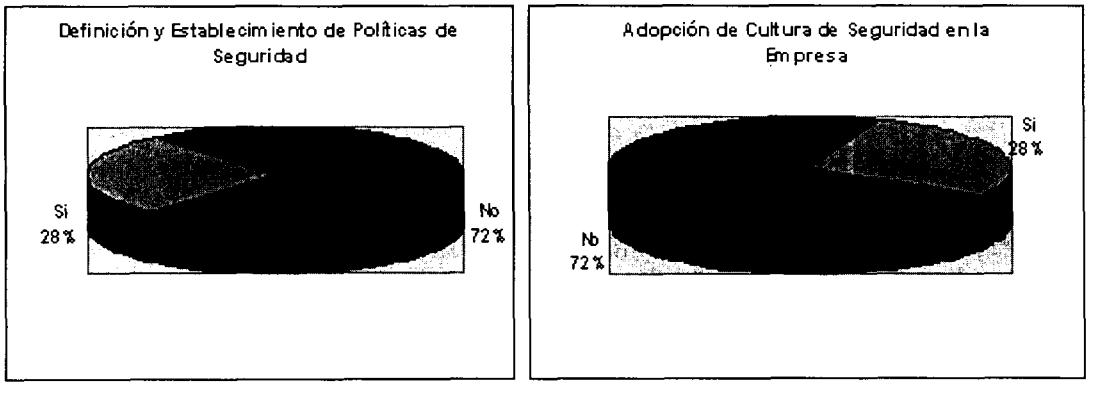

Figura 33.- Adopción de Políticas de Seguridad y Cultura de Seguridad

El constante cambio de la tecnología y los constantes incidentes registrados en el mundo de la información, ha creado la necesidad de la formación de equipos o grupos de personas encargadas de garantizar la seguridad de la información en las empresas, la cual se considera el más importante de los activos, antes o después de los recursos humanos. Para lograr el éxito de las funciones de estos grupos especializados, es necesario contar con la participación de los altos directivos de la empresa, lo cual permitirá permear esta cultura tan difícil y ardua de establecer. Es así como cada día podemos ver como esta área gana terreno permitiéndonos suponer un mayor crecimiento en los próximos años.

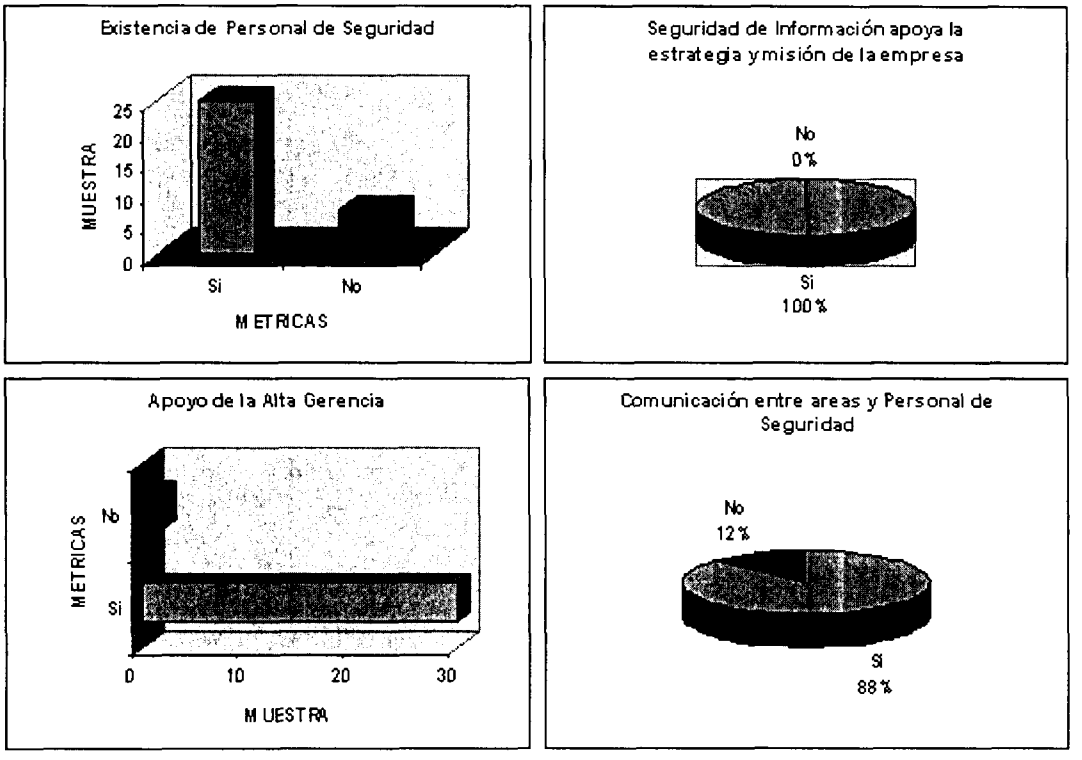

Figura 34.- Relación de la Creación de Grupos de Seguridad y el Apoyo de la Alta Gerencia a las Áreas de Seguridad

La siguiente información esta relacionada a la adopción y/o generación de alguna metodología o análisis riguroso para poder determinar los riesgos de seguridad de la información en los sistemas o dispositivos tecnológicos inalámbricos utilizados por las empresas, la utilización de estándares de seguridad y/o utilización de mecanismos tecnológicos que garanticen seguridad en las redes inalámbricas móviles de las empresas en Monterrey.

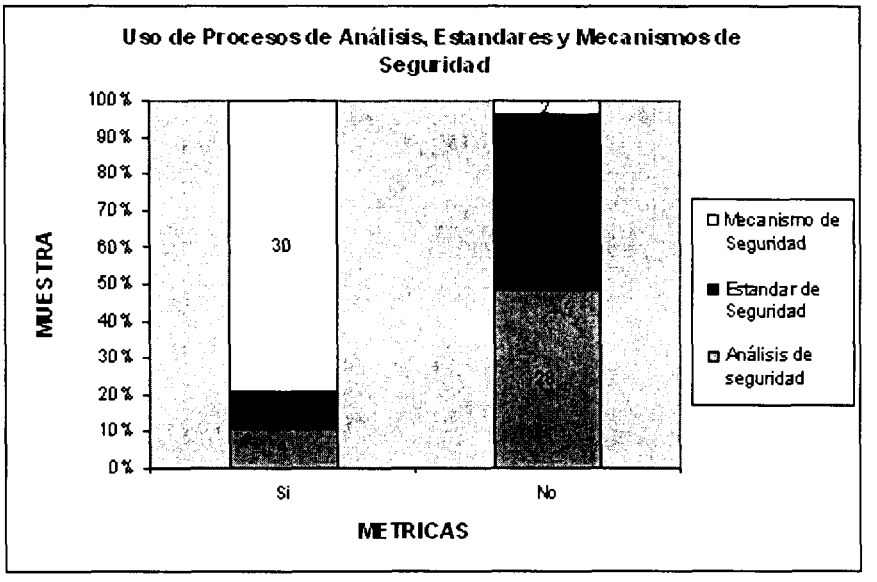

Figura 35.- Adopción o uso de Procesos de Análisis de Seguridad, Estándares y Mecanismos de Seguridad en las empresas encuestadas de Monterrey

Algunos de los mecanismos de seguridad utilizados para garantizar la seguridad de la información en algunas de las empresas encuestadas son: certificados para celular, PDA's así como para manejo de páginas WAP

Esto nos permite entender la importancia que tiene la seguridad de la información en las tecnologías inalámbricas, las cuales al ser de naturaleza diferente a las redes tradicionales (alámbricas) están expuestas a una gran variedad de amenazas.

Las tecnologías de información tienen una naturaleza cambiante, por lo cual siempre podremos ver nuevas formas de llevar la información de un lugar a otro, este es el caso de las tecnologías inalámbricas, las cuales nos ofrecen la ventaja o si se quiere ver como facilidad, de movernos de un lugar a otro y poder mantener una comunicación constante.

Así como la tecnología evoluciona, también existe una evolución constante de las amenazas y vulnerabilidades que pueden ser explotadas a través de diferentes medios, esto hace necesario contar con algún plan de contingencia que permita recuperarnos en caso de algún ataque informático y en complemento poder tener algún proceso de monitoreo capaz de detectar estos ataques. En la siguiente figura se puede ilustrar el grado de adopción de estas medidas en las diferentes empresas encuestadas en la ciudad de Monterrey.

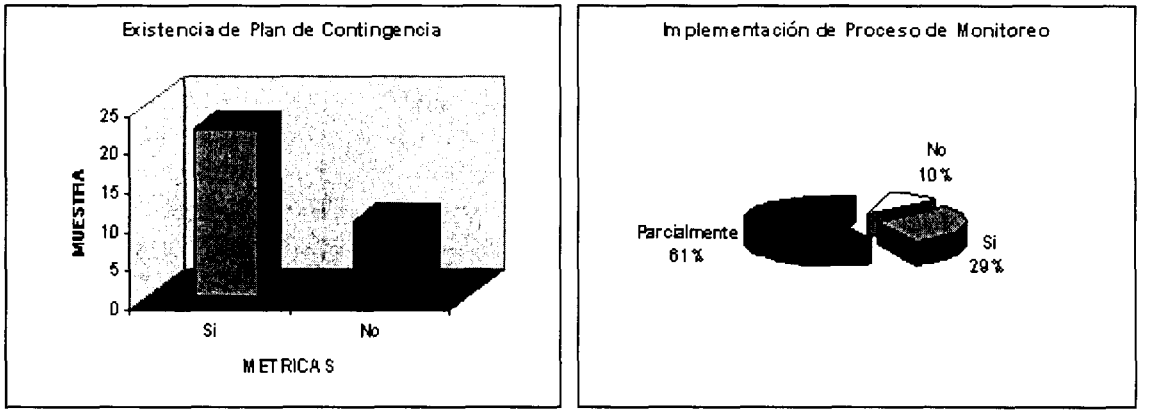

Figura 36.- Porcentaje de utilización de Procesos de Monitoreo y Planes de Contingencia

Se puede observar que existe una carencia en cuanto a la tramitación de certificados de seguridad, por lo cual podemos ver un gran campo de crecimiento y explotación. Las empresas encuestadas casi en su totalidad carecen de estos certificados.

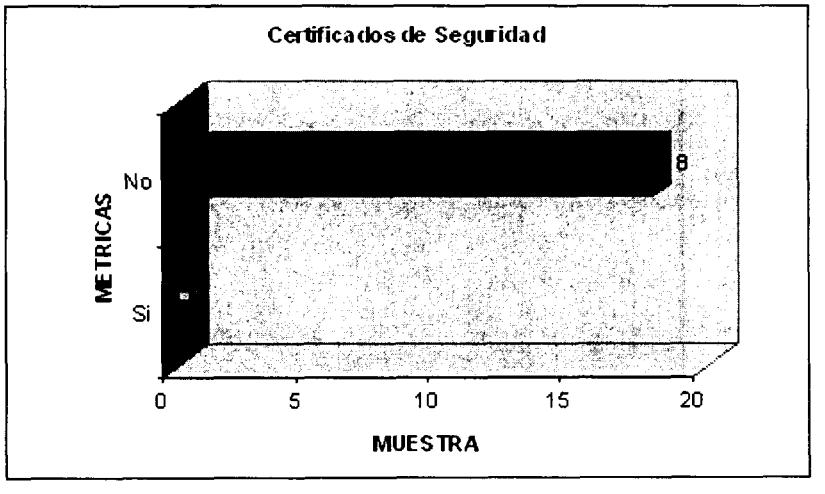

Figura 37.- Numero de Certificaciones de Seguridad de Información en las Empresas Encuestadas

De acuerdo con el resultado obtenido, se puede comprobar que la totalidad de las empresas encuestadas han sufrido algún intento de hackeo o un ataque en los últimos tres años, lo cual le da un mayor empuje a la adopción de medidas de seguridad en sus procesos y tecnologías usadas.

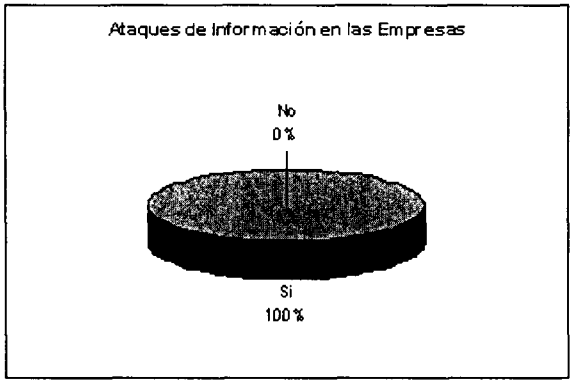

Figura 38.- La existencia de Ataques Informáticos en los últimos 3 años en las empresas de Monterrey

El uso de la tecnología inalámbrica en las empresas esta incrementándose, por lo cual, el grado de adopción y la variedad de usos para estas tecnologías también se ha incrementado. Como podemos ver, de acuerdo con los resultados obtenidos, el uso de equipos inalámbricos se hace presente en la totalidad de las empresas encuestadas.

Las actividades laborales están cada vez mas definidas en tiempo y recursos, y esto crea la necesidad de aprovechar al máximo el tiempo y recursos destinados, es así como la creación de usuarios inalámbricos móviles se hace presente a causa de la dinámica generada por las relaciones laborales.

Gracias a la movilidad que ofrece la tecnología inalámbrica, el número de usuarios móviles esta incrementándose día con día. Todos estos factores los podemos observar en la figura 36 que a continuación se muestra.

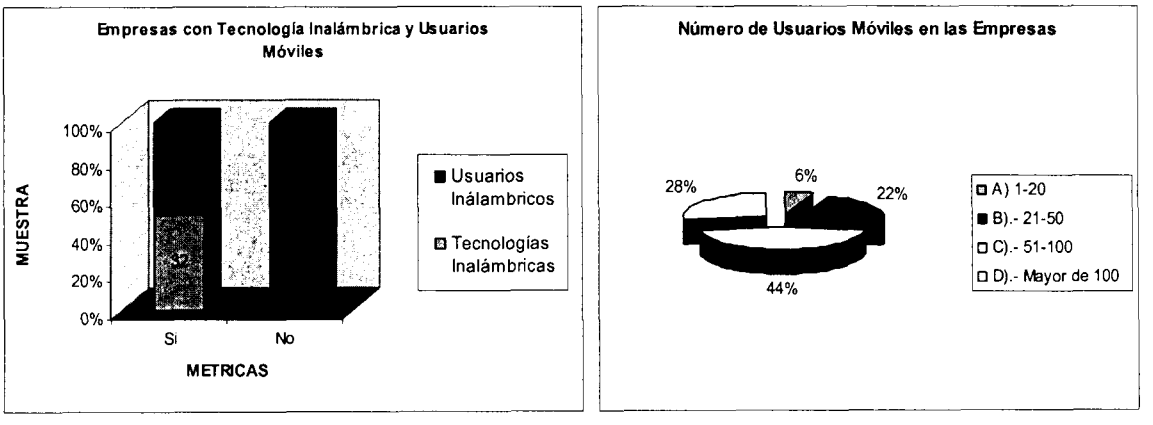

Figura 39.- Utilización de Tecnologías Inalámbricas y Usuarios Móviles en las Empresas

Como era de esperarse, el factor económico es algo muy importante que toda empresa debe tener en cuenta al momento de querer implantar algún método o mecanismo de seguridad de información en la organización, de ahí la importancia de realizar un análisis o estudio adecuado para poder así tomar una decisión acertada.

El capital en la mayoría de las empresas se considera una limitante, esto se muestra en la figura 37, en la cual se muestra el % de adopción de estudios de inversión.

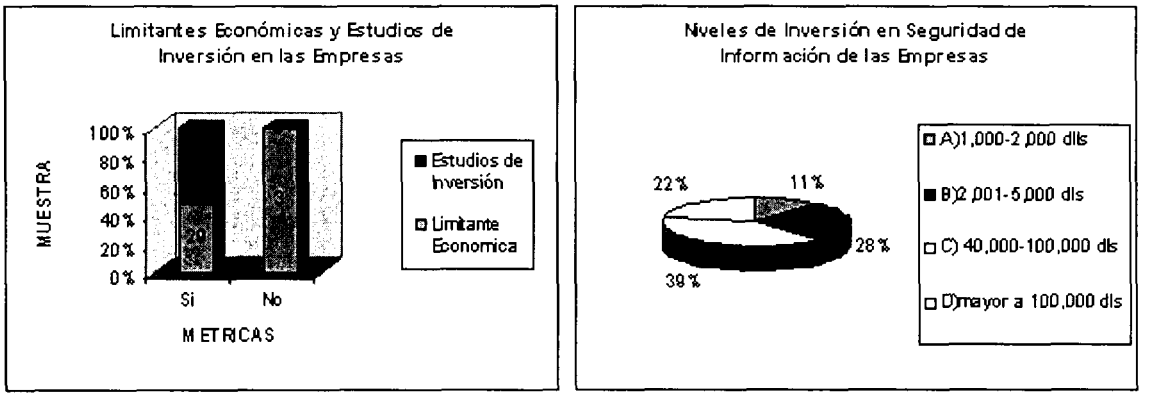

Figura 40.- El Factor Económico como Factor Limitante en las Empresas

La tecnología inalámbrica tiene poco tiempo de adopción, lo cual indica que aun está en proceso de estudio y mejora, es por eso que en los próximos años se espera un incremento en la variedad de dispositivos inalámbricos que pueden ser utilizados en las redes de cualquier empresa.

De acuerdo con los resultados obtenidos podemos ver que la creación de un modelo de seguridad orientado a tecnologías inalámbricas se hace necesaria en las empresas de hoy.

La confiabilidad que ofrecen los dispositivos inalámbricos de mayor utilización por los clientes móviles es menor de la deseada, esto se puede ver en la figura 39; este factor de confiabilidad también repercute en los dispositivos electrónicos utilizados en las empresas para crear o implantar sus redes inalámbricas y ofrecer movilidad.

La confiabilidad que ofrecen los dispositivos móviles es un factor independiente a la confiabilidad que ofrecen las empresas mediante sus redes inalámbricas.

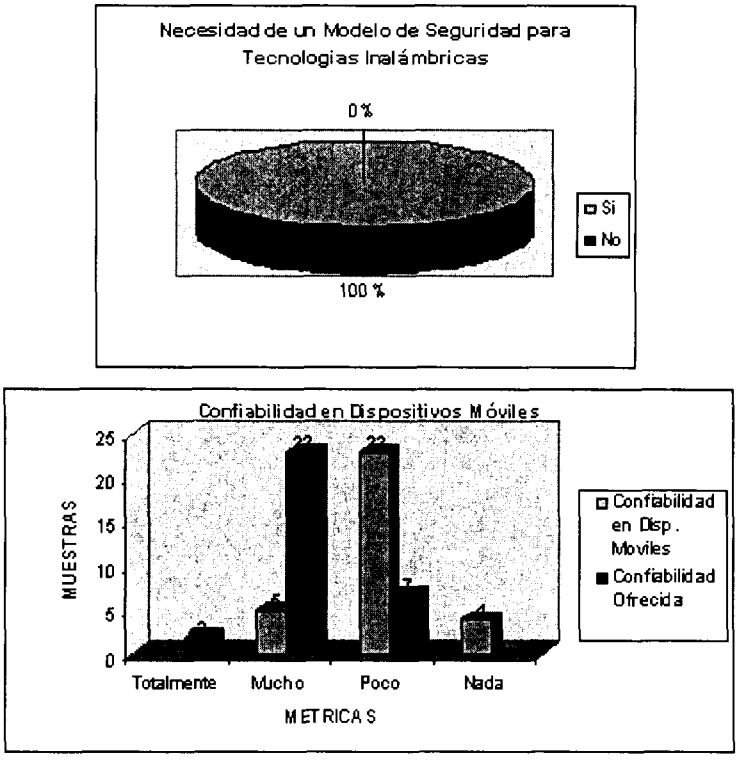

Figura 41.- Necesidad de un Modelo de Seguridad y Confiabilidad de los dispositivos inalámbricos usados

Gracias a la utilización de la tecnología inalámbrica se pueden ofrecer una gran variedad de servicios a través de la utilización de diferentes dispositivos como lap-top, palm, etc. Lo cual permite transportar información de un lugar a otro en sus diferentes presentaciones (datos, voz, vídeo, etc). Esto se puede observar en la siguiente figura, en la cual se muestra el tipo de información utilizada en las redes inalámbricas móviles de las empresas participantes en esta investigación.

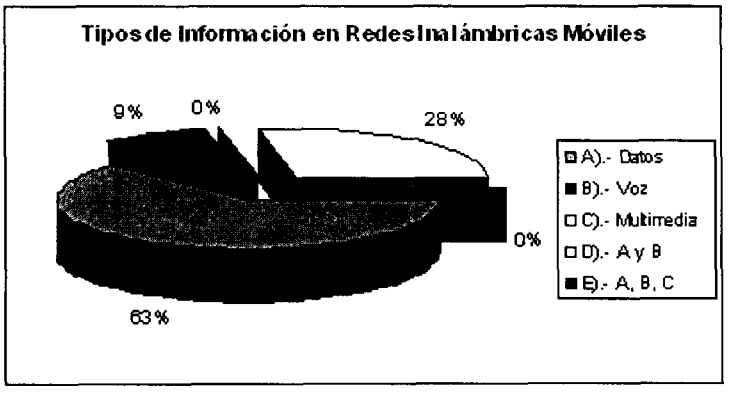

Figura 42.- Tipos de Información utilizada en Redes Inalámbricas Móviles en las Empresas Encuestadas

Gracias a los resultados obtenidos en la encuesta aplicada, se puede tener una opinión más certera del estado que guarda la seguridad de información en las comunicaciones inalámbricas de las empresas en la ciudad de Monterrey.

4.4.2.- EL ESTADO DE LA SEGURIDAD EN TECNOLOGÍAS INALAMBRICAS EN LA CIUDAD DE MONTERREY, NUEVO LEON, MÉXICO.

Al igual que en países que cuentan con un mayor desarrollo en el área, falta mucho por hacer, se requiere de métodos adicionales para garantizar la seguridad en puntos de acceso que ofrecen conectividad inalámbrica por métodos de propagación dispersa, se requiere de un diseño adicional para autentificar usuarios, mas no existe aun un modelo que evite el análisis del medio de transmisión por entidades dañinas.

El estado de la seguridad, incluyendo las tecnologías inalámbricas esta en etapa embrionaria, lo cual hace ver que aun falta mucho por hacer en esta área y la adopción de metodologías o estándares de seguridad en las empresas esta en un proceso de crecimiento.

La adopción de la tecnología inalámbrica tiene pocos años y poco a poco se ha presentado un incremento en el número de clientes que utiliza este tipo de tecnología.

Son peligrosos los servicios celular (esquema tradicional) ya que su información no es segura desde el hecho de que pueden fácilmente hackear todo el celular.

La variedad creciente de servicios que se pueden ofrecer y de dispositivos que se pueden utilizar es un factor importante en el incremento de vulnerabilidades y amenazas. Tal es el caso de los hotspots y de los servicios celulares que integran la tecnología de internet, así como la incorporación de Wi-Fi y GPRS a los dispositivos PDA para su comunicación móvil.

De acuerdo con la investigación realizada podemos ver que existe interés por parte de las empresas de Monterrey en ofrecer servicios seguros de comunicación, esto permitirá que la adopción de modelos, metodologías, mecanismos tecnológicos orientados a la protección de la confiabilidad, integridad y disponibilidad de la información que viaja por sus redes inalámbricas se presente de una forma menos limitada.

4.4.3.- ¿PORQUE ADOPTAR UN MODELO DE SEGURIDAD INALAMBRICA?

La seguridad en redes inalámbricas, es un tópico que carece de madurez, las prácticas de seguridad más saludables que se pueden utilizar son políticas que involucren atención continua en este servicio. Aún no existe un estándar que implemente y garantice una comunicación libre de riesgos.

Hoy en día se vuelve un tema muy importante, ya que se transmite información mucho más confidencial que en caso de ser intervenida puede generar serios problemas para muchas personas.

La tecnología cada día es más sofisticada y flexible, lo cual deja muchas áreas de oportunidad con respecto a la vulnerabilidad de las mismas. Los "Hackers" por su parte cada día generan mejores y más peligrosos softwares para penetrar parámetros de seguridad.

Al ser una tecnología de naturaleza cambiante y de reciente adopción comparada con otras tecnologías, hace necesario la utilización de mecanismos, metodologías y procesos de seguridad que garanticen la disponibilidad, integridad y confiabilidad de la información transportada.

Garantizar estos factores de seguridad es muy importante para que los usuarios se sientan atraídos hacia la adquisición de nuevos dispositivos y servicios inalámbricos, haciendo así que el mercado de la tecnología inalámbrica sea más rentable y atractivo.

CAPITULO 5

CONCLUSIONES

5.1.- CONCLUSIONES

Gartner anticipa que para 2005 existirán 44 millones de usuarios de Hot Spots en el mundo y, de acuerdo con sus estudios, para 2006, 85% de las computadoras portátiles, 60% de los asistentes personales (PDA) y 5% de los teléfonos celulares serán adquiridos con tarjetas para red inalámbrica.

La implantación de la tecnología inalámbrica en las empresas tendrá un incremento en los próximos años, gracias a la demanda de los clientes por nuevos y mejores servicios de comunicaciones, más rápidos y de convergencia, esto se transformará en nuevas ofertas que permiten realizar nuevas funciones y aumentar la productividad en las empresas actuales.

Los nuevos servicios y dispositivos inalámbricos, permiten que el usuario tenga movilidad y se encuentre "always on" en alguna red corporativa o en Internet.

Así como se presenta el incremento de servicios inalámbricos y la gran variedad de dispositivos inalámbricos, los riesgos de seguridad también incrementarán, descubriendo nuevas vulnerabilidades y surgiendo nuevas amenazas.

El problema parte de que los virus evolucionan al ritmo de la tecnología. Amenazas como troyanos y gusanos son cada vez más sofisticadas, y su detección se vuelve más difícil día con día. De hecho, se ha detectado que los atacantes ya no buscan cometer sus destrozos a través del servidor, sino que ahora han encontrado la manera de llegar al usuario y, desde su máquina, causar serios problemas en cuestión de segundos. Esto lo podemos concluir basandonos en el comportamiento que tienen los virus o ataques actualmente, los cuales se propagan a través de metodologías que incluyen ingenieria social, atrayendo a los usuarios para que ejecuten de manera no intencionada algún proceso (programa, script, etc.) malicioso se encuentra oculto, provocando así una reacción en cadena.

Por eso, la seguridad ya no consiste en tener únicamente un antivirus, sino que hace sentido una solución completa de incluir productos y herramientas de seguridad, así como metodologías y mecanismos de alerta temprana. Es necesario un trabajo de prevención, de respuesta ante incidentes críticos, de análisis de riesgo, de identificación de los procesos críticos internos, para dar soluciones que disminuyan el riesgo.

Los hackers desarrollan software cada vez mejores para poder accesar de forma no autorizada a las redes de las empresas, en las cuales se maneja información confidencial, pudiendo así afectar a muchas personas, claro esta que los proveedores de tecnología tratan de crear nuevos métodos de encripción en las comunicaciones, pero este esfuerzo se ve contrarrestado por el esfuerzo de los hackers que pretenden ser reconocidos creando nuevas y mejores formas de ataque.

Es por esto que la seguridad de información juega un papel muy importante ya que la información es cada día más valiosa. El grado o nivel de importancia de la información esta determinado particularmente por el valor que esta tiene para una compañía determinada y sus competidores, esto se puede determinar mediante análisis de negocios y/o valuaciones de los activos de información.

La tecnología inalámbrica se encuentra en un estado de descubrimiento de sus capacidades, aun esta en proceso de implementación y sus ventajas aun no se terminan de descubrir. Las mejoras de Wi-Fi con el surgimiento de 802.11g lo cual incrementa el bit-rate, necesario para ofrecer nuevos y mejores servicios, las mejoras en los métodos de encripción a través de 802.11i, las mejoras de GSM a través de la combinación de WAP y GPRS que permiten nuevas formas de transportar información con menos recursos, lo que motiva a la creación de mejores dispositivos de comunicación como palm, laptop, pda, smart-phones, etc.

Como se comentó anteriormente, la seguridad de información no es un método, es una cultura, la cual debe ir de la mano con el desarrollo de la organización, convirtiéndose de esta forma en una actividad en ejecución día con día, transformándose en políticas y normas, procesos y mecanismos tecnológicos que combinados permitirán garantizar la confidencialidad, integridad y disponibilidad de la información y los servicios inalámbricos ofrecidos por la empresa y utilizados por los subscriptores y usuarios de las empresas.

Se pudo identificar que en las empresas encuestadas; las personas encargadas de la administración de TIC tiene el interés de proteger adecuadamente la información que viaja a través de sus redes inalámbricas, pero la resistencia encontrada en los usuarios por la adopción de nuevas formas y procedimientos de seguridad propicia que no se presente en forma adecuada.

Un factor muy importante identificado en esta investigación de tesis es que la totalidad de las personas encuestadas no tienen conocimiento de la existencia de algún modelo o metodología enfocada específicamente a la problemática inalámbrica que hay actualmente, lo cual da lugar a la propuesta realizada y permite servir como base para futuras investigaciones relacionadas a este tipo de tecnologías.

El modelo propuesto de administración de seguridad inalámbrica tiene como objetivo cubrir los factores más importantes de seguridad como son *integridad, confiabilidad y disponibilidad*, a diferencia de los modelos existentes como el de Bell Lapadula, Biba y Clark Wilson, los cuales están enfocados únicamente a los métodos de control de acceso y a la integridad de la información, en este modelo tomando como base el BS7799 se trata de cubrir en sentido más amplio los factores de seguridad mencionados anteriormente.

Los resultados obtenidos de la investigación realizada en la entidad de Monterrey, permiten deducir que el estado de la seguridad de información en las tecnologías inalámbricas en estas empresas, aun esta en etapa de despegue o de inicio de implementación, lo cual es un factor clave para tomar en cuenta esta metodología propuesta al momento de querer implantar u ofrecer alguna red o servicio inalámbrico, lo que permitirá minimizar los riesgos existentes por el uso de esta tecnología y sí poder prevenir eventos que afecten de alguna forma adversa las labores de la organización que presta este tipo de servicios a sus usuarios y/o clientes.

Uno de los factores clave a considerar es el surgimiento de nuevas amenazas y la evolución de las ya existentes, por lo cual se identifica una carencia en el estándar británico, en el cual solamente se consideran 64 amenazas, las cuales se mencionan como las más comunes e importantes a considerar en un análisis de seguridad. La limitante esta en que no se puede agregar alguna amenaza diferente a las ya definidas, porque se perdería la relación amenaza-control establecida por el estándar. Esto se considera como un área de oportunidad para mejorar un poco más el estándar BS7799, de ahí la importancia de la sección *3.2.1 Interpretación de Amenazas Inalámbricas a Amenazas del BS7799* del modelo de seguridad propuesto. Con esto se pretende lograr un mapeo adicional de las amenazas definidas, lo cual permitirá considerar nuevas amenazas y vulnerabilidades sin perder la relación de amenaza-control establecida en el estándar británico de seguridad.

Esta carencia del estándar abre una puerta de mejora, la cual permitirá servir como punto de partida para nuevas o futuras investigaciones relacionadas con este tema.

Se pudo concluir que existe un cierto interés por parte de las personas encargadas de la administración de TIC de implementar el modelo de seguridad propuesto, ya que lo consideran como una herramienta importante para establecer medidas adecuadas de seguridad

Claro que para esto será necesario la definición y desarrollo de un proceso muy bien definido de implementación del modelo, para poder adoptarlo adecuadamente.

Cabe señalar que lo que se busca es poder hacer comprender la importancia que juega la seguridad de información en la implementación y manejo de la tecnologías inalámbricas, y de esta forma lograr concientizar en cierto grado a las personas para reforzar su interés por el mundo tan complejo de la seguridad de información y se haga participe de esta cultura tan importante en la actualidad.

5.2.- TRABAJOS FUTUROS

Esta investigación y propuesta de modelo de seguridad tuvo el propósito de generar un marco de referencia que pueda ser utilizado por las compañías, instituciones y cualquier organismo o empresa que cuenta o tiene pensado implementar la tecnología inalámbrica para el desarrollo de sus labores. Las compañías tienden generalmente a evolucionar a través de la inclusión de tecnología en sus procesos, y si no se presenta de manera adecuada, puede provocar grandes pérdidas. Es por eso que el modelo de administración de seguridad de información para redes móviles puede ayudar a las compañías a considerar todas las posibilidades de agresión y así poder realizar una correcta implementación de la tecnología, a través del diseño de esquemas adaptables en un entorno cambiante como lo son las comunicaciones inalámbricas.

Entre las propuestas para trabajos de investigaciones derivados de esta tesis, tenemos los siguientes:

- Seguridad de Información en Tecnologías de 3G.
- La cultura de Seguridad de Información en México.
- La influencia que tiene la seguridad de información en el ámbito empresarial.
- El Estándar Británico BS7799 como modelo educativo en seguridad de información.
- Modelos de Seguridad de Información para Instituciones Educativas.
- La adopción del Estándar Británico BS7799 en las empresas como base en la generación de modelos de seguridad.
- La Seguridad de Información como proceso innovador en la adopción de tecnologías en las empresas de hoy.
- Analizar "Best Practices " en seguridad relacionadas con tecnologías inalámbricas para poder hacer aportaciones y/o mejoras al modelo de seguridad propuesto
- Investigar otros estándares o metodologías de administración de seguridad emitidas o desarrolladas por otras instituciones u organismos, para poder generar otros modelos de administración de seguridad
- Incluir tecnologías inalámbricas de nueva generación al modelo de seguridad con sus aportaciones respectivas para poder incrementar su alcance.
- Desarrollar los pasos o metodología para la adecuada implementación del estándar de seguridad ISO17799.

Apéndice

Esta sección contiene la encuesta completa que se aplico en la investigación de esta tesis.

Inicia describiendo la finalidad de esta investigación y aclarando los conceptos principales a los que se hace referencia, con la finalidad de lograr un mejor entendimiento por parte del personal encuestado.

MODELO DE SEGURIDAD PARA REDES INALÁMBRICAS BASADO EN EL ESTANDAR DE SEGURIDAD BS7799
(ENCUESTA)

¡Gracias por atender este estudio!

Objetivo: El objetivo de este proyecto de tesis de maestría es poder conocer la opinión de gente especializada en el área de seguridad y/o tecnología inalámbrica en cuanto al uso de modelos de seguridad de información en las empresas, para tener una perspectiva más real y actual de la tecnología inalámbrica y de las tendencias relacionadas con los métodos y mecanismos de seguridad en los próximos años.

Alcance: El alcance de este modelo comprende las tecnologías de Wi-Fi LANs y 3G, y los dispositivos móviles considerados en la etapa inicial son: Computadoras Notebook, Asistentes Personales Digitales (PDA), Teléfonos Inalámbricos Móviles que utilizan el protocolo WAP.

Usuario Móvil: se consideran aquellos que pueden conectarse de una red a otra, utilizando dispositivos portátiles (PDA, Smart Phone, Tarjetas de red Inalámbricas), también se consideran a los usuarios que están en movimiento *(on road)*.

Seguridad de Información: Se considera como la acción de preservar la confidencialidad, disponibilidad e integridad de la información que viaja a través de los medios de comunicación utilizados por las compañías. En este caso se enfocara a las redes inalámbricas.

NOMBRE:	
CARGO QUE OCUPA:	

Preguntas: *Marque con una **X** la opción elegida.*

1.- ¿Qué tan necesario considera la creación e implementación de políticas de seguridad que garanticen la concientización de los empleados de la empresa y conduzcan al uso adecuado de las reglas y normas establecidas para garantizar la seguridad de la información?.

Totalmente ( ) Mucho ( ) Poco ( ) Nada ( )

2.- ¿Se tienen bien definidas y establecidas las políticas de seguridad de información en la empresa?

Si ( ) No ( )

3.- ¿Existe un área o personal dedicado a la seguridad de la información en su empresa?

Si ( ) No ( )

En caso de que su respuesta sea *No*, pase a la pregunta 9

4.- ¿El área de seguridad de la información apoya o soporta las estrategias de negocio y la misión de su empresa?

Si ( ) No ( )

5.- ¿Prevalece en toda la empresa una cultura de seguridad de la información?

Si ( ) No ( )

6.- ¿El personal encargado de la seguridad de la información es suficiente para cubrir las necesidades de la empresa?

Si ( ) No ( )

7.- ¿La Alta Gerencia apoya y se encuentra involucrada con el área o personal de seguridad de la información de la empresa?

Si ( ) No ( )

8.- ¿Existe una marcada comunicación entre las diversas áreas funcionales de su empresa y el área o personal encargado de la seguridad de la información?

Si ( ) No ( )

9- ¿Existe un proceso de análisis riguroso para determinar los riesgos en seguridad de la información en los sistemas o dispositivos tecnológicos que utiliza su empresa?

Si ( ) No ( )

10- ¿Utiliza algún estándar de seguridad de información como referencia para poder implementar mecanismos y/o procesos de seguridad en su empresa?. *Ejemplo: Estándar Británico BS7799.*

Si ( ) No ( ).

En caso afirmativo Menciónelo: _____

_____

11- ¿La empresa ha tramitado con alguna autoridad certificadora un certificado de seguridad de información?. *Ejemplo: BSI, VerySign, etc.*

Si ( ) No ( ) En caso afirmativo Mencionarla.: _____

12- ¿Se cuenta con un plan de contingencia escrito en caso de posibles ataques informáticos? *Ejemplo: Denegación de servicio, Virus, etc.*

Si ( ) No ( )

13- ¿Se tiene establecido algún proceso de monitoreo constante de vulnerabilidades en los sistemas de información antes de que se presente algún tipo de ataque?

Si ( ) Por implementar ( ) No ( )

14- ¿Se ha detectado algún intento de *"Hackeo"* a la organización en los últimos tres años, ya sea por personal interno o externo?

Si ( ) No ( )

15.-¿Utiliza en su empresa equipos inalámbricos de comunicaciones?, específicamente redes inalámbricas Wi-Fi o 3G.

Si ( ) No ( )

16.- ¿Tiene usuarios inalámbricos móviles en su empresa?.

Si ( ) No ( )

17.- ¿Utiliza algún método (tecnológico y/o de procedimientos) para garantizar la seguridad de la información, orientado a redes inalámbricas en su empresa?.

Si ( ) No ( ).

En caso afirmativo mencionar cual es:

_____

_____

18.- ¿Considera el factor económico como una limitante importante en la empresa para poder brindar un nivel de seguridad de información aceptable?

Si ( ) No ( )

19.- ¿Se realizan estudios de inversión antes de tomar una decisión de compra de algún producto relacionado con la seguridad de la información de la empresa?

Si ( ) No ( )

20.- ¿Tiene pensado invertir en los próximos meses en algún mecanismo tecnológico de seguridad de información para su empresa?.

Si ( ) No ( ).

En caso afirmativo defina el rango de inversión

A).-1,000-2,000 dls. ( ) B).- 2,001-5,000 dls. ( ) C).- 40,000-100,000 dls. ( )

D).- mayor a 100,000 dls. ( )

21.- ¿Cree necesario utilizar algún modelo de seguridad enfocado en redes inalámbricas a consecuencia de la aparición de nuevas amenazas y vulnerabilidades que se presentan día a día?

Si ( ) No ( ).

22.- ¿Qué tanto confías en los dispositivo portátiles (LapTop, PDA, Teléfono Inalámbrico, etc.) respecto al nivel de seguridad de la información que ofrecen?.

Totalmente ( ) Mucho ( ) Poco ( ) Nada ( )

23.- ¿Qué tan confiable es el nivel de seguridad de información que ofrece la tecnología inalámbrica de tu empresa a los usuarios inalámbricos móviles?.

Totalmente ( ) Mucho ( ) Poco ( ) Nada ( )

24.- A consecuencia de que la tecnología esta en constante cambio, ¿que tan necesario cree usted que es mantener actualizados los mecanismos, procesos, normas y reglas establecidas para garantizar un alto nivel de seguridad de información en una empresa?

Totalmente ( ) Mucho ( ) Poco ( ) Nada ( )

25.- ¿Qué cantidad de usuarios móviles tiene su red inalámbrica?

A) 1-20 ( ) B).- 21-50 ( ) C).- 51-100 ( ) D).- Mayor de 100 ( )

26.- ¿Qué tipo de información viaja por su red inalámbrica?

A).- Datos ( ) B).-Voz ( ) C).- Multimedia ( ) D).- A y B ( ) E).- A, B, C ( )

Preguntas: *Proporcione la información solicitada haciendo uso de la experiencia laboral, profesional, etc.*

27.- ¿Qué tipo de servicios y/o aplicaciones proporciona su red inalámbrica? *Ejemplo: Messenger, VPN, etc*

28.- ¿Cuál es su opinión relacionada con el uso de un modelo de seguridad para redes inalámbricas en su empresa, que permita determinar el nivel de riesgo de sus tecnologías y pueda mitigar o reducir a un grado de impacto mínimo las amenazas y vulnerabilidades a las cuales esta expuesta este tipo de tecnologías?.

29.- ¿Qué opina del estado actual de la seguridad de la información en México, relacionado específicamente con las redes inalámbricas y a los usuarios móviles?.

30.- ¿Cuál cree que sea la expectativa respecto a la aparición de nuevas amenazas y vulnerabilidades que se presentan día a día en la seguridad de la información en las redes inalámbricas en los próximos años?.

31.- ¿Cuál cree que sea la tendencia en cuanto a la demanda de servicios y redes inalámbricas para usuarios móviles en los próximos años?.

Glosario

Activo: cualquier cosa que tenga valor para la organización, con las operaciones de negocio y su continuidad.

Análisis de Riesgos: el resultado de un incidente no deseado.

Administración de Riesgos: actividades coordinadas para dirigir y controlar una organización con consideraciones de riesgo.

Amenaza: causa potencial de un incidente no deseado, la cual resulta en un daño para el sistema u organización.

Control de Seguridad: práctica, procedimiento o mecanismo que reducen el riesgo de seguridad.

Impacto: resultado de un incidente no deseado.

Información: el significado que es asignado actualmente a los datos por el significado de las convenciones aplicadas a estos datos.

Seguridad de Información: Protección de la información por:

- *Confidencialidad*: protección de información sensitiva de divulgación no autorizada o de intercepción.
- *Integridad*: resguardar la precisión y cumplimiento de la información y aplicaciones de cómputo.
- *Disponibilidad*: asegurar que la información y los servicios vitales estén disponibles para los usuarios cuando lo requieran.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia.

Vulnerabilidad: debilidad de un activo o grupo de activos, que pueden ser explotada por una amenaza.

Bibliografía

Ansi, American National Standards Institute. 2003 [Online]. Disponible: [2003, Marzo 7].

Aguirre, José Eduardo. "Redes Inalámbricas". Monografía. Marzo 7, 2002.

BCR, Business Communications Review. Septiembre, 2003.

Bsi, The British Standard Institution. "British Standard BS-7799-2". 2003.

Campbell, Roy. "Analisys of Third Generation Mobile Security". Computer Science Department University of Illinois at Urbana-Champaign. June, 2002.

Crane, Adam. "EDGE Deployment and Interoperability". SIEMENS Mobile. March, 2003.

CSI/FBI. "Computer Crime and Security Survey". Computer Security Institute, 2004. Disponible: [2004, Abril 8].

Gralla, Preston. "How Wireless Works". QUE Corporation. 2002.

Hefferan, Rosslynne. "BS7799- Information Security Management". Institute of Scientific & Technical Communicators, 2003 [Online]. Disponible: [2003, Marzo 7].

Hernández, Roberto. "Metodología de la Investigación". Tercera Edición. Mc Graww Hill, 2003.

Lindup, Ken. "A Unified Model for Information Security". Information Security Bulletin. Febrero, 2002.

Mackey, David. "Information Security Policy Models". April, 2002.

Muller, Nathan. "Wireless Data Networking", Artech House Publishers, 2000.

Miller, Stewart S. "WiFi Security". Mc GrawHill Networking, 2003.

Proforum. "Time Division Multiple Acces (TDMA)". The International Engineering Consortium. Septiembre, 2000.

Rappaport, Theodore S. "Wireless Communications (principles and practices)". Second Edition. Prentice Hall, 2002

Revista RED. "Guía de Redes". Cisco Systems, Inc. Mayo, 2003.

Ruíz Peidró, José Julio ."Soluciones Wireless para Comerciales", Gelioss Mobile Solutions, 2002 [Online]. Disponible: [2003, Marzo 7].

SYMANTEC, América Latina. "Riesgos y realidades de la fidelidad inalámbrica (Wi-Fi) en la empresa". Articulo ID: 2344. Publicado en EEUU 16 de Julio del 2003. Publicado en LAM 30 de Septiembre del 2003. Disponible:

SYMANTEC, América Latina. "La Cara Cambiante de los Ciberataques". Articulo ID: 2305. Publicado en LAM 16 de Julio de 2003. Disponible:

Sapphire Technologies. "BS7799", 2003 [Online]. Disponible:. [2003, Marzo 7].

Smith, David . "EDGE Business Case Small and Regional Operators". Nortel Networks. March, 2002

Solarte, Zaide. "Seguridad en Redes". Monografía. 1999.

Temple, Robert. "Internet and Wireless Security". Institution of Electrical Engineers. BTexact communications technology series ; v. 4, 2002.

Tss, Trinity Security Services. "Is BS7799 for you?", Security Bulletin Feb 2002.

UNAM-CERT. "Equipo de Respuesta a Incidentes en Seguridad de Computo". 2004. Disponible:

Vinay Anand. "Cisco IOS Mobile Networks Enabling Networks in Motion". Cisco Systems, Inc. 2003. Disponible: [Octubre,2003]

5a. Conferencia Anual de Seguridad de Información. "Soluciones Seguras en un Mundo Seguro". México, D.F. Mayo, 2003.