TECNOLÓGICO
DE MONTERREY

TECNOLÓGICO
DE MONTERREY

Campus Ciudad de México

Escuela de Graduados en Ingeniería y Arquitectura

Tesis

Proceso para Administrar la Seguridad de la Información en Sitios de Acceso Público Inalámbrico a Internet

---

para la obtención del grado de

Maestro en Administración de las Telecomunicaciones

Autor:
Daniel César Razo

Director: Dr. José Ramón Alvarez Bada

Sinodales: Dr. Teresa Ibarra Santa Ana
Dr. G. Alfonso Parra Rodriguez

Diciembre 2007

Resumen

El presente trabajo de tesis desarrolla el proceso de seguridad de la información basado en el estándar internacional ISO-27002, actualmente reconocido dentro de la industria de telecomunicaciones, el cual nos guía para considerar los elementos de seguridad esenciales con los que se asegura tener un alto grado de integridad, confidencialidad y disponibilidad de la información al hacer uso de un sitio publico de acceso inalámbrico a Internet.

Contenido

CONTENIDO

Capitulo 3

Capitulo 4

Capitulo 5

Lista de Tablas

Lista de Figuras

CAPÍTULO 1

Introducción

1.1. Antecedentes

No hay duda que el uso de la Internet se ha convertido en una herramienta casi imprescindible en el día a día de las actividades que desarrollamos cada uno, desde simplemente chatear a través del messenger hasta realizar movimientos o consultas importantes, aunado a esto también esta presente el tema de la movilidad el cual refuerza aun mas su uso.

Las redes inalámbricas públicas Wi Fi con acceso publico a Internet también llamadas *hot spot*, sin duda forman parte de esta movilidad y la expansión que estas redes están presentando en todo el mundo también se ha hecho presente en México.

Entre las diferentes variantes para contar con un acceso a la red de Internet tenemos el acceso a Internet mediante la línea conmutada (A), el acceso a través de una línea digital de suscriptor asimétrica (*ADSL*) (B) y por medio de un acceso dedicado (n x 64, E1, E3, STM1) (C), pero todas estas soluciones son fijas y nos obligan a estar presentes físicamente ya sea en la casa o a la oficina. Ahora también se tiene la posibilidad de tener un acceso a Internet vía una red inalámbrica (D). El caso de nuestro interés, en donde el acceso es público a cualquiera que lo requiera y que tenga una computadora portátil con su tarjeta inalámbrica instalada y configurada.

Partiendo de la figura 1 se representan los casos antes mencionados en que una empresa proveedora del acceso a Internet (ISP) usa para brindar el servicio de Internet:

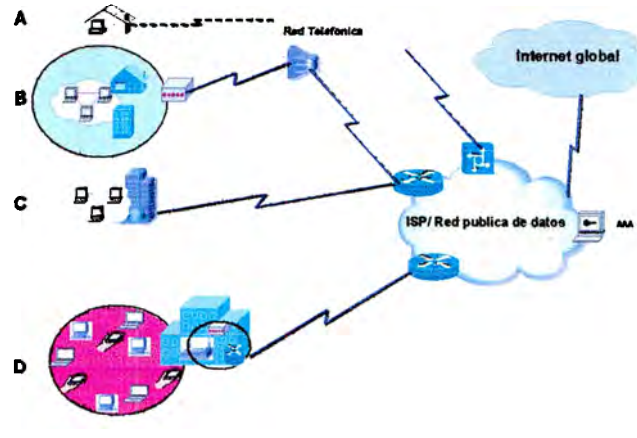


Figura 1.1: El servicio de Internet ofrecido con diferentes tecnologías.

Los clientes actualmente tienden a visitar con mayor frecuencia a este tipo de infraestructura inalámbrica pública con la finalidad de obtener un mejor aprovechamiento de su tiempo, por lo que las empresas proveedoras del servicio de Internet intentan cubrir este nuevo nicho de mercado.

Debido al gran interés para los proveedores del servicio de Internet de tener más clientes cautivos, estos buscan maneras versátiles de llegar a ellos. Las soluciones van mas allá de poder darles acceso a Internet solo en su hogar u oficina, se puede anexar un valor agregado cuando el cliente puede acceder a Internet desde gran variedad de lugares, manteniéndolos comunicados sin tener que estar en sitios limitados a una conexión fija.

Para poder ofrecer la modalidad de acceso a Internet público sin cables se tuvo la necesidad de instalar una nueva infraestructura inalámbrica la cual permite que un usuario equipado con su computadora portátil se pueda conectar a Internet. Los sitios públicos donde se da el servicio público de acceso a Internet de banda ancha se denominan comúnmente *hot spot.*

Los sitios *hot spot* están generalmente ubicados en áreas con alta concentración de personas como hoteles, universidades, centros de convenciones, centros comerciales, cafés, restaurantes, aeropuertos, terminales de autobuses, etc. Lo anterior convierte a los sitios *hot spot* vulnerables a cualquier tipo de alteración, ya que son nodos de comunicaciones que se encuentran co-ubicados dentro de instalaciones ajenas al proveedor del servicio. Por lo tanto surge la necesidad de diseñar un proceso para la administración de la seguridad de la información que se adapte a las necesidades particulares de un sitio *hot spot.*

1.2. Definición del problema

Para los sitios *hot spot* se tiene la necesidad de desarrollar un proceso de seguridad de la información para garantizar la continuidad del servicio y se elimine al máximo el riesgo de la perdida de la información, además con el fin de establecer un marco eficaz de gestión de la seguridad de la información.

En todos los sitios *hot spot* existe la problemática de que no cumplen con algún proceso de seguridad, ya que en un inicio, lo importante era ofrecer el servicio lo mas pronto posible y esto no permitió que la implantación de los equipos tuviera un esquema estructurado de seguridad integral en los sitios y esto los hace vulnerables para garantizar un control de la seguridad.
Entre las vulnerabilidades detectadas:

- "El cifrado en Wi-Fi es violable y los clientes pueden ser monitoreados o sujetos a ataques "hombre en medio" (man-in-the-middle).

  Es casi-imposible hacer una red inalámbrica privada porque su rango de cobertura será mas de lo que tu puedas esperar y puede ser captado desde largas distancias. Wi-Fi para protección comúnmente usa el protocolo WEP (Wired Equivalent Privacy), expertos apuntan que este puede ser violado fácilmente". [CHE-05]
- El control físico de los *sites* de comunicaciones, tales como adecuaciones eléctricas, espacio y clima que no cumplen con las especificaciones de los proveedores de los equipos.

- Lentitud por falta de ancho de banda en los enlaces de salida.
- *Sites* vulnerables a intrusión de personal no autorizado.
- Falta de políticas de seguridad para administrar los sitios.
- Falta de plan de contingencia en caso de desastres.

El proceso de seguridad para los sitios *hot spot*, debe ser una guía bien definida y que involucre a algún estándar internacional reconocido en buenas prácticas de Tecnologías de Información. Entre de los principales estándares internacionales se encuentran ITIL, COBIT e ISO 27002:2005.

Figura: 1.2. Sitio *hot spot* operando sin cumplir un proceso de seguridad.

Debido a que la problemática planteada va dirigida a los sitios *hot spot*, el estándar ISO 27002:2005 es el adecuado para certificar esta unidad de negocio, por lo que éste será el estándar de referencia para resolver la problemática planteada.

En encuestas globales sobre seguridad de la información se reconoce que el ISO 27002:2005 es un estándar internacional que cubre cada una de las fases del espectro de seguridad de la información; por lo que Consultores Ernst & Young, lo han adoptado como marco de referencia para desarrollar la herramienta web de análisis comparativo (benchmarking), la cual provee la base para efectuar una evaluación objetiva de las prácticas de seguridad de la información en una organización y hacer comparaciones con otras organizaciones manteniendo, estrictos estándares de confidencialidad. [ERN-07]

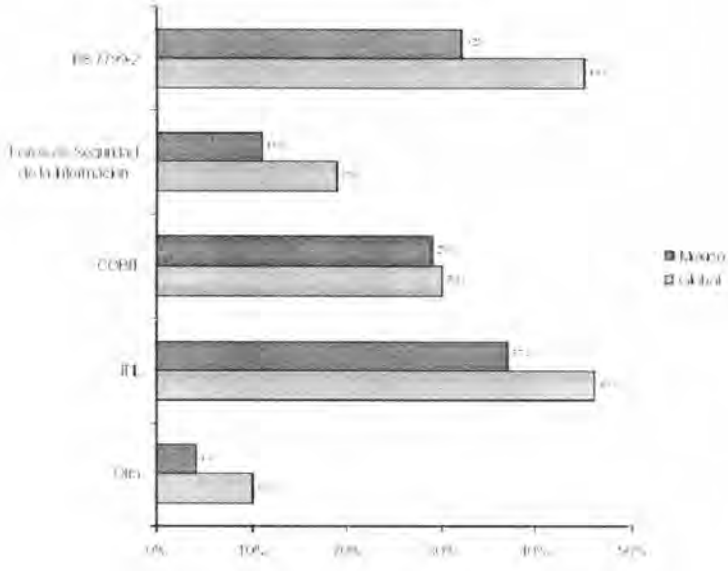


Figura 1.3.Comparación entre estándares en planes de adopción por 1200 empresas encuestadas en 48 países, incluyendo México. [ERN-07]

1.3. Objetivo

El objetivo de esta tesis es desarrollar un proceso de seguridad de la información que deberán cumplir los sitios *hot spot* con el fin de garantizar que la información que viaja a través de estos sitios de acceso inalámbrico cumpla con las premisas de confidencialidad, integridad y disponibilidad de la información.

1.4. Justificación

Dada la evolución que esta presentando el acceso a Internet y a la convergencia de los servicios de voz, datos y video, surge la necesidad de asegurarles a los clientes una alta seguridad y disponibilidad del servicio desde los nodos de acceso y para esto se requiere que cumplan con un proceso de seguridad que permita garantizar que estos nodos de acceso al servicio cumplen con los requerimientos mínimos de seguridad de la información respaldados por un estándar oficial reconocido por la industria de telecomunicaciones y que dé como resultado minimizar las probabilidades de pérdida de información desde el acceso.

"*Telmex estimó que las autoridades podrían dar una resolución para que puedan entrar a dar el "triple play" (voz, datos y video) en el primer trimestre del próximo año 2008*" comento Adolfo Cerezo, director de finanzas de Telmex. [GAS-06]

Lo anterior aunado a la creciente competitividad de las empresas para abarcar un mayor mercado con el único fin de mantener la rentabilidad de estas, da como resultado un compromiso para ofrecer un servicio de alta calidad a los clientes.

La empresa consultora Yankee Group estima que una tercera parte de las llamadas inalámbricas están actualmente dentro del rango de algún tipo de servicio Wi Fi y como las redes Wi Fi continúan expandiéndose, es la oportunidad para que los operadores aumenten más y más sus utilidades. [ANK-05]

Además de acuerdo con las investigaciones globales de la firma Gartner, el número de sitios hot spots públicos en Estados Unidos se ha duplicado en 2004, mientras las investigaciones de Pyramid Research estiman que cerca de 6000 hoteles alrededor del mundo proveen ahora acceso a Internet vía Wi Fi y se espera que en 2007 sean alrededor de 25,000 sitios *hot spot*. [ANK-05]

Ubicando estos escenarios en el mercado mexicano se tuvieron instalados a finales de 2006, 491 sitios *hot spot* distribuidos como se ve en las tablas 1.1 y 1.2, así como su representación en las figuras 1.4 y 1.5. [INT-07]

ESTADO	NO. SITIOS HOT SPOT
AGUASCALIENTES	5
BAJA CALIFORNIA NORTE	17
BAJA CALIFORNIA SUR	3
CAMPECHE	2
CHIAPAS	5
CHIHUAHUA	8
COAHUILA	5
COLIMA	2
DURANGO	4
EDO. MEXICO	36
LEON, GUANAJUATO	6
ACAPULCO, GUERRERO	15
HIDALGO	1
GUADALAJARA, JALISCO	36
MEXICO, D.F.	201
MORELIA, MICHOACAN	6
MONTERREY	31
CUARNAVACA, MORELOS	3
OAXACA	6
PUEBLA	13
CANCUN, Q. ROO	23
QUERETARO	7
SAN LUIS POTOSO	4
SINALOA	10
SONORA	13
TABASCO	8
TAMAULIPAS	1
VERACRUZ	7
MERIDA, YUCATAN	10
ZACATECAS	3

Tabla 1.1. Sitios "hot spot" operando en el territorio mexicano hasta 2006. [INT-07]

SITIOS HOT SPOTS	OPERANDO EN 2006
AEROPUERTOS	53
ANTROS	13
REST. Y CAFETERIAS	275
CENTROS COMERCIALES	32
CINES	2
CENTROS DE CONVENCIONES	7
HOSPITALES	8
HOTELES	64
LIBRERIAS	7
OTROS	7
UNIVERSIDADES	23
TOTAL	**491**

Tabla 1.2. Listado de los sitios públicos de acceso inalámbrico *hot spot* por unidad de negocio en México. [INT-07]

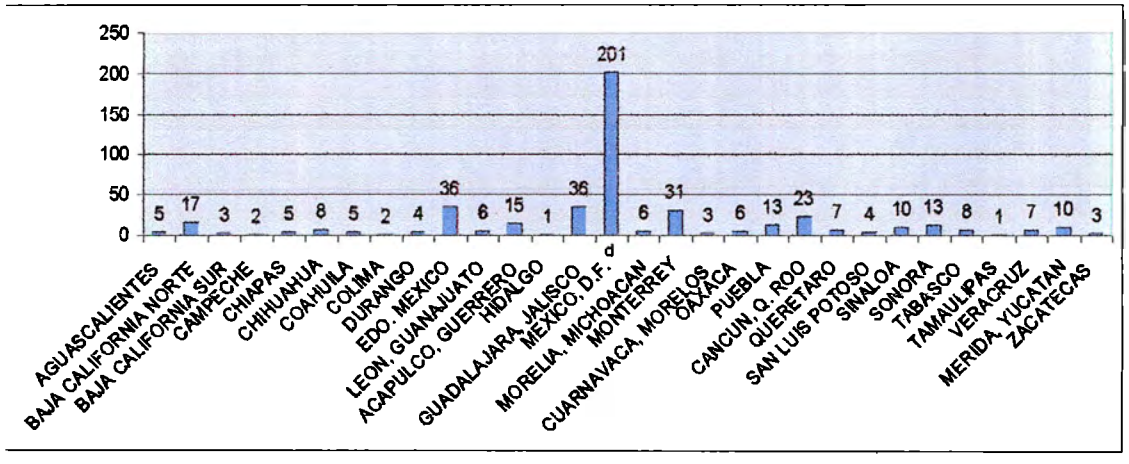


Figura 1.4. Comparación entre Estados de los sitios *hot spot* operando en el Territorio Mexicano hasta 2006. [INT-07]

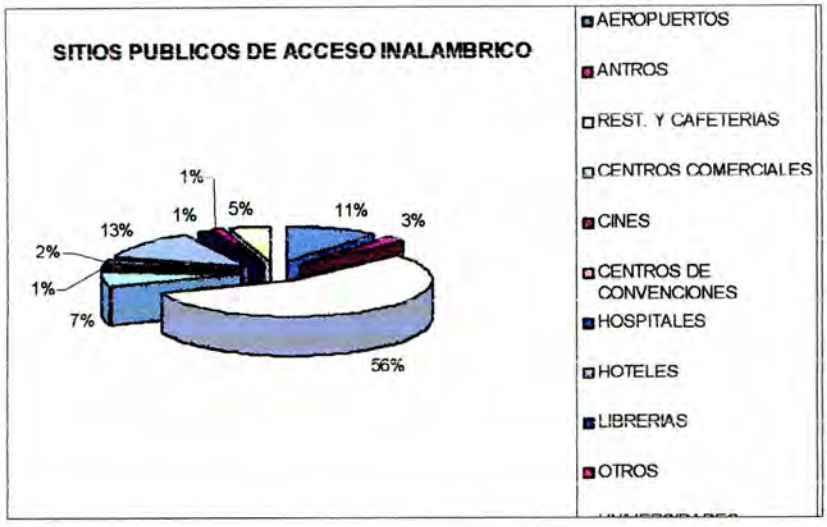


Figura 1.5. Distribución por unidad de negocio de los sitios públicos de acceso inalámbrico *hot spot*. [INT-07]

Al cumplir los sitios *hot spot* con un proceso de seguridad estructurado podrían ser candidatos para alcanzar una certificación internacional.

1.5. Hipótesis

El proceso a desarrollar supone garantizar una alta seguridad de la información que viaja a través de la infraestructura de la red inalámbrica haciendo que estos nodos cuenten con los niveles de seguridad de información requeridos por la Organización Internacional de Estandarización y con la finalidad de contar con los requerimientos mínimos necesarios para certificar los nodos *hot spot* bajo un estándar en caso de que este sea el fin y así asegurar un alto grado de confidencialidad, integridad y disponibilidad de la información en el acceso a la red de Internet en los sitios *hot spot*.

1.6 Limitaciones del proyecto

El trabajo de tesis contempla desarrollar un proceso de seguridad dirigido a los sitios *hot spot* Wi-Fi en México, por lo que el proceso de seguridad desarrollado podrá ser aplicado en todos los sitios *hot spot* actualmente en operación y en los nuevos que surjan, incluso puede aplicarse para aquellos sitios que operen bajo algún otro estándar de la IEEE diferente al 802.11b/g.

Los sitios *hot spot* no son todos iguales, existen dos perfiles bien definidos, de acuerdo a la cantidad de clientes concurrentes que se estima recibir en la conexión inalámbrica y son:
Sitio *hot spot* grande con dos antenas por sitio, es recomendado para soportar hasta 30 clientes concurrentes inalámbricos. [PRO-05]
Sitio *hot spot* extra-grande con un rango entre 3 a 6 antenas instaladas, recomendado para soportar hasta 60 clientes concurrentes inalámbricos. [PRO-05]

CAPÍTULO 2

Marco Teórico

En este capítulo sentaremos las bases para entender la estructura básica de las redes inalámbricas y sobre las cuales se soporta la parte tecnológica de los sitios *hot spot*, además también se describirá la estructura del estándar de seguridad de la información, con base en el cual se propondrá el proceso de seguridad que deben cumplir estos sitios para que cumplan con los requerimientos de seguridad que requiere la información.

2.1. Redes inalámbricas

2.1.1 Definición del Estándar 802.11b/g

802.11 fue el primer Standard de LAN inalámbrico el cual surgió al notar que se obtenía un beneficio mutuo de definir estándares entre los fabricantes y los usuarios, por lo que en 1991 diversos individuos que representaban una variedad de partes interesadas, entre los que se incluyen fabricantes competidores como NCR, Proxim Technologies y Symbol Technologies entre otros, emitieron una solicitud de autorización del proyecto a la IEEE, a fin de establecer un estándar ínter-operable para las LAN inalámbricas. [STA-05]

Puesto que el IEEE es una organización internacional, como regla general se inclina hacia los estándares que tienen una aplicación alrededor del mundo; esta tendencia se inclinó hacia el formado entorno a la banda de 2.4 GHz.

Este primer estándar marcó el comienzo de una nueva era y estableció los fundamentos para el siguiente estándar, 802.11b, que fue ratificado en 1999 y ofrece una velocidad de datos de 11 Mbps, aproximadamente la misma velocidad que el estándar Ethernet.

Normalmente las compañías más grandes son las que tienden a solicitar productos que estén basados en estándares, debido a que esto les asegura varios aspectos clave como:

- Madurez tecnológica
- Estabilidad en el diseño básico
- Interoperabilidad

Madurez tecnológica. Las compañías más grandes no son muy flexibles, aunque actualmente están entendiendo que la velocidad en que cambian tiene ventajas significativas en términos de ser competitiva, eficiente y rentable. Cuando comienzan a desplegar un proyecto basado en una nueva tecnología en particular, se muestran reacios a realizar estos despliegues de manera masiva debido a las fallas asociadas con el diseño, ya que al hacerlo se generan muchos costos y consumo de tiempo. Su rechazo se debe, en parte, al hecho de que existen costos financieros y de tiempo asociados con la capacitación y equipamiento que requieren sus equipos de despliegue para la tecnología nueva.

Estabilidad del diseño. La estabilidad de una tecnología normalmente, pero no siempre, está relacionada con su madurez. Durante las fases más tempranas del despliegue de una tecnología, el diseño fundamental tiene mayores posibilidades de cambios y durante las cuales ocurre la mayor parte de las ventas.

Interoperabilidad: La interoperabilidad se define en parte como la capacidad de que elementos distintos desarrollen sus funciones en conjunto con una degradación pequeña de la velocidad, confiabilidad o mantenimiento. Uno de los aspectos más importantes que los clientes afrontan cuando se despliegan estándares nuevos de tecnología es la interoperabilidad con equipos existentes. [CAR-04]

Para disponer de una red inalámbrica, sólo hace falta instalar una tarjeta de red inalámbrica en las computadoras involucradas, hacer una pequeña configuración y listo. Esto quiere decir que instalar una red inalámbrica es un proceso más rápido y flexible que instalar una red cableada. Una vez instalada la red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada. Las computadoras que forman parte de la red pueden comunicarse entre si y compartir toda clase de recursos.

Por lo anterior las soluciones inalámbricas están poco a poco ocupando un lugar más destacado dentro del panorama de las posibilidades que tienen dos equipos informáticos de intercomunicarse.

No obstante hoy por hoy, las soluciones inalámbricas tienen también algunos inconvenientes como: menor ancho de banda (velocidad de transmisión) y, en general, son más caras que las soluciones por cable. El ancho de banda de las soluciones inalámbricas actuales se encuentra entre los 11 y los 54 Mbps.

Existen 3 estándares de redes inalámbricas (WLAN), de los cuales se enlistan algunas de sus características más importantes en la tabla 2.1.

- Home RF
- BlueTooth
- 802.11

	Home RF	BlueTooth	802.11b
Capa fisica	FHSS	FHSS	FHSS, DSSS, IR
Saltos de frecuencia	50 saltos por segundo	1600 saltos por segundo	2.5 saltos por segundo
Potencia de transmisión máxima	100 mW	100 mW	800 mW
Velocidades de datos	1 o 2 Mbps	1 Mbps	11 Mbps
Numero máximo de dispositivos	Hasta 127	Hasta 26	Hasta 256
Seguridad	Formato Blowfish	0, 40, y 64 bits	40 y 28 bits RC4 TKIP MIC, SSN
Rango	150 pies	30 pies	400 pies en exteriores
Versión actual	V1.0	V1.0	V1.0
Costo	Ni mas ni menos costoso	Menos costoso	Mas costoso
Tamaño fisico	Ni mayor ni menor	El mas pequeño	El mas grande
Alcance exterior al hogar	No	No	Si

Tabla 2.1: Estándares competidores en Radio Frecuencia desarrollados para Interiores. [CAR04]

El estándar 802.11 tiene un conjunto de variantes por ser el estándar que ha capturado la atención de los principales proveedores de esta tecnología y disfruta por un amplio margen la mayor parte del mercado.

Estándar	Frecuencia portadora	Velocidad de datos	Resumen
802.11a	5.1-5.2 Ghs 5.2-5.3 GHz 5.7-5.8GHz	54 Mbps	La potencia máxima es 40 mW en la banda 5.1,250 mW en la banda 5.2 y 800 mW en la banda 5.7 (en Estados Unidos)
802.11b	2.4-2.485 GHz	11 Mbps	Es el estándar que se vende más mientras escribia esta tesis
802.11d	N/D		Múltiples dominios reguladores
802.11e	N/D	N/D	Calidad de servicio
802.11f	N/D	N/D	Protocolo de conexión entre puntos de acceso (Inter-Access Point Protocolo, IAPP, por sus siglas en inglés)
802.11g	2.4-2.485 GHz	36 o 54 Mbps	
802.11h	N/D	N/D	Selección dinámica de frecuencia (Dynamic Fre-quency Selection, DFS, por sus siglas en inglés)
802.11i	N/D	N/D	Seguridad

Tabla 2.2: Resumen de las versiones mas comunes del estándar 802.11b. [CAR-04]

La tecnología inalámbrica empleada para los nodos *hot spot*, está especificada en el estándar IEEE 802.11b, el cual establece las reglas para la comunicación de redes LAN inalámbricas a velocidades de 11 Mbps., en la banda de frecuencia de 2.4 GHz y a distancias de hasta 100 metros, utilizan la técnica de modulación de secuencia directa (Direct Secuence Spread

Spectrum).

En la práctica, la velocidad de 11 Mbps no es totalmente real debido a distintas razones:

- Las interferencias y ruidos hacen que la velocidad baje.
- El propio protocolo consigue menos rendimiento que en sistemas cableados.
- Las conexiones a los puntos de acceso son un cuello de botella.

Por otro lado, la mayoría de las tarjetas inalámbricas de las estaciones son semi-duplex, por lo que pueden trasmitir o recibir, pero no ambas cosas simultáneamente. [ENG-05]

Anteriormente las redes inalámbricas de computadoras se construían utilizando soluciones particulares de cada fabricante. Estas soluciones llamadas propietarias, tenían el gran inconveniente de no permitir interconectar equipos de distintos fabricantes. La única forma de resolver este problema es desarrollar un sistema normalizado que acepten los fabricantes como sistema común. En el caso de las redes locales inalámbricas, el sistema que se esta imponiendo es el normalizado por IEEE con el nombre de 820.11b. A esta norma se le conoce más habitualmente como *Wi Fi o Wireless Fidelity* (Fidelidad Inalámbrica). [WIF-07]

De esta forma, desde abril de 2000 según la norma IEEE 802.11b bajo la marca *Wi-Fi*, se certifica la interoperabilidad de equipos. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tienen el sello *Wi-Fi* pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. (3Com, Aironet, Intersil, Lucent Technologies, Nokia y Symbol). El equipo que recibe las conexiones inalámbricas y que funciona como concentrador es llamado Punto de Acceso *AP* (*Access Point*). [REI-04]

2.2. Topologías de una red inalámbrica

Hay dos formas de configurar una red con el estándar 802.11:

Ad-hoc: computadoras que arman una red en el espacio, no hay estructura en la red, no hay puntos fijos, y usualmente cada nodo puede comunicarse con otro. El algoritmo "Spokesman Election Algorithm" designa una máquina como maestro y las otras como esclavos; una comunicación de este modo es par a par.

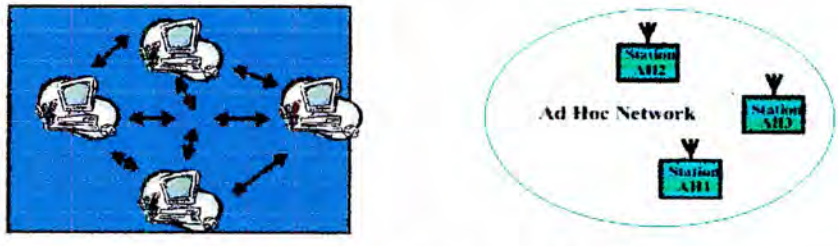


Figura 2.1: Arquitectura WLAN Ad-Hoc.

Infraestructura: Usa un punto de acceso fijo con el cual se comunican los nodos móviles. Toda comunicación es a través de un Punto de Acceso (AP), la función del *AP* es formar un puente entre a red inalámbrica y una red cableada. [CAR-04]

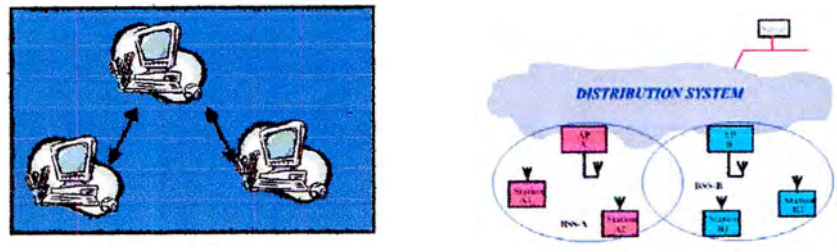


Figura 2.2: Arquitectura WLAN Infraestructura

2.3. Introducción al estándar ISO 27002:2005

Como objetivo del documento para alinear el servicio de Internet inalámbrico a alguna normatividad reconocida internacionalmente en cuanto a seguridad de información, comenzaremos a definir de manera básica los términos esenciales del estándar seleccionado.

A continuación se describen cada uno de los diferentes estándares relacionados a la gestión de la seguridad de la información:

ITIL (*Information Technology Infrastructure Library*) es un estándar en TI que se utiliza para certificar personas, no organizaciones. ITIL certifica a directores y profesionales. No se puede hablar de un producto con certificación ITIL ni de conformidad con ITIL. La gente frecuentemente confunde a ITIL con un marco de auditoria, como Cobit, lo que no corresponde, ya que es sólo un proceso.

COBIT (*Control Objectives for Information and related Technology*): es un estándar basado en un marco de auditorias, un marco del control para la tecnología de información. El marco de COBIT fue desarrollado por el instituto del gobierno de la tecnología de información (ITGI) bien antes de que SOX (*Sarbanes-Oxley Act*) fuera decretado, y especifica la necesidad de estándares en empresas grandes para la selección de productos de tecnología que se basen en requerimientos del negocio.

ISO 27002:2005 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad TI sino que abarca todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. Este concepto marca la diferencia con el de seguridad informática; la norma considera también los riesgos organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica.

En 1995 el BSI (*British Standard Institute*) publicó la norma BS 7799 "Código de buenas prácticas para la gestión de la seguridad de la información". En 1998, también el BSI publica la norma BS 7799-2 "Especificaciones para los sistemas de gestión de la seguridad de la

información" el cual se revisa en 2002. Tras una revisión de ambas partes de BS 7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799 en 2002. Se revisa nuevamente la ISO17799 y esta pasa formalmente a renombrarse como ISO 27002:2005 el 1 de Julio de 2007 y manteniendo el contenido así como el año de publicación formal de la revisión.

Las mejores prácticas tales como COBIT, ITIL e ISO 17799 se utilizan por todo el mundo para mejorar el funcionamiento, valor y control de las organizaciones que invierten en Tecnologías de Información (TI). Hasta este momento, su valor y propósito se han discutido principalmente entre los profesionales de las TI. En clima de los negocios de hoy, esto no es suficiente. Los ejecutivos senior necesitan un alto nivel de conocimiento de estos estándares y como pueden integrarlos para gobernar su empresa en las TI. [ALI-05]

De acuerdo a la definición proporcionada por la Organización Internacional de Estandarización y a la Comisión Internacional de Electrotecnia (ISO/IEC), la información es un activo que, como otros activos importantes en el negocio, es esencial para la organización y por consecuencia necesita estar protegido. Esto es especialmente importante en el ambiente de crecimiento de la interconectividad entre empresas y como un resultado de este incremento de interconexiones, la información esta expuesta a un número mayor de amenazas y a una amplia variedad de vulnerabilidades. La información puede existir en muchas formas, tales como impresa o escrita, bajo almacenamiento electrónico, trasmitida por correo postal o usando medios electrónicos, mostrada en filmes o verbal. Cualquier forma que la información tome o medio por el cual se comparta, debería estar siempre protegida apropiadamente.

La seguridad de la información es la protección de la información desde un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los riesgos de este y maximizar el retorno de inversión y las oportunidades de negocio.

La seguridad de la información es alcanzada al implementar un apropiado conjunto de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software. Estos controles necesitan estar establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que la especificación de seguridad y objetivos del negocio de la organización sean conocidos.

Las organizaciones, sus sistemas y redes de información dan la cara con las amenazas a la seguridad desde un amplio rango de fuentes, incluyendo fraudes, espionaje, sabotaje, vandalismo, incendios o inundaciones. Causas por prejuicio o daño como códigos maliciosos, ataques a computadoras y los ataques para negar el servicio, que son los más comunes y ambiciosos por lo que han incrementado su sofisticación.

La seguridad de la información es importante para los sectores público y privado para proteger la infraestructura crítica. En ambos sectores, la seguridad de la información debe funcionar para evitar o reducir los riesgos más relevantes.

La interconexión entre redes públicas y privadas para compartir las fuentes de información incrementa la dificultad para lograr el control del acceso. También la tendencia hacia el cómputo distribuido ha debilitado la efectividad del control centralizado especializado.

Muchos sistemas de información no han sido diseñados para ser seguros, y la seguridad que puede ser alcanzada a través de medios técnicos es limitada, por lo que se debe soportar también con procedimientos y administración adecuados. Identificando, cuáles controles deberían estar y en que lugar, y para esto se requiere de una cuidadosa planeación y atención. La administración de la seguridad de la información requiere, como mínimo, de la participación de todos los empleados en la organización. Esto puede requerir desde la participación de los accionistas, proveedores, terceros, clientes y externos; los avisos especializados hacia fuera de la organización también pueden ser necesarios. [ISO-05] "Si usted observa la manera como la ISO 27001 se está presentando, se observa cómo están intentando tomar lo mejor de todos los mundos," dice a Dick Mackie, director de systems experts. [MIM-05]

2.4. Estructura del estándar ISO 27002:2005 y los elementos que lo componen

Este estándar contiene 11 cláusulas del control de la seguridad, siendo las siguientes:

a) Política de Seguridad
b) Aspectos Organizativos para la Seguridad.
c) Clasificación y Control de Activos.
d) Seguridad relacionada a los Recursos Humanos.
e) Seguridad Física y del Entorno.
f) Administración de las Comunicaciones y Operaciones.
g) Control de Accesos.
h) Desarrollo y Mantenimiento de los Sistemas.
i) Administración de los Incidentes de Seguridad.
j) Administración de la Continuidad del Negocio.
k) Conformidad con la Legislación.

1. Política de Seguridad

Este elemento dentro del estándar se encarga de dirigir y dar soporte a la gestión de la seguridad de la información y así asegurar que se establezcan los lineamientos de seguridad mínimos a los que se deben apegar los procesos de la organización para que sus usuarios los conozcan y respeten.

2. Aspectos Organizativos para la seguridad

Este control contempla la gestión la seguridad de la información dentro de la organización, así como mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros. También considera mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

3. Clasificación y Control de los Activos
Esta guía dentro del estándar ISO 27002:2005 nos permite mantener una protección adecuada sobre los activos de la empresa, así como asegurar un nivel de protección particular a los activos de la información.

4. Seguridad relacionada a los Recursos Humanos
Este punto contempla reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios, así como asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Además también su intención es minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

5. Seguridad Física y del Entorno
Esta es una guía más a considerar que se encarga de aplicar los controles de acceso adecuados con el fin de evitar accesos no autorizados, daños, interrupciones e interferencias así como evitar pérdidas o comprometer los activos de la organización.

6. Gestión de las Comunicaciones y Operaciones
Este componente del estándar tiene la finalidad de asegurar la correcta y segura operación de los recursos que se encargan del tratamiento de la información, minimizar el riesgo de fallas en los sistemas, proteger la integridad del software y de la información, mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación, asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo, evitar daños a los activos e interrupciones de actividades de la organización, prevenir la pérdida, modificación o mal uso en el intercambio de la información.

7. Control de Acceso
Sobre este control descansan responsabilidades tales como: controlar los accesos a la información, evitar accesos no autorizados a los sistemas, evitar accesos a usuarios no autorizados, protección de los servicios en red, evitar accesos no autorizados a los equipos de comunicaciones, evitar accesos no autorizados a la información contenida en los sistemas, detectar actividades no autorizadas, garantizar la seguridad de la información durante la utilización de los dispositivos móviles.

8. Desarrollo y Mantenimiento de Sistemas
La función de este componente es asegurar que la seguridad está incluida dentro de los sistemas de información., evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones, proteger la confidencialidad, autenticidad e integridad de la información, asegurar que los proyectos de TI y las actividades complementarias son llevadas a cabo de una forma segura, mantener la seguridad del software y la información de la aplicación del sistema.

9. Administración de los Incidentes de Seguridad
Este elemento marca la guía para tomar en cuenta los incidentes que suceden en la organización y que ponen en riesgo la seguridad de la información, por lo que es importante llevar un control de estos, con el fin de prevenir o predecir alguna situación recurrente mediante la detección de

patrones de comportamiento.

10. Administración de la Continuidad del Negocio
Este componente del estándar ISO 27002:2005 contempla la situación de cómo reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres.

11. Conformidad con la Legislación
Este control nos lleva a evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad, a garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma, maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoria de sistemas.

2.5. Valoración de los riesgos, su tratamiento y la selección de los controles.

Los resultados de la valoración de los riesgos ayudarán a guiar y determinar las acciones apropiadas y las prioridades para administrar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerlo contra esos riesgos. La valoración de los riesgos debería ser repetida periódicamente para direccionar cualquier cambio que deba influenciar los resultados de la valoración de los riesgos.

Una vez que los requerimientos y los riesgos han sido identificados y las decisiones para el tratamiento de los riesgos han sido hechas, los controles apropiados deberían ser seleccionados e implementados para asegurar la reducción de los riesgos en un nivel aceptable. Los controles pueden ser seleccionados desde este estándar o desde otro conjunto de controles, o también nuevos controles pueden ser diseñados apropiadamente de acuerdo a las necesidades específicas del negocio. La selección de los controles de seguridad es dependiente sobre las decisiones de la organización basadas en el criterio para aceptar el riesgo, opciones de tratamiento de los riesgos y la administración general del riesgo, enfocados a aplicarse a la organización y que deberían también estar sujetas a todas las legislaciones y regulaciones relevantes ya sean nacionales e internacionales.

Algunos controles en éste estándar pueden ser considerados como guía para la administración de la seguridad de la información y aplicables a la mayoría de las organizaciones.

Un cierto número de controles pueden ser considerados como un buen punto de arranque para implementar la seguridad de la información. Los requerimientos legislativos o los considerados como una práctica común, cualquiera de los dos son esenciales para la seguridad de la información.

Los controles considerados que pueden ser esenciales para una organización desde un punto de vista legislativo incluyen, dependiendo de la aplicación de la legislación:
a) Protección de datos y privacidad de la información personal.
b) Salvaguardar los registros de la organización
c) Derechos de propiedad intelectual

Controles considerados para ser una práctica común para la seguridad de la información incluyen:
a) Documento de las políticas de la seguridad de la información
b) Asignación de responsables de la seguridad de la información
c) Concientizar, educar y entrenar sobre la seguridad de la información
d) Aplicación correcta de los procesos
e) Vulnerabilidad de la administración
f) Administración de la continuidad del negocio
g) Incidentes y mejoras de la administración de la seguridad de la información

Estos controles pueden aplicar a la mayoría de las organizaciones y en la mayoría de los ambientes. Debería ser notado que si bien todos los controles en este estándar son importantes y deberían estar considerados, la relevancia de cualquier control debería ser determinada de acuerdo a los riesgos específicos que una organización enfrenta. Si bien lo mencionado arriba es considerado un buen punto de arranque, esto no reemplaza la selección de controles basados sobre una valoración de los riesgos.

2.6. Factores críticos de éxito

La experiencia ha demostrado que los siguientes factores son con frecuencia críticos para el total éxito de la implementación de la seguridad de la información dentro de una organización:
a) Las políticas de seguridad, los objetivos y las actividades que reflejen los objetivos del negocio.
b) Un enfoque y un marco de trabajo para implementar, mantener, monitorear y mejorar la seguridad de la información y que sean consistentes con la cultura organizacional.
c) Un soporte que sea visible y comprometido desde todos los niveles de la administración.
d) Una buena comprensión de los requerimientos de la seguridad de la información, valoración de los riesgos y administración de los riesgos.
e) Mercadotecnia efectiva de la seguridad de la información para todos los administradores, empleados y otras partes para alcanzar la concientización.
f) Distribución de una guía sobre políticas de seguridad de información y estándares para todos los administradores, empleados y otros.
g) Provisión de fondos para financiar actividades relacionadas a la administración de la seguridad de la información.
h) Dar de forma adecuada la concientización, entrenamiento y educación.
i) Establecer un proceso efectivo para la administración de los incidentes de la seguridad de la información.

2.7. Desarrollar guías particulares

Este código de práctica puede ser considerado como un punto de inicio para el desarrollo de guías especificas en las diferentes unidades de negocio de la empresa. No todos los controles o guías en este código pueden ser aplicables, incluso pueden agregarse algunos controles adicionales que se requieran.

Como se menciono en el punto 2.4, la estructura del estándar se compone de 11 elementos de seguridad, los cuales se analizaran con la problemática presentada en los sitios *hot spot* y al final del análisis se seleccionaran los elementos que el desarrollarse individualmente ayuden a resolver dicha problemática. Se menciona nuevamente la problemática planteada y que se tiene como objetivo resolver:"*Para los sitios hot spot se tiene la necesidad desarrollar un proceso de seguridad de la información para garantizar la continuidad del servicio y se elimine al máximo el riesgo de la perdida de la información, además con el fin de establecer un marco eficaz de gestión de la seguridad de la información. En todos los sitios hot spot existe la problemática de que estos no cumplen con algún proceso de seguridad, ya que en un inicio, lo importante era ofrecer el servicio lo mas pronto posible y solo dio tiempo de la implantación de los equipos sin poder estructurar un esquema de seguridad especifico en el sitio*".

Por lo que en base a esta problemática, se enfocaran los esfuerzos para alcanzar su solución y así pueda ser de utilidad este documento a la empresa en la unidad de negocio de redes inalámbricas.

CAPÍTULO 3

Metodología

En este capítulo se muestra una revisión del documento de diseño de seguridad existente para red de datos en general dentro de la empresa NET, que es la que instala y gestiona el servicio de Internet inalámbrico, después de esta revisión se determinará el alcance del documento con la finalidad de conocer si son suficientes los controles de seguridad que éste contiene para resolver la problemática de la red inalámbrica en los sitios *hot spot*.

También se realizará un análisis de los riesgos en los sitios *hot spot*, con base en los equipos de los que depende el servicio, en las instalaciones donde se brinda el servicio y el personal involucrado en la prestación de este y finalmente calculara el numero de muestras que deberán ser recabadas para poder validar y priorizar el proceso a desarrollado, al tener presentes las vulnerabilidades en los sitios *hot* spot para disminuir los riesgos de amenaza detectados.

3.1. Actual documento de diseño para la seguridad.

Las políticas de seguridad que se tienen escritas en la empresa NET están basadas en el estándar británico BS7799, el cual es la base del estándar ISO 27002:2005. En la definición general del documento existente llamado "Diseño de la Administración de Seguridad" se menciona que para asegurar el conocimiento y seguimiento de estas políticas es necesario que cada integrante de la empresa realice una evaluación sobre los aspectos mas importantes de seguridad, teniendo que refrendarse cada año, con el fin de tenerlas siempre actualizadas. Lo anteriormente mencionado no se cumple, ya que el personal involucrado en el servicio *hot spot* no tiene conocimiento de la existencia del documento de diseño.

A continuación se mencionan los elementos de seguridad que se describen en el documento "Diseño de la Administración de Seguridad" que se tiene desarrollado.

3.1.1. Seguridad

Este control de seguridad de la información forma parte del documento mencionado y esta compuesto por 3 políticas, en donde la primera indica que las políticas de seguridad son aplicables a todas las unidades de negocio de la empresa, a sus empleados regulares y empleados no regulares tales como temporales, por honorarios, contratistas, proveedores y consultores; la segunda política indica que la subgerencia de seguridad deberá preparar, mantener y distribuir los manuales de seguridad que describan las políticas y procedimientos de seguridad; y la tercera menciona que con el objeto de difundir y capacitar al personal en aspectos de seguridad, se hace necesario preparar un programa de concientización dirigido a los diferentes niveles organizacionales de la empresa.

3.1.2. Organización de la seguridad

El desarrollo sobre este control lo componen 11 políticas que describen que la responsabilidad de emitir la normatividad de seguridad recae únicamente en la subgerencia de seguridad y a su vez debe apegarse a las políticas generales de seguridad de la empresa.

3.1.3. Clasificación y Control de Activos

Este elemento de la seguridad lo componen 9 políticas que se deben aplicar para llevar a cabo la clasificación de los activos y sus dueños, como responsables de estos, y considerando que la información es un activo de la empresa este se clasifica como confidencial, privado y publico.

3.1.4. Responsabilidad del personal

Este componente del diseño de seguridad se describe en 7 políticas a cumplir por el personal de la empresa, indicando que debe existir un concientización de la seguridad informativa de hacia los empleados, con la finalidad de que sean acatadas las disposiciones marcadas y que en caso de violación o desacato de estas repercutirían en acciones legales hacia los empleados.

3.1.5. Seguridad Física

Esta guía del estándar sólo indica una política general que describe un completo apego a las políticas de seguridad física definidas para el grupo de empresas al que pertenece NET.

3.1.6. Administración de Operaciones y de red de Comunicaciones

Este control del estándar contiene 17 políticas definidas en las cuales indica que deben existir formalmente documentados todos los procedimientos operativos de la red, con la finalidad de manejar los incidentes de seguridad que permitan una rápida y efectiva respuesta en casos de contingencia y desastre, indicando que los incidentes de seguridad de la información serán manejados por el personal de la subgerencia de seguridad. También se menciona en este apartado que se establecerán los controles que vigilen la integridad, confidencialidad y autenticación de la información transmitida vía correo electrónico. Además los intercambios de software o datos con terceros requerirán de un acuerdo formal por escrito.

3.1.7. Control de Acceso

Para esta elemento del estándar se tiene 32 políticas escritas y hablan de mantener un control estricto del acceso a la información mediante perfiles de acuerdo a su área de responsabilidad y con la autorización del dueño de la información para acceder a esta, contando con sistemas de monitoreo que detecten y reporten inmediatamente cualquier violación o intento de acceso no autorizado. Además también se contempla estar en coordinación con el área de recursos humanos para mantener la base de usuarios actualizada, en caso de bajas del personal con un acceso registrado.

3.1.8. Desarrollo y Mantenimiento de Sistemas

Este componente del diseño de seguridad lo integran 23 políticas, indicando que los sistemas nuevos y actuales deben contemplar los controles de seguridad que cubran los aspectos de confidencialidad, integridad y disponibilidad de la información, gravando eventos auditables para eventos relevantes, la toma de respaldos de información, planes de recuperación y reportes especiales. Considera que cualquier sistema de información que sea liberado a producción deberá estar plenamente identificado y documentado para su administración. También menciona que la información confidencial deberá ser codificada antes de respaldarse y almacenarse así como que sin excepción, todos los programas y documentación generados o elaborados por los empleados, consultores o personal contratado son propiedad exclusiva de esta.

3.1.9. Planeación de continuidad del negocio

Este elemento compuesto por 10 políticas hacen referencia a que se deberá definir una estrategia permanente de recuperación para las diferentes plataformas de la red , así como desarrollar, documentar, probar y mantener los planes de recuperación que conduzcan a la restauración de los sistemas críticos de información del negocio, con el objeto de dar continuidad al negocio. El plan de continuidad del negocio deberá tener una copia de respaldo fuera de las instalaciones centrales conjuntamente con los respaldos de la información crítica y deberá probarse por lo menos cada seis meses.

3.1.10. Cumplimiento

Este control del estándar esta integrado por 19 políticas a respetar, las cuales expresan básicamente que el software instalado en todas las computadoras de la empresa deberá ser desarrollado internamente o estar de acuerdo a los compromisos de licencias, leyes de protección de copia y los acuerdos de compra. También indica que se deberá contar con la información que se acuerde debe ser retenida para fines de auditoria y que deberá conservarse por un periodo de acuerdo a las regulaciones vigentes y las auditorias se deberán realizar de forma periódica para verificar el cumplimiento de las políticas de seguridad.

3.2. Análisis del actual diseño de seguridad de la información

Los controles que componen el "Diseño de la Administración de Seguridad" presentado y que debería estar aplicando para todas la unidades de negocio de la empresa NET, realmente no contemplan políticas especificas para administrar la seguridad de la información de los sitios de acceso público inalámbrico a Internet, por lo que estos controles específicos serán los sugeridos por el estándar ISO 27002:2005, y se buscara que el proceso definido sea escalable a otras tecnologías inalámbricas para redes en sitios *hot spot*.

3.3. Elementos del estándar seleccionados dentro del proceso desarrollado

A continuación se presentara como se incluyeron cada uno de los elementos del estándar ISO 27002:2005 dentro del proceso de seguridad de los sitios de acceso público a Internet.

3.3.1. Política de seguridad

Este elemento del estándar se considero para que las políticas de seguridad existentes en la empresa sean ampliadas, con el fin de que se considere el soporte a la gestión de la seguridad en los sitios *hot spot* y así los lineamientos que se generen se apeguen a los procesos de operación de los *hot spot,* para así difundirse hacia las áreas que deban conocerlos para asegurar que los clientes que utilizan el servicio de Internet inalámbrico tengan mayor índice de seguridad en el uso del servicio.

3.3.2. Aspectos organizativos para la seguridad

Este control del estándar contribuyo para que se vigile que las políticas de seguridad de la información en los sitios *hot spot* sean aplicadas de manera correcta, principalmente cuando deban ser aplicadas por terceros dentro de las ubicaciones donde esta el equipo que brinda el servicio de Internet inalámbrico, ya que esta intervención puede ser derivada de algún mantenimiento correctivo o de algún mantenimiento preventivo programado.

3.3.3. Clasificación y control de los activos

Este elemento del estándar servio para definir una clasificación de criticidad de los activos relacionados a la red inalámbrica que permita proporcionar a cada activo un nivel de protección adecuado a su nivel de criticidad dentro de la red, mismo que debe ser reflejado en mantener un control del inventario de refaccionamiento en almacén en caso de los equipos.

3.3.4. Seguridad relacionada a los recursos humanos

Este componente de seguridad se aplicó al proceso de seguridad de los *hot spot* indicando políticas de seguridad sencillas de entender y muy precisas, para que el personal que interactúa con la operación y uso de los sitios *hot spot* sea conciente del valor del servicio para los clientes y así dar valor a su trabajo para poderlo cuidar y mejorar.

3.3.5. Seguridad física y del entorno

Este elemento del estándar se hizo presente al desarrollar o mejorar controles de acceso a las ubicaciones físicas dentro de los *hot spot* donde se tiene alojada la infraestructura instalada para el servicio de Internet inalámbrico, con la finalidad de restringir el acceso a personal no autorizado y dar el uso adecuado al espacio asignado al *site* de comunicaciones.

3.3.6. Gestión de las comunicaciones y operaciones

Para los sitios *hot spot* la gestión de las comunicaciones y operaciones se realiza de manera centralizada en la empresa, con una infraestructura de monitoreo robusta, que supervisa todas las plataformas de la red de datos, incluyendo los equipos de los sitios *hot spot*, por lo que no será un tema a desarrollar en la problemática planteada.

3.3.7. Control de acceso

Para este elemento de control del estándar que contemplo como proteger la seguridad de la conexión inalámbrica entre los equipos móviles, (computadoras portátiles, PDAs, teléfonos multimedia, etc.) y las antenas de acceso de la red inalámbrica, ya que a partir de esta conexión se pueden presentar vulnerabilidades en la seguridad mediante ataques maliciosos como "*Man in the middle*".

3.3.8. Desarrollo y mantenimiento de sistemas

Para este elemento del estándar se tomó en cuenta el mantenimiento de los sistemas de seguridad de la red, ya que cuando se logre tener un sistema que cumpla con los controles de seguridad requeridos por el estándar, es necesario operarlo, mantenerlo y mejorarlo por el área responsable de la seguridad que se designe dentro de la estructura de la organización.

3.3.9. Administración de los incidentes de seguridad

Este elemento formo parte del proceso de seguridad de los sitios *hot spot*, ya que a través de los incidentes bien documentados se pueden predecir vulnerabilidades en la red o en el servicio que se pueden corregir en tiempo antes de que sean un problema grave. Por ejemplo problemas de lentitud en horas pico por falta de crecimiento en el ancho de banda de los enlaces o señal baja en algunas zonas del sitio *hot spot* por remodelaciones en el negocio.

3.3.10. Administración de la continuidad del negocio

Casi cualquier problemática o eventualidad inesperada debe estar contemplada en los lineamientos de seguridad de la red inalámbrica, es decir, se considerarlo que hacer para reestablecer o mantener el servicio inalámbrico en caso de eventos inesperados que puedan ser controlados. Por ejemplo como protegerse de los cortes de energía eléctrica, de las inundaciones, de los accesos físicos no autorizados, de los daños físicos de algún equipo.

3.3.11. Conformidad con la legislación

Para los sitios *hot spot* este control juega es importante, ya que la regulación de las señales de radiofrecuencia es administrada por el gobierno, así que se debe acatar la regulación establecida y para no incurrir en alguna falta, debemos conocer que la tecnología desarrollada para los equipos inalámbricos cumplen con los estándares establecidos. Para este punto se incluyo lo que menciona la COFETEL respecto a la tecnología Wi-Fi, que es con la que operan los *hot spot*.

3.4. Análisis de los riesgos

Este análisis de riesgos en los sitios *hot spot* se realizó para determinar la valoración para cada uno de los siguientes puntos:

- Análisis de riesgos para el equipo instalado que ofrece el servicio de Internet inalámbrico.
- Análisis de riesgos para las instalaciones en donde se ubican los equipos de comunicaciones de los que depende el servicio de Internet inalámbrico.
- Análisis de riesgos del personal involucrado en la continuidad del servicio de Internet inalámbrico.

Teniendo en cuenta los elementos de los cuales depende la entrega del servicio de Internet inalámbrico en los sitos *hot spot* se comenzó por desglosar cada uno de los componentes y así identificar el impacto de cada uno de ellos en la entrega del servicio al cliente final.

NOMBRE DEL RECURSO	MODELO	FUNCION EN LA RED	UBICACION EN EL SITIO
ENRUTADOR DEL CLIENTE	CPE 575 Speedstream 5200	Este equipo es el encargado de recibir por un lado el enlace de trasmisión y por otro lado se conecta en LAN al equipo suscriptor.	Site de comunicaciones
SUSCRIPTOR DE USUARIOS	SMS 200	Este equipo se encarga de la administración y asignación de algunos recursos de red y control hacia el usuario final; es el encargado de administrar el ancho de banda que el usuario tiene contratado; es además el encargado de interactuar con el servicio de RADIUS de la red publica de datos para permitir o negar el servicio a los usuarios; también asigna la dirección IP, DNS, Default Gateway y dominio a través del protocolo DHCP.	Site de comunicaciones
SWITCH DE LARGO ALCANCE CONCENTRADOR DE PUNTOS DE ACCESO	CISCO 2912 LRE CISCO 3524 PWR	Es el equipo encargado de proporcionar conectividad en la LAN en donde se encuentran las AP.	Site de comunicaciones
PUNTOS DE ACCESO (AP)	AP 1120	Este elemento es el encargado de brindar la conexión inalámbrica hacia el usuario final utilizando el protocolo estándar 802.1b, previa validación con el SSID y llave de encripcion.	Site de comunicaciones

Tabla 3.2: Funciones del Equipamiento del sitio *hot spot*.

Debido a que la premisa del proceso de seguridad desarrollado implica cumplir con los términos de Integridad, Disponibilidad y Confidencialidad de la información, clasificaremos los riesgos como:

- Riesgo alto, implica tener cualquier tipo de afectación en el servicio y comprometer la seguridad de la información en cualquier nivel.

- Riesgo bajo, se presenta al no tener ninguna afectación en la seguridad de la información durante la operación del negocio, al tener algún tipo de redundancia operativa cuando se dañé algunos de los componentes.

3.4.1. Valoración de los riesgos asociados al equipamiento del sitio *hot spot*

El equipamiento con el que cuentan los sitios *hot spot* es imprescindible para la entrega del servicio de Internet inalámbrico a los clientes, por lo que de su correcta operación depende la calidad del servicio. Los equipos asociados al sitio *hot spot* tienen un nivel de riesgo alto, ya que de acuerdo a las características de cada uno cualquier falla que presente alguno de ellos repercute en el servicio global, así como las funciones que desempeña dentro de la red son criticas, ya que de las funciones que realiza cada uno depende servicio proporcionado.

3.4.2. Valoración de los riesgos asociados a la ubicación donde esta el equipamiento de los sitios *hot spot*

Los riesgos asociados al *site* de comunicaciones, que es donde se encuentra instalados los equipos de comunicaciones del servicio de Internet inalámbrico, que deben ser considerados son:

- Debe existir un dispositivo que proporcione corriente ininterrumpida a los equipos que se encuentran operando dentro del *site* de comunicaciones y que formen parte de la infraestructura de la red inalámbrica.
- El acceso al *site* debe estar controlado por el responsable del sitio *hot spot*.

3.4.3. Riesgos asociados con el personal

Por ultimo, se consideraran los riesgos potenciales que surjan del personal que se encuentra laborando en el negocio donde se encuentra ubicado el sitio *hot spot*, así como del personal de ingeniería de campo que se encarga de resolver cualquier falla técnica en el servicio de acceso inalámbrico a Internet.

- Inconformidad Laboral.
- Problemas con sus superiores.
- Falta de experiencia laboral.
- Errores humanos

NOMBRE DEL RECURSO	TIPO	En Caso de Falla representa un Riesgo
ENRUTADOR DEL CLIENTE	Equipamiento	ALTO
SUSCRIPTOR DE USUARIOS	Equipamiento	ALT0
SWITCH DE LARGO ALCANCE CONCENTRADOR DE PUNTOS DE ACCESO	Equipamiento	ALTO
PUNTOS DE ACCESO (ANTENAS)	Equipamiento	ALTO
SITE DE COMUNICACIONES	Ubicación	ALTO
PERSONAL DEL NEGOCIO	Personal	ALTO
PERSONAL DEL SERVICIO	Personal	ALTO

Tabla 3.3: Valoración de los Riesgos en el sitio *hot spot.*

El recurso humano asociado al servicio de los *hot spot* es una pieza en especial importante para que el servicio que se brinde sea satisfactorio y de alta calidad hacia los usuarios del servicio, ya que finalmente ellos son los que dan la cara hacia el cliente para la solución de los problemas que se presenten.

3.5. Validación del proceso desarrollado

Para identificar las prioridades de cada una de las políticas desarrolladas se requirió estimar el número de encuestas que se aplicarían a los clientes y responsables del servicio para tener una confiabilidad de al menos el 90%, por lo que se tiene la siguiente expresión para su cálculo:

$$n = \frac{n'}{1 + n'/N}$$

Como lo que tenemos N = 491 sitios hot spot, y para tener una información adecuada con un error estándar "se" menor al 0.015 para tener una confiabilidad del 99%.

Siendo la varianza poblacional $\sigma^2 = se^2 = (0.015)\,(0.015) = 0.000225$

s^2 Es la varianza de la muestra, la cual podrá determinarse en términos de probabilidad.

p es la probabilidad para obtener el porcentaje confiabilidad.

$$s^2 = p(1-p) = .99\ (1 - .99) = 0.0099$$

Por lo que:

$$n^2 = s^2 / \sigma^2 = 0.0099 / 0.000225 = 44$$

Así el número de muestras n:

$$n = [44 * \{1 + (44/491)] = 47.94$$

El tamaño requerido para la muestra es el entero mayor de esa expresión, siendo 48 el número de encuestas que al menos se deben aplicar para alcanzar el 99% de confiabilidad, por lo que las encuestas se aplicaron a 57 clientes y 10 administradores involucrados en el servicio en los *hot spot*.

3.6. Modelo de negocio *hot spot*

Actualmente el servicio público de Internet inalámbrico de Telmex que se ofrece en los *hot spot* esta operando bajo tres esquemas:

i. Las personas que contratan a Telmex el servicio de *prodigy móvil* exclusivamente para tener acceso a la infraestructura del servicio público inalámbrico de acceso a Internet.

ii. Las personas que no son clientes de Telmex y requiere tener acceso al servicio de prodigy móvil, lo pueden hacer adquiriendo una tarjeta de prepago en los negocios en donde se ofrece el servicio *hot spot*.

iii. Los clientes Telmex que tienen contratado en servicio de Internet de "Prodigy infinitum" se les proporciona de manera gratuita una cuenta autorizada para utilizar el servicio publico de Internet inalámbrico en los *hot spot*.

De acuerdo a los escenarios anteriores, lo que se busca con el proceso de administración de seguridad de la información desarrollado es robustecer el servicio de prodigy móvil para que aumente el volumen de clientes que contratan exclusivamente *prodigy móvil*, y esto es factible que se cumpla con el impacto de la convergencia de los servicios de voz, datos y video, ya que se considera debe ser favorable para el servicio inalámbrico, si este cumple con las premisas de los clientes.

Esta convergencia de servicios podría beneficiar al servicio que brindan los *hot spot*, ya que si estos responden a las necesidades de seguridad de los clientes, se tendrá acceso a mas recursos en la red de Internet de manera segura y además accesar a nuevas aplicaciones en estos lugares, como son el video en demanda y video juegos en línea.

Para soportar esta convergencia los equipos con tecnología 802.11b con los que opera actualmente el *hot spot* son compatibles con su estándar superior 802.11g, el cual soporta una velocidad mayor de aproximadamente 54 Mbps, lo que representa una velocidad casi 5 veces más alta a la que actualmente ofrece 802.11b.

El estándar 802.11g, ha sido compatible con redes inalámbricas desde 2002, mantiene la compatibilidad con productos anteriores Wi Fi y no es más costoso que los equipos 802.11b. [ADSL-07]

Para hacer uso del servicio de prodigy móvil actualmente solo es posible hacerlo con un equipo portátil como Laptop o PDA (PocketPC o Palm) preparado para el acceso inalámbrico WiFi (802.11b) a través de:

- Tecnología WiFi integrada en el equipo.
- Tarjeta inalámbrica externa.

Actualmente no se tiene considerado otro tipo de dispositivo móvil que se utilice para proporcionar el servicio de Internet inalámbrico a través de los *hot spot*, ya que por ejemplo existen dispositivos móviles como los teléfonos *black berry*, los cuales comercializan los proveedores del servicio celular, ofreciendo con un costo adicional el servicio de Internet a los clientes que los adquieren, pero el servicio de Internet se entrega vía conexión a la red de telefonía celular, por lo que la cobertura se restringe a la cobertura de esta.

Aunque el proveedor del servicio hasta el día de hoy tiene contemplado en el contrato que acuerda con los clientes recibir dispositivos móviles adicionales no ha liberado hasta el momento ningún otro dispositivo móvil que indique cumple con los requerimientos establecidos.

EQUIPO TERMINAL MÓVIL: Equipo portátil que tenga instalado una tarjeta de acceso inalámbrico compatible con las especificaciones establecidas por TELMEX y que están de acuerdo a la especificación IEEE-802.11b también conocida como WiFi (Wireless Fidelity), como una computadora personal portátil (LapTop), computadora de Bolsillo (PocketPC), agenda electrónica (PDA), o cualquier otro dispositivo móvil que se libere en el futuro y que cumpla técnicamente con las especificaciones de conexión al SERVICIO PRODIGY MÓVIL. [TMX-07]

De acuerdo a estudios realizados por el INEGI, la población en México tiene una alta concurrencia para utilizar los sitios públicos que brindan el servicio público de Internet, lo que significa que existe un nicho de mercado importante en el sentido de que ocupan un servicio público y están acostumbrados a hacerlo.

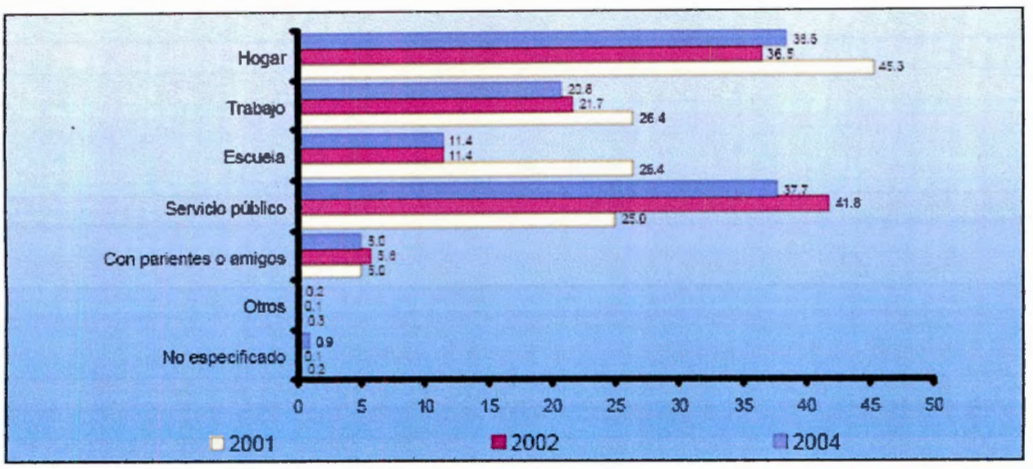


Figura 3.1. Población que utiliza computadoras por lugares de acceso. [INE-07]

Lo que limitaría utilizar el servicio de los *hot spot* es la adquisición de un dispositivo móvil para su conexión, aunque en México ha ido en aumento la compra de computadoras, aunque aun falta mucho por avanzar.

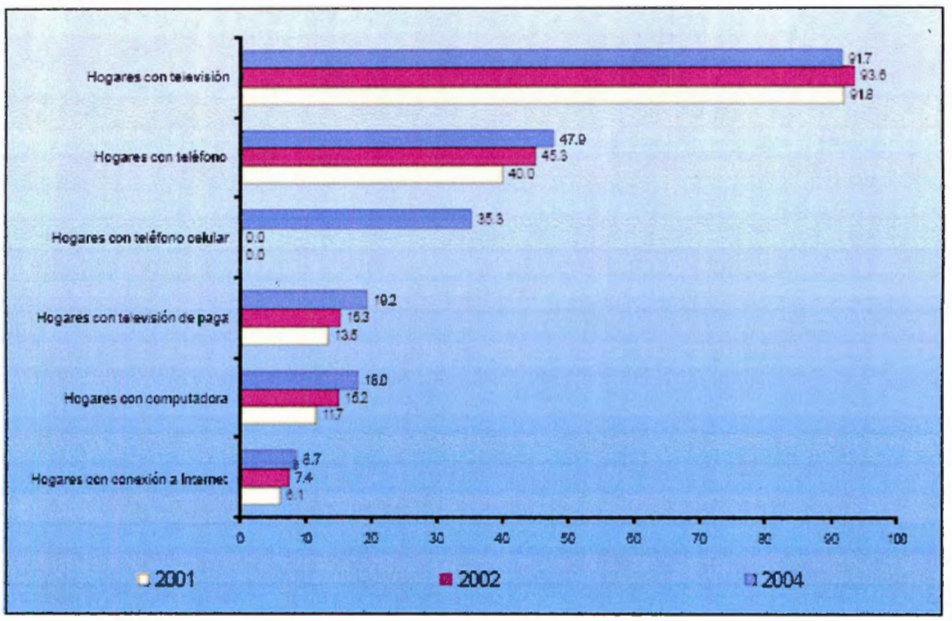


Figura 3.2. Equipamiento de tecnologías de información y comunicaciones en hogares. [INE-07]

Aunque en los últimos años se ha incrementado la manera de adquirir una computadora.

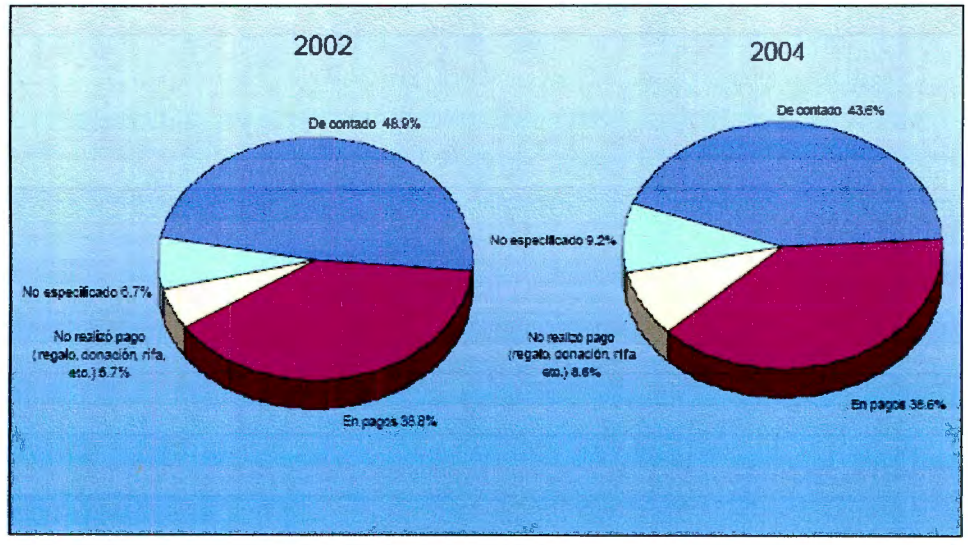


Figura 3.3. Financiamiento para la compra de computadoras. [INE-07]

Por lo que el modelo de negocio actual de los *hot spot* puede cambiar a favor de los clientes actuales y futuros.

CAPÍTULO 4

Resultados

4.1. Desarrollo de los controles del proceso para administrar la seguridad de la información en sitios *hot spot*

4.1.1. Política de seguridad

El servicio de Internet inalámbrico debe ser proporcionado como un producto en el que se proporcione la más alta calidad, la cual debe ser proporcionada al brindar una conexión permanente y segura.

Como punto inicial, para vigilar la gestión de la seguridad de la información se requiere la definición clara de las políticas de seguridad que deben regir el uso del servicio de Internet inalámbrico en los sitios *hot spot*. Las políticas de seguridad de la red *alámbrica* deben estar alineadas con las políticas de la red *inalámbrica*. Todas las vulnerabilidades o debilidades que pueda producir un acceso inalámbrico, es producto de una mala política de seguridad, o simplemente una configuración no adecuada de la computadora.

Política 1A
Los usuarios del servicio inalámbrico en los sitios públicos deberán respetar el radio de cobertura del servicio inalámbrico, ya que la distancia máxima de alcance de la señal de radio frecuencia en lugares cerrados desde la antena del proveedor hasta la antena de la computadora del cliente es de máximo 45 metros.

"*Los usuarios ahora consideran una rutina la operación y compra de productos inalámbricos confiables tales como PCs Wi-Fi que acompañan en los viajes de negocio a los viajeros de hoy. El vagar estando conectado a la red es posible ahora dentro de los límites de un ambiente tales como un hospital, en donde el acceso inmediato a los expedientes de los pacientes en lugares arbitrarios alrededor del campus se logra por medio de los sitios hot spot, sitios que también ya adornan las salas de los aeropuertos. Los usuarios residenciales y de la pequeña empresa, valoran también la conveniencia de las redes inalámbricas, que están libres de la necesidad de tender cableados. Esta razón ayuda a explicar porqué las redes residenciales y SOHO (small-office/home-office) representan la mayoría de las ventas de equipos ethernet inalámbrico*". [EDN-04]

Política 1B
La seguridad de la red inalámbrica será controlada en base a las siguientes premisas:
- Los usuarios del servicio deben configurar su computadora para obtener una dirección IP

dinámica utilizando el protocolo DHCP.
- Los usuarios deben configurar su computadora con conexión inalámbrica con los parámetros para que su conexión maneje codificación WPA, la cual tiene mayor grado de seguridad que la codificación WEP.

Política 1C
Solamente podrán conectarse a la red inalámbrica del sitio *hot spot* los clientes que cuentes con una clave de acceso a la red que haya sido proporcionada por el proveedor de servicio, la cual puede ser sido obtenida a través de una tarjeta de prepago o la realización de un contrato del servicio. *"Se pueden habilitar cientos de hot spot, iluminar todo el país, pero si no existen políticas adecuadas de seguridad y privacidad, la adopción de esta tecnología de acceso a la red, quizá no alcance su plenitud, madurez y confianza por parte del cliente para introducirse sólidamente en el mercado. Cuando la comodidad y la tecnología están en contra de la seguridad, generalmente ésta falla."*[CHA-05]

Política 1D
La subgerencia de seguridad debe vigilar y fomentar la aplicación de todas las políticas de seguridad definidas.

Este elemento del estándar como política de seguridad tiene su base en su desarrollo con el fin de tener una definición clara de lo que debe hacer para que se pueda garantizar la seguridad de la información en el mayor grado posible, por lo que cualquier aspecto que se pueda anexar a este control es valido.

4.1.2. Aspectos organizativos para la seguridad de los sitios *hot spot*

Para asegurar que las políticas definidas sean respetadas, se debe indicar de manera clara a quien debe respetarla como hacerlo:

Política 2A
Anunciar el radio de cobertura de la señal con al menos buena calidad, mediante señales luminosas que sean colocadas en las áreas limite dentro de los 45 metros.

Política 2B
Cuando el cliente realice por primera vez su conexión a la red del sitio *hot spot* le debe aparecer un mensaje de invitación para configurar su dispositivo móvil utilizando el algoritmo de codificación sugerido por el proveedor del servicio, en este caso WPA, concientizandolo que este método de codificación le proporcionara una conexión segura a la red inalámbrica, protegiendo así la seguridad de la información que comenzara a intercambiar.

Lo que se intenta resaltar con los controles organizativos es indicar la manera ordenada de lo que se debe hacer y como, para que la seguridad de la información no sea puesta en riesgo y esta pueda ser controlado con aspectos organizativos que se puedan aplicar.

4.1.3. Clasificación y control de los activos

Los activos relacionados al servicio inalámbrico se muestran en la tabla 3.1 y de la cual se concluye que debido a que cada uno de los equipos tiene dependencia directa de otro, en la cadena de valor todos son críticos en la prestación del servicio inalámbrico, por lo cual se vuelve importante contar con un control de refaccionamiento adecuado de cada elemento dentro de almacén, así como el tiempo de respuesta en la atención a fallas que llegaran a presentarse por causa de daño en alguno de los activos.

NOMBRE DEL RECURSO	TIPO	Criticidad del recurso para el servicio	Valor del Recurso	Pone en Riesgo otros Recursos
ENRUTADOR DEL CLIENTE	Equipamiento	ALTA	ALTO	SI
SUSCRIPTOR DE USUARIOS	Equipamiento	ALTA	ALTO	SI
SWITCH DE LARGO ALCANCE CONCENTRADOR DE PUNTOS DE ACCESO	Equipamiento	ALTA	ALTO	SI
PUNTOS DE ACCESO (ANTENAS)	Equipamiento	ALTA	MEDIO	SI
SITE DE COMUNICACIONES	Ubicación	ALTA	ALTO	SI
PERSONAL DEL NEGOCIO	Personal	MEDIO	MEDIO	SI
PERSONAL DEL SERVICIO	Personal	ALTA	ALTO	SI

Tabla 4.1: Criticidad de los Activos en el sitio *hot spot*.

Política 3A
Los activos de la red inalámbricas deben ser protegidos adecuadamente.

Política 3B
La clasificación de los activos de la red inalámbrica se debe realizar en base a la criticidad de cada uno de ellos para su refaccionamiento.

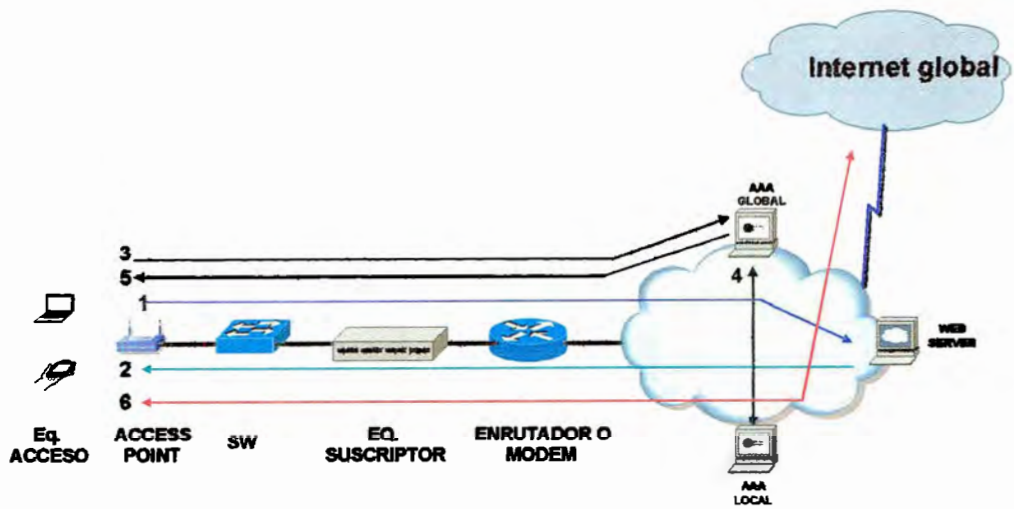
Política 3C
Se debe revisar la obsolescencia de los activos de la red inalámbrica al menos una vez al año.

Un rubro que es muy importante tomar en cuenta, es que es necesario conocer la importancia que juega cada uno de los elementos que intervienen en el ofrecimiento del servicio con la finalidad de que se le de una clasificación de atención particular a cada uno.

4.1.4. Seguridad relacionada a los recursos humanos

Las personas que interactúan con la operación, mantenimiento y uso del servicio de los sitios *hot spot* debe tomar en cuenta las siguientes políticas.

Política 4A
Las personas involucradas en la prestación del servicio de Internet inalámbrico deben conocer:
La topología básica de un sitio *hot spot* la cual se muestra en la figura 3.1 y además de manera básica como opera, lo cual se describe a continuación:



1– Valida en web server id y webkey
2– Indica que pase al AAA
3– Valida en aaa global user y ps en global como servicio deprodigy de algun tipo
4– Valida en aaa local cuenta de prodigy movil
5 – Indica que permite el acceso
6– Estable comunicación con Internet

Figura 4.1. Proceso de conexión a Internet a través de la red inalámbrica.

Cuando un cliente requiere navegar por Internet dentro de un sitio *hot spot,* su dispositivo móvil debe estar debidamente configurado con el nombre de la red inalámbrica a la que quiere acceder (SSID = Prodigy Móvil) y también tener configurado un tipo de encripcion habilitado (WPA KEY) y la opción ANY para que su dispositivo se asocie a cualquier Punto de Acceso o Antena.

Con las funciones anteriores previamente configuradas el dispositivo del cliente realiza una solicitud del servicio al punto de acceso o antena (AP) mas cercano o al AP que tiene mayor potencia de señal.

La solicitud llega al *lanswitch* que concentra las APs, el cual se comporta como un *bridge* (puente) y deja pasar la solicitud sin hacerle nada, la cual es entendida por el equipo suscriptor, el

cual tiene funciones de DHCP Server y le asigna una dirección IP dinámica a la maquina del cliente.

Al tener la maquina del cliente una IP asignada, el cliente ya esta en posibilidades de realizar una solicitud para navegar por Internet, y al hacerla la solicitud este "*request access*" vuelve a ser atendido por el equipo suscriptor el cual le pega a la dirección IP origen datos adicionales como dirección MAC y puerto origen de la petición, para así redireccionar este "*request access*" a través del enrutador hacia el WEB Server, el cual le regresa una pantalla preguntándole su "*User y password*".

El cliente al teclear sus contraseñas se envía la solicitud de "*Access Request*" la cual llega al equipo suscriptor, el cual intercepta y redirecciona la solicitud *http* hacia el *Radius* Global, el cual a su vez reconoce el servicio de Internet solicitado y lo vuelve a redireccionar hacia el RADIUS LOCAL el cual cuenta con todos los datos del cliente para validar su *user y password* para poder acceder al servicio.

Si el *Radius* Local reconoce la solicitud del cliente como un USUARIO VALIDO, este Server envía de regreso un "*Accept Request*" y posterior a esta envía el perfil completo del cliente el cual incluye el tiempo de conexión máximo, el tiempo de desconexión máximo y el ancho de banda máximo asignado.

Con los parámetros anteriores asignados, el cliente puede hacer uso del servicio de acuerdo al perfil contratado; en caso de que el cliente no sea un USUARIO NO VALIDO, el equipo suscriptor a través del equipo WEB Server permite a este usuario tener acceso solo a paginas gratuitas configuradas en este, estas paginas gratuitas son generalmente las paginas de publicidad de la empresa que presta el servicio, este servicio configurado se le conoce como *Walled Garden.*

Entre todo este proceso funcional existe un proceso de seguridad entre el equipo suscriptor y el Web Server para levantar una sesión segura SSL.
Aunque ya se menciono, es importante resaltar que el equipo suscriptor lleva el control de la sesión con el perfil asignado por Prodigy Móvil.

Política 4B
Al recurso humano se le debe hacer de su conocimiento la clasificación de los equipos referente al nivel de criticidad de estos dentro de la red, para así brindarles una atención acorde a sus responsabilidades.

Política 4C
El recurso humano debe conocer los requerimientos de operación de los equipos que brindan el servicio, como son condiciones ambientales adecuadas en el cuarto de comunicaciones, ya que el rango de temperatura de operación de los equipos es entre 0 y 45 grados centígrados; además la gente debe identificar las etiquetas que muestran la ubicación de los interruptores de corriente y que de preferencia que cuenten con corriente eléctrica regulada e ininterrumpida en caso de fallas en el suministro de la corriente comercial.

Política 4D
El personal debe conocer las perspectivas de crecimiento del servicio.
"A nivel nacional, los accesos inalámbricos son un mercado con alto potencial de crecimiento dentro del mercado residencial, que esperan se acelere cuando las autoridades nacionales establezcan a detalle las condiciones para la operación de las redes de cobertura metropolitana de alta velocidad, conocidas como *WiMax*, comentó el especialista en telecomunicaciones de la consultora IDC, Alejandro Valdez." [CHA-05]

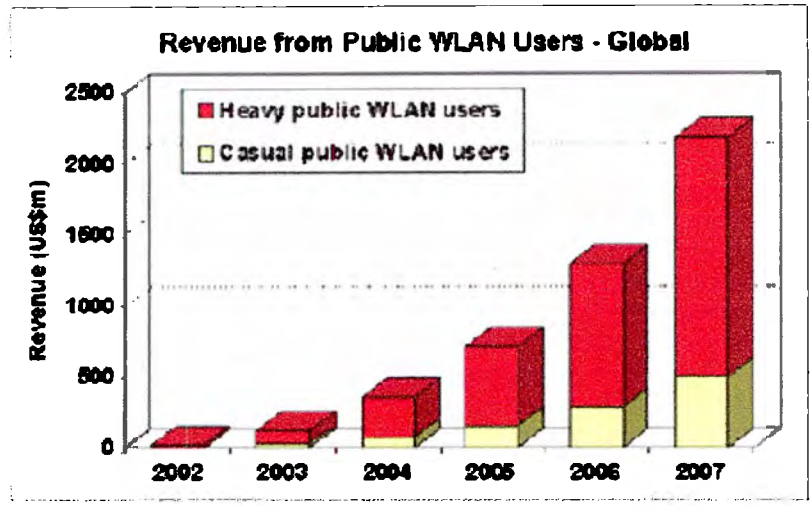


Figura 4.2. Perspectivas de crecimiento global del servicio inalámbrico. [MIM-05]

Política 4E
Al recurso humano se le debe valorar la importancia de su trabajo y los beneficios que aporta cuando lo realiza correctamente, reconocimientos vía correo corporativo en base a proyectos terminados, objetivos organizaciones cumplidos y metas alcanzadas.

No hay que olvidar que el recurso humano es la pieza clave del servicio y sobre del cual recae todo tipo de responsabilidad, por lo que las políticas que ayuden reforzar una adecuada supervisión y ejecución de las tareas en las que están involucradas las personas, deben ser evaluadas e implementadas en el menor tiempo posible con la inalidad de hacer mas fácil el trabajo y disminuir los riesgos de falla.

4.1.5. Seguridad física y del entorno

Los controles de acceso a los sitios *hot spot* deben ser manejados de manera simple y segura.

Política 5A
Se debe hacer llegar a los responsables de los sitios *hot spot* vía correo electrónico un listado del personal autorizado a permanecer dentro del *site* de comunicaciones únicamente con previa

identificación con gafete de la empresa. La lista a distribuir debe contener nombre completo de la persona autorizada, numero de empleado, área a la que pertenece, empresa a la que pertenece (para no excluir a los contratistas), Jefe inmediato, teléfono celular del jefe inmediato y periodo de vigencia. El correo electrónico debe ser dirigido a responsable del sitio *hot spot* y a un supervisor asignado.

Política 5B
El *site* de comunicaciones debe permanecer cerrado y únicamente podrá permitir el acceso el jefe en turno o por el supervisor asignado.

Política 5C
En caso de no permitirse al acceso a personal no considerado en la lista publicada, se deberá pedir autorización vía correo electrónico al menos del supervisor en turno del centro de operaciones de la red que monitorea los sitios *hot spot.*

Política 5D
El responsable en turno o supervisor del sitio *hot spot* no deberá permitir utilizar el *site* de comunicaciones como bodega general en donde pueda tener acceso algún extraño al negocio. En caso de que el *site* de comunicaciones sea compartido para otro fin, este deberá ser controlado internamente por el responsable del sitio *hot spot.*

"La integridad y seguridad de datos para cualquier software en el cuidado de la salud o para cualquier proveedor de servicios es absolutamente imprescindible," dijo Dan Peterson, presidente y CEO de Cereplex. Los "hospitales necesitan saber que la información que nos están transmitiendo sea totalmente segura. Nuestro compromiso con la seguridad, las mejores prácticas y el cumplimiento con ISO 27002, proporcionamos esa parte en la mente a nuestros clientes." [BUS-06]

La importancia de la seguridad física en los *hot spot* debe contemplar todo el ambiente sobre el cual se ofrece el servicio, ya que al resguardar la integridad física de todos los recursos asociados al servicio, se garantiza una de las partes esencial para asegurar la integridad de la información.

4.1.6. Control de acceso

Es muy importante proteger la conexión inalámbrica entre los equipos móviles y las antenas del sitio *hot spot* mediante la aplicación del procedimiento de configuración definido.

Política 6A
Los usuarios del servicio deben configurar su computadora para:
Obtener una dirección IP dinámica utilizando el protocolo DHCP.
Obtener una dirección de DNS automática.
Nombre del perfil: Prodigy
Nombre de la red inalámbrica SSID: prodigymovil
Modo de operación: Red (infraestructura)
Autenticación de redes: Abierta

Activar 802.1X: habilitado
Dominio: Dejar en blanco
Tipo de codificación de datos: CKIP
Proporcionar nombre de usuario y contraseña

"Tener una red inalámbrica significa que los usuarios no necesitan permanecer en su escritorio para estar conectados, les permite trabajar y ser igualmente productivos en cualquier lugar donde exista un hot spot que los conecte a la red, ya sea en un restaurante, librería o cualquier lugar público o privado que tenga este servicio." [CAR-05]

Política 6B

Se debe tener un sistema de autenticación robusto que impida tener acceso a las configuraciones de los equipos y sistemas que son accedidos por terceros, ya sea por asuntos de mantenimiento o actualizaciones.

4.1.7. Desarrollo y mantenimiento de sistemas

Política 7A
El proceso desarrollado para administrar la seguridad de la información en los sitios de acceso público a Internet deberá mantenerse actualizado bajo la responsabilidad de la Subgerencia de Seguridad.

"sin los estándares internacionales más altos sobre software de seguridad para Tecnologías de información, los mercados financieros del mundo no podrían funcionar de la manera que lo hacen. No importa que tan avanzados sean nuestros sistemas, somos siempre vulnerables. Desde que ADSM fue establecido, hemos estado constantemente de revisando y actualizando nuestros sistemas de seguridad en línea con nuestro crecimiento. Pero, para traer a nuestros sistemas hasta un estándar internacional necesitamos la certificación de la ISO 27002" [KHA-05]

Política 7B
La subgerencia de seguridad debe asegurarse que todos los desarrollos que se integren a la red no pongan en riesgo la seguridad de la información.

Política 7C
La subgerencia de seguridad debe mediante reuniones o boletines, concientizar a las áreas involucradas, la importancia de la seguridad de la información.

4.1.8. Administración de los incidentes de seguridad

Para llevar un control adecuado de los incidentes de seguridad relacionados a los sitios *hot spot* es necesario documentarlos en una bitácora que contenga los criterios necesarios y que deberá ser completada bajo la responsabilidad del subgerente o supervisor en turno del área del centro de control de operaciones de la red.

Política 8A
Para llevar un control adecuado de los incidentes relacionados a la seguridad los sitios *hot spot* es necesario documentarlos en una bitácora.

Política 8B
La subgerencia de seguridad debe preparar una estrategia de concientización dirigida a los responsables de los sitios hot spot y a las áreas operativas de la red inalámbrica, que resalte la importancia de llevar una control de los incidentes que se presentan.

Política 8C
La subgerencia de seguridad debe actualizar el formato de la bitácora y su contenido:
Fecha del Incidente.
Hora del Incidente.
Nombre de la persona que documento el incidente.
Nombre del sitio *hot spot* donde se presento el incidente
Descripción del Incidente.
Causa Probable del incidente.
Afectación provocada por el incidente.
Solución al incidente.
Incidente relacionado a otro caso.
Fecha y hora del cierre del incidente.

4.1 .9. Administración de la continuidad del negocio

Como se debe reaccionar frente a grandes fallos o desastres para dar continuidad al negocio:

Política 9A
Se debe tener desarrollado un plan de contingencia para saber como reaccionar frente a grandes fallos o desastres para dar continuidad al negocio.

Política 9B
El responsable del sitio *hot spot* debe nombrar a un responsable sustituto de sus actividades en todo momento.

Política 9C
Los equipos de comunicaciones deben estar conectados a un dispositivo que proporcione corriente ininterrumpida.

Política 9D

Se debe mantener el *site* de comunicaciones cerrado y bajo llave.

Política 9E
El *site* de comunicaciones debe estar alejado de fuentes de agua y no debe ubicarse bajo desnivel del suelo.

Política 9F
Las antenas instaladas en pared y techo se deben ubicar donde no sufran desperfectos naturales o intencionados.

"Al final todas las redes inalámbricas llegan a una infraestructura de cable, que permite llevar las comunicaciones de última milla hacia el centro de operaciones, que seguirán comunicándose por medio de cable de cobre o fibra óptica, el cual deberán soportar mayor tráfico y ser más resistente a las caídas del servicio, porque un mayor número de redes dependerá de un sólo cableado" [FUN-05]

4.1.10. Conformidad con la legislación

Política 10A
Se debe acatar la norma regulatoria del servicio inalámbrico en México. (121 SCT94) Anexo I.
"Dentro del paquete de licitaciones 2007 la Cofetel prevé las asignaciones de la banda 1.9 Gigahertz (GHz) tiene una disponibilidad de 30 megahertz en todas las regiones, excepto en la 8 que corresponde a los estados de Puebla, Tlaxcala, Veracruz, Oaxaca y Guerrero" [CHA-06]
Los espacios entre los 70-80 GHz, para ser utilizada para enlaces punto a punto y ofrece grandes capacidades para ayudar a establecer enlaces de banda ancha para redes locales. El espacio radioeléctrico de 1.7 a 2.1 GHz se empleará para servicios móviles de tercera generación o IMT-2000, que incluyen más características y aplicaciones, que demandan una mayor capacidad de espectro" [CHA-06]

Política 10B
Se debe respetar el contrato de trabajo de los empleados.

Política 10C
Se debe respetar la confidencialidad de la información.

Política 10E
Se debe respetar la privacidad de las personas.

4.2. Resultados de la encuesta a clientes de los sitios *hot spot* acerca de las políticas de seguridad desarrolladas de acuerdo al estándar ISO-27002

Teniendo desarrolladas las políticas de seguridad a las que se deben apegar los sitios *hot spot*, lo que resta definir es la prioridad de implantación de estas, de acuerdo a la experiencia de los clientes en el uso del servicio inalámbrico publico y a la opinión de los responsables de los sitios *hot spot*.

En este capítulo se presentarán los resultados de la experiencia del cliente para cada uno de los elementos que componen el estándar ISO 27002 y también se mostraran los resultados de las opiniones de los responsables de los sitios *hot spot*.

La encuesta aplicada se enfoca para que los clientes validen que es lo más importante para ellos cuando utilizan el servicio de Internet inalámbrico público y además conocer de parte de los administradores los sitios hot spot cuales son sus prioridades.

El estudio se aplicó a 57 usuarios del servicio y a 10 responsables de los sitios *hot spot*. La encuesta aplicada es mostrada en el apéndice A, la cual busco cubrir aspectos relacionados al servicio de Internet inalámbrico que se ofrece a los clientes actuales, para que a través de la experiencia que ellos tienen con el servicio, sirva para implementar los controles particulares.

4.2.1. Elemento de seguridad 1: Política de seguridad

Sobre este elemento del estándar, los clientes de los sitios *hot spot* expresan que requieren que el proveedor del servicio de Internet inalámbrico se comprometa para que las cuentas de acceso al servicio sean administradas correctamente, en el sentido de que ninguna persona que no posea una cuenta de acceso otorgada por el proveedor pueda llegar a utilizar los recursos de la red *hot spot*.

Por otro lado, los clientes están de acuerdo en configurar sus dispositivos móviles de acuerdo como el proveedor del servicio les indique, con la finalidad de que se garantice una mayor seguridad de la información y también esperan que el proveedor del servicio se encargue de vigilar la correcta aplicación de las políticas establecidas, así como el hecho de fomentar su uso a nivel global, es decir, que los empleados, clientes, proveedores y todas las personas relacionadas con el servicio las conozcan y apliquen.

Los clientes no consideran importante el área de cobertura de la señal, principalmente porque dentro del sitio hot spot, se colocaran las antenas necesarias para que en cada espacio destinado al cliente se tenga la calidad de señal adecuada, y tienen razón ya que esto se contempla por el proveedor del servicio desde el diseño de la red en cada *hot spot*.

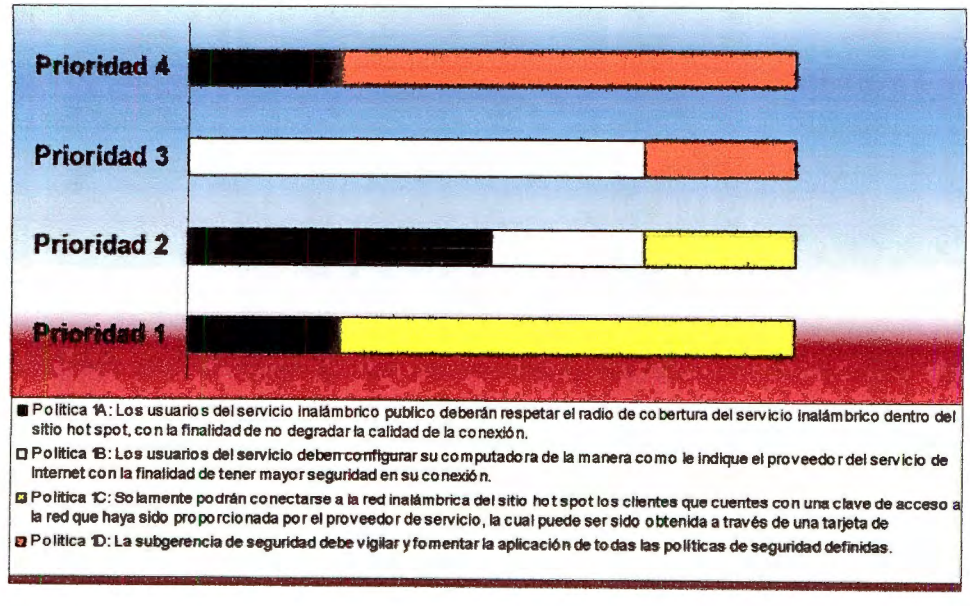


Figura 4.3. Resultado cuantitativo de los controles de la política de seguridad.

4.2.2. Elemento de seguridad 2: Aspectos organizativos de la seguridad

Los clientes de los sitios *hot spot* están de acuerdo y le dan mucha importancia al hecho de que el proveedor del servicio garantice que el sistema les muestre al iniciar su conexión a la red inalámbrica, el mensaje de invitación del porque deben configurar su dispositivo móvil y como lo deben de hacer.

Los clientes indican que no esperan que se instalen anuncios en donde se de a conocer el radio de cobertura de la señal inalámbrica, ya que es responsabilidad del proveedor del servicio entregar la señal en las áreas destinadas al cliente, los clientes saben que en áreas lejanas o externas al hot spot la calidad de la señal no es responsabilidad el proveedor del servicio.

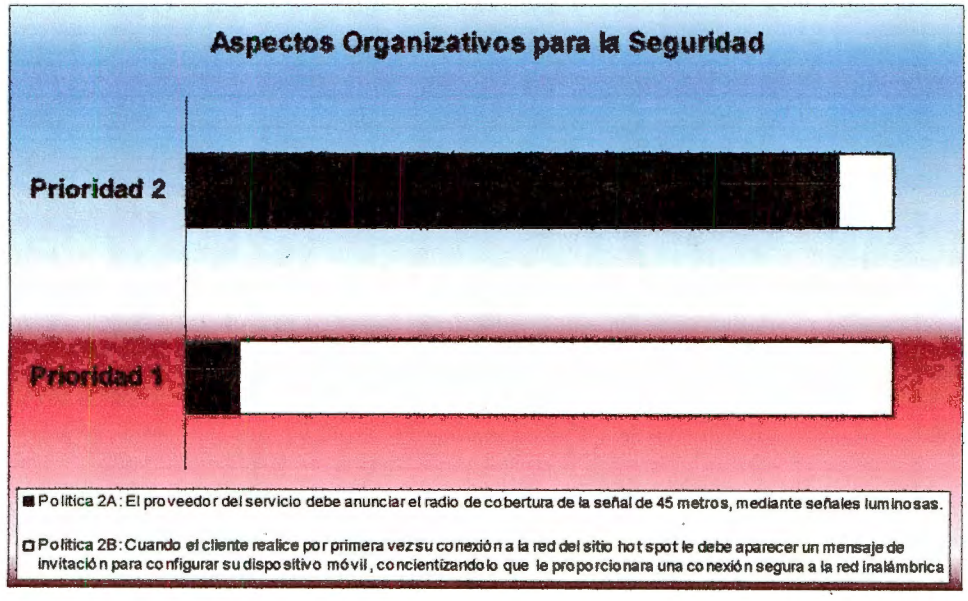


Figura 4.4. Resultado de los controles relacionados al aspecto organizativo de la seguridad.

4.2.3. Elemento de seguridad 3: Control y clasificación de los activos

Los clientes de los sitios *hot spot* esperan que el proveedor del servicio se asegure de proteger adecuadamente los activos que forman parte de la red inalámbrica, ya que de estos depende completamente el servicio que se les otorga, También los clientes marcan como aspecto importante determinar la criticidad de cada activo de la red inalámbrica con la finalidad de que se le de el cuidado especifico requerido.

Aunado a lo anterior los clientes no consideran un punto crítico la revisión de la obsolescencia de los activos de la red inalámbrica, aunque es necesario considerar el papel que juega cada uno de ellos en el servicio, para realizar esta revisión de manera periódica.

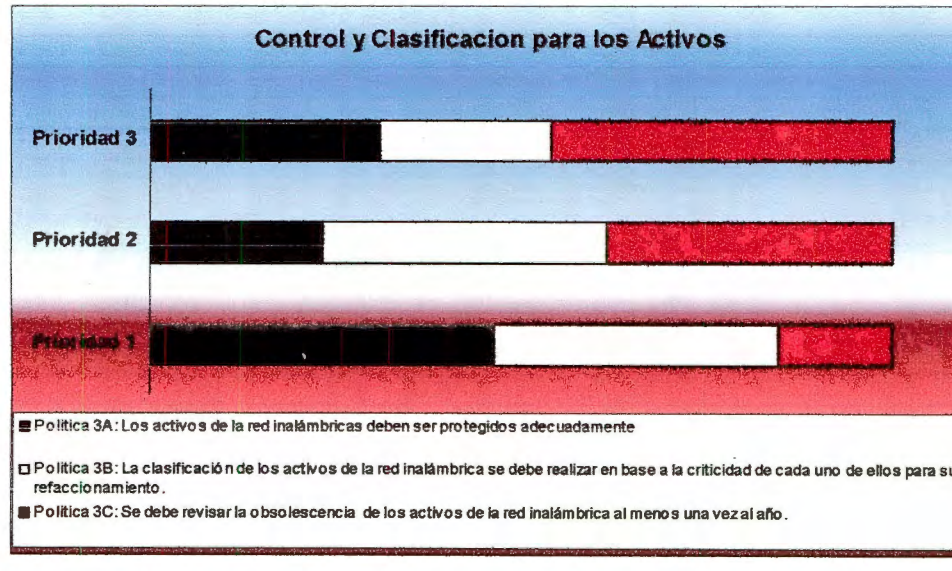


Figura 4.5. Resultados relacionados al control y clasificación de los activos.

4.2.4. Elemento de seguridad 4: Seguridad relacionada a los recursos humanos

Los clientes de los sitios *hot spot* esperan que el recurso humano que interactúa con el servicio de Internet publico inalámbrico tenga los conocimientos básicos del funcionamiento del servicio así como la topología básica que lo compone.

Los usuarios de los sitios *hot spot* piden al proveedor del servicio que el recurso humano involucrado en la prestación del servicio conozca los requerimientos básicos de operación de los equipos y también esperan que las personas relacionadas al servicio publico inalámbrico conozca el nivel de criticidad de los equipos con la finalidad de conocer la prioridad de atención que se le debe dar a cada uno y quien es el responsable de dársela.

Los clientes de los sitios *hot spot* califican de baja importancia el hecho de que los empleados deben conocer las perspectivas de crecimiento del servicio para así ellos conozcan el valor que le aporta a este para aumentar su crecimiento y demanda y tampoco valoran de gran manera la importancia de reconocer el trabajo del recurso humano que esta involucrado alrededor del servicio.

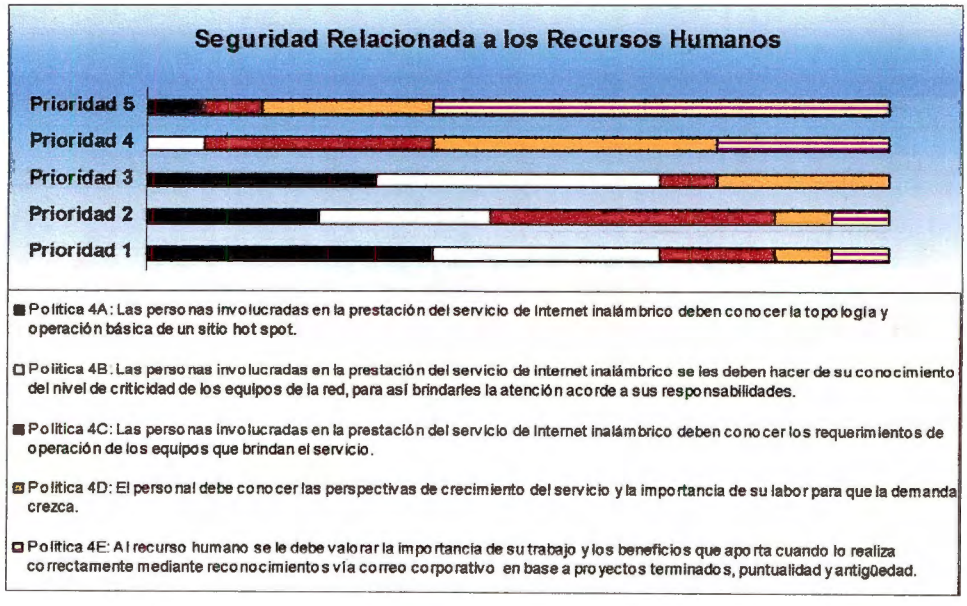


Figura 4.6. Resultados de las políticas de seguridad relacionadas al recurso humano.

4.2.5. Elemento de seguridad 5: Seguridad física y del entorno

Los clientes de los sitios *hot spot* consideran que el *site* de comunicaciones debe permanecer cerrado y el acceso a este debe estar plenamente controlado por el responsable del negocio donde se encuentra ubicado el *hot spot*, también califican como punto importante el notificar a los responsables de los *hot spot* la lista de personas autorizadas para acceder al *site* de comunicaciones por razones de mantenimiento del servicio.

Los clientes ven importante que en caso de que la persona que requiere tener acceso al *site* de comunicaciones y no se encuentre en la lista preautorizada sea solicitada la autorización de acceso a los supervisores del centro de operación de la red inalámbrica, ya que seguramente si ellos lo autorizan es porque existe algún mantenimiento programado.

Los clientes de acuerdo a sus opiniones no le dan demasiada importancia al hecho de que el *site* de comunicaciones sea utilizado como bodega.

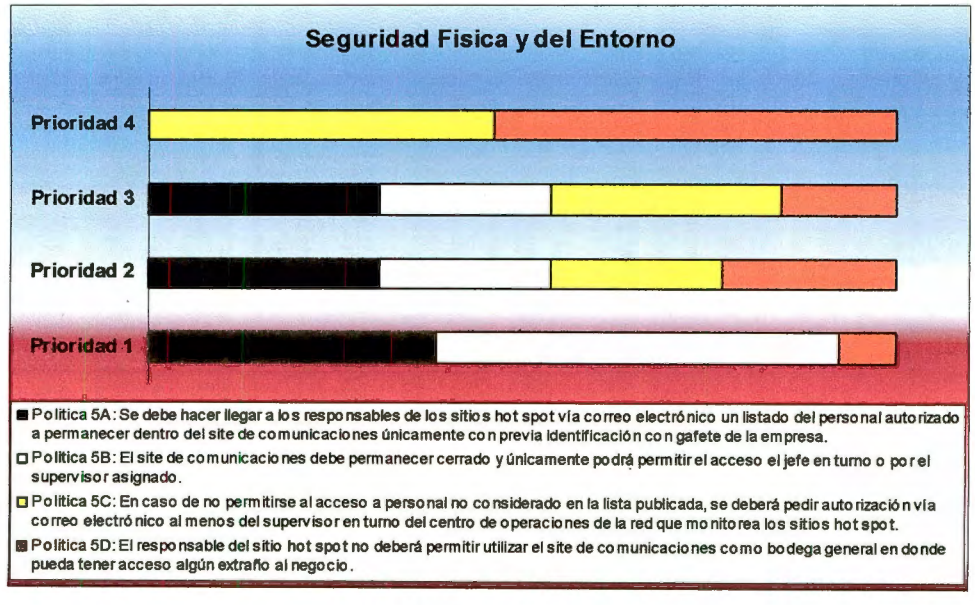


Figura 4.7. Resultados de los controles de la seguridad física y del entorno.

4.2.6. Elemento de seguridad 6: Control de acceso

Los usuarios del servicio inalámbrico público están concientes de que el proveedor del servicio debe tener un sistema de autenticación robusto para acceder a los recursos de la red inalámbrica y le dan una menor prioridad a la seguridad de la conexión inalámbrica entre el dispositivo móvil y la antena del servicio inalámbrico.

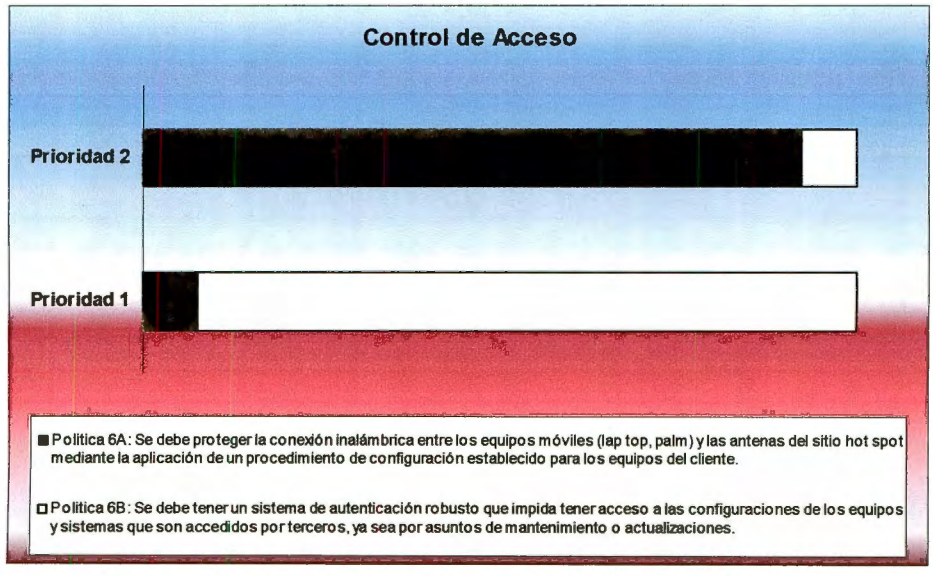


Figura 4.8. Resultados de la seguridad del control de acceso.

4.2.7. Elemento de seguridad 7: Desarrollo y mantenimiento de sistemas

Los clientes del *hot spot* están de acuerdo en que la subgerencia de seguridad es el área responsable de parte del proveedor del servicio de actualizar el proceso de seguridad desarrollado, también consideran que esta subgerencia de seguridad sea la responsable de asegurarse que los nuevos desarrollos que se integren a la red, no pongan en riesgo la seguridad de la información y aunado a lo anterior indican que también debe ser la responsable de concientizar a las áreas involucradas en el servicio de Internet inalámbrico de la importancia que tiene aumentar y mantener la seguridad de la información.

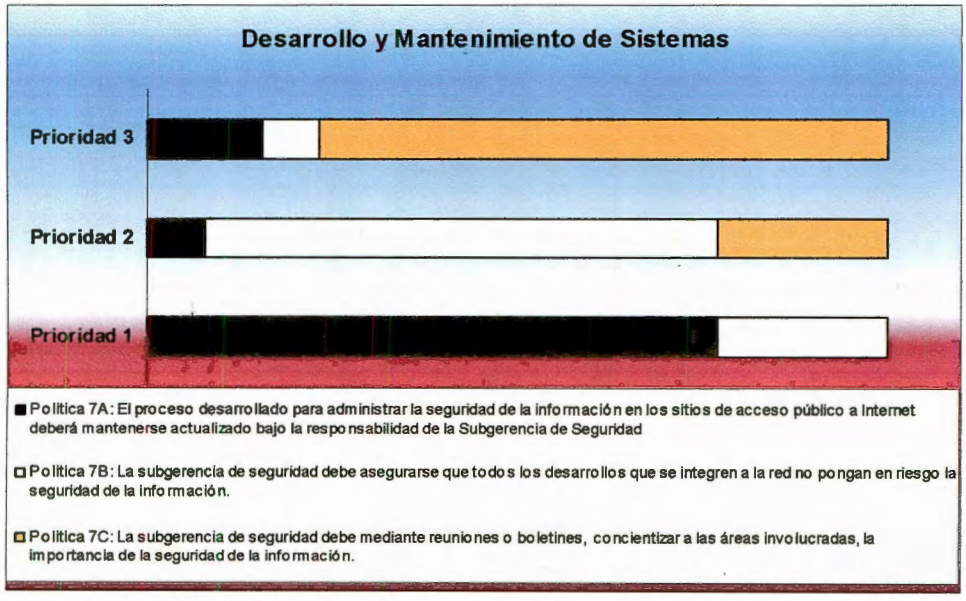


Figura 4.9. Resultados relacionados al desarrollo y mantenimiento de sistemas.

4.2.8. Elemento de seguridad 8: Administración de los incidentes de seguridad

La mayoría de los clientes de los sitios *hot spot* coinciden en que es importante documentar en una bitácora los incidentes de seguridad que se presenten, así como que la subgerencia de seguridad es la que se debe de encargar de definir y mantener actualizado el formato a llenar, así como encargarse de preparar y aplicar una estrategia de concientización dirigida a las áreas usuarias de la importancia de llevar y mantener una bitácora de los incidentes de seguridad.

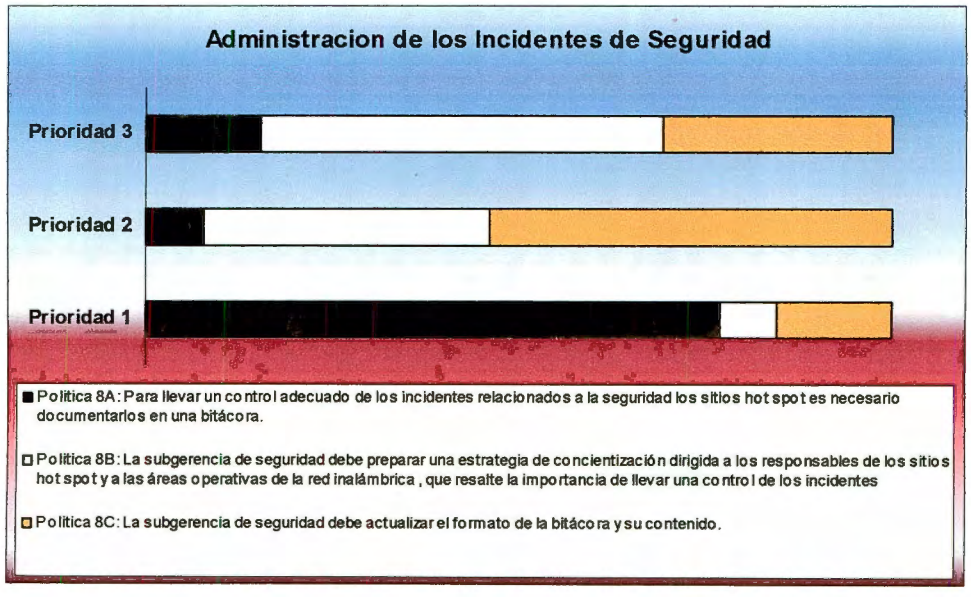


Figura 4.10. Resultados relacionados a la administración de los incidentes de seguridad.

4.2.9. Elemento de seguridad 9: Administración de la continuidad del negocio

En general los clientes de los sitios *hot spot* consideran importante que deba existir un plan de contingencia para que el personal involucrado en la prestación del servicio conozca cono reaccionar en caso de fallos grandes o desastres.

También los clientes coinciden en la importancia de tener los equipos de comunicaciones del sitio alimentados por corriente ininterrumpida y ven la importancia de mantener el *site* de comunicaciones cerrado y bajo llave. Para los clientes no tiene mayor importancia la ubicación de las antenas, ya que consideran que el proveedor realizo su trabajo de ingeniera correctamente.

Los usuarios del servicio no le dan importancia al hecho de que el administrador del negocio nombre un responsable sustituto en el sitio en caso de que el titular no este, y tampoco les importa el lugar físico en donde se encuentre ubicado el *site* de comunicaciones dentro del negocio.

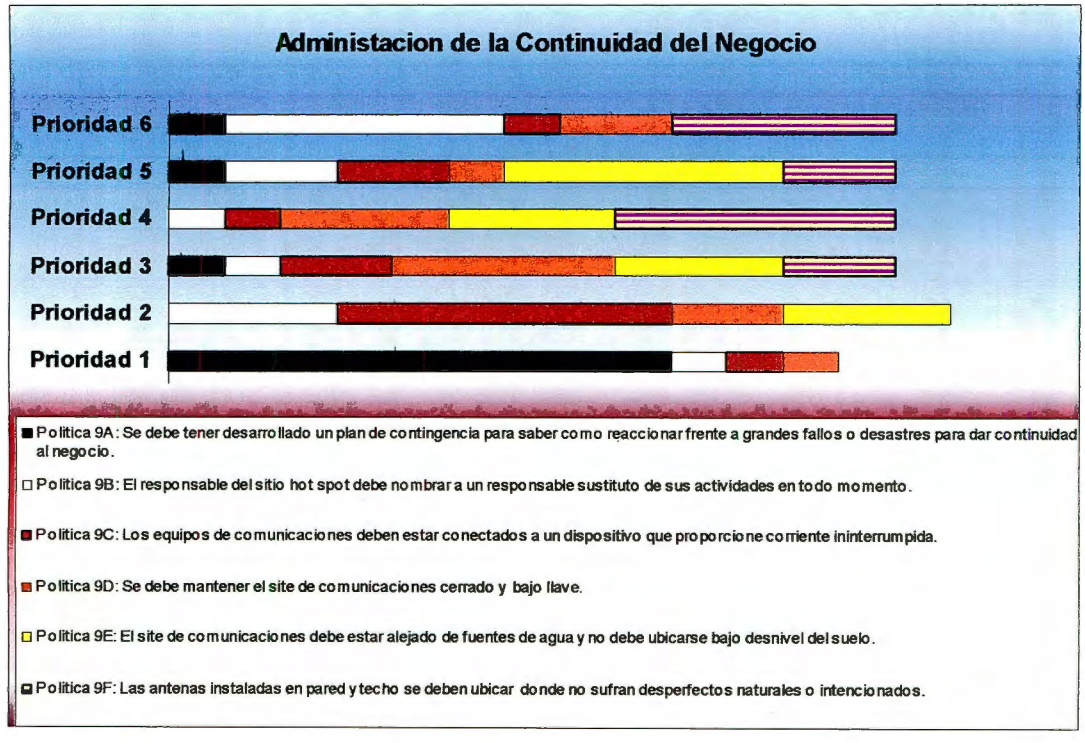


Figura 4.11. Resultados relacionados a la administración de la continuidad del negocio.

4.2.10. Elemento de seguridad 10: Conformidad con la legislación

Los clientes de los sitios *hot spot* coinciden en que lo mas importante es acatar la legislación relacionada a las comunicaciones inalámbricas y que rige la SCT, también consideran importante el que se respete la confidencialidad de la información que se intercambia a través de estos sitios.

También los usuarios indican que se debe respetar la privacidad de las personas que intercambian información a través de estos sitios y lo que si consideran pero como ultima prioridad es el que se respete el contrato laboral de los empleados relacionados al servicio publico de Internet inalámbrico.

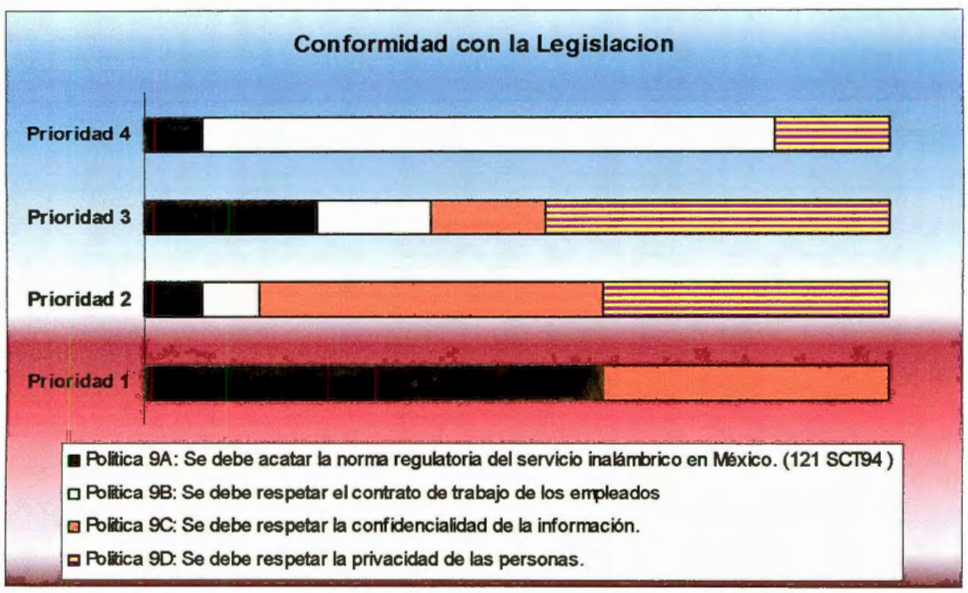


Figura 4.12. Resultados relacionados a la conformidad con la legislación.

4.3. Resultados de la encuesta a los responsables de los sitios *hot spot* acerca de las políticas de seguridad desarrolladas de acuerdo al estándar ISO-27002

La encuesta propuesta no se aplico totalmente a los responsables de los sitios hot spot, ya que existen elementos particulares del estándar que para ellos no son relevantes y que incluso ni se enteran, debido a que son responsabilidad total del proveedor del servicio.
Los controles excluidos de esta encuesta se determinaron al momento de aplicarla.

4.3.1. Elemento de seguridad 1: Política de seguridad

Los responsables de los sitios *hot spot* están de acuerdo en que los accesos a la red inalámbrica sean controlados estrictamente, en el sentido de que ellos realizan la venta de las tarjetas prepagadas en el negocio, también consideran importante el área de cobertura de la señal, principalmente para que dentro del sitio hot spot se tenga un área especifica en donde se pueda ofrecer este servicio, que por ejemplo en el área de restaurante, ya que en existen áreas en donde no se considera adecuado permitirlo.

Para los responsables de los sitios *hot spot* la seguridad de la información no tiene mucha importancia para ellos, ya que su negocio es otro, aunque consideran que el intercambio de información de cualquier manera debe ser de la manera más segura.

También para los gerentes de los sitios *hot spot*, opinan que si el proveedor del servicio le interesa que sus clientes tengan seguridad en su información, entonces el proveedor es el que se debe de encargar de vigilar la correcta aplicación de las políticas establecidas.

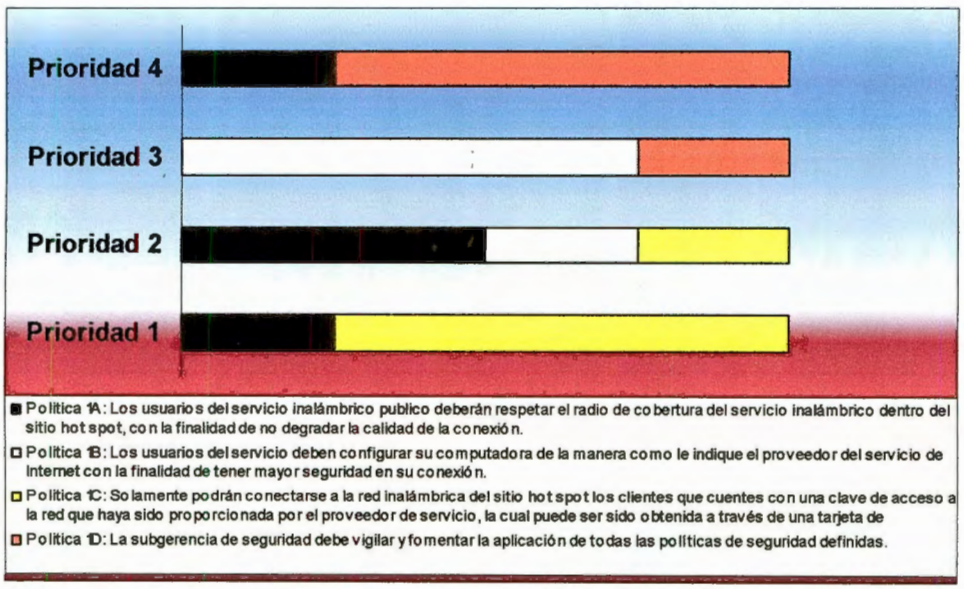


Figura 4.13. Resultado de la encuesta referente a la política de seguridad.

4.3.2. Elemento de seguridad 2: Aspectos organizativos de la seguridad

Los responsables de los *hot spot* esperan que se instalen anuncios en donde se de a conocer el limite de cobertura de la señal inalámbrica, con la finalidad de tener espacios exclusivos para los cibernautas y se invadan áreas inapropiadas.

Los responsables de los sitios *hot spot* están de acuerdo al hecho de que el proveedor del servicio les muestre a los clientes al iniciar su conexión a la red inalámbrica el mensaje de invitación para concientizarlos del porque deben configurar su dispositivo móvil, que aunque finalmente a ellos no les beneficia en su posición como responsables, si es importante cuando ellos llegaran a jugar el papel de un cliente.

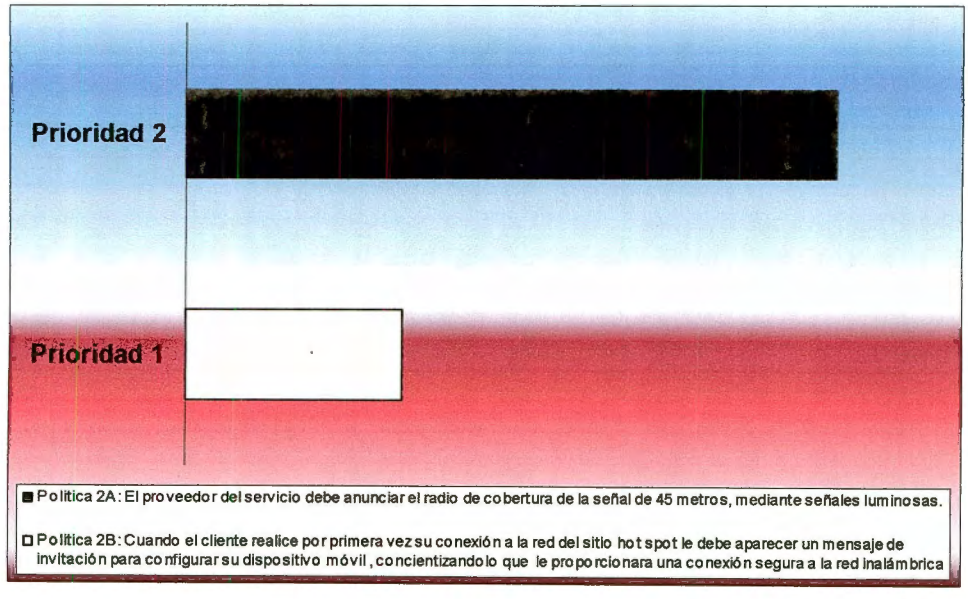


Figura 4.14. Resultado de los controles relacionados al aspecto organizativo de la seguridad.

4.3.3. Elemento de seguridad 3: Control y clasificación de los activos

Para los responsables es una medida importante el tener un control de los activos para dar mayores probabilidades de que el servicio opere adecuadamente, ya que protegiendo los equipos asociados al servicio, se garantiza en mayor porcentaje que los clientes realicen sus actividades programadas, lo cual se refleja en que disfruten de su estancia en el lugar y regresen pronto.

Tampoco ellos perciben el nivel de criticidad de cada activo de la red inalámbrica, aunque saben que es importante que se tome en cuenta, así como la obsolescencia de los equipos no representa una prioridad alta, pero están concientes que es algo importante que el proveedor del servicio debe tener en cuenta.

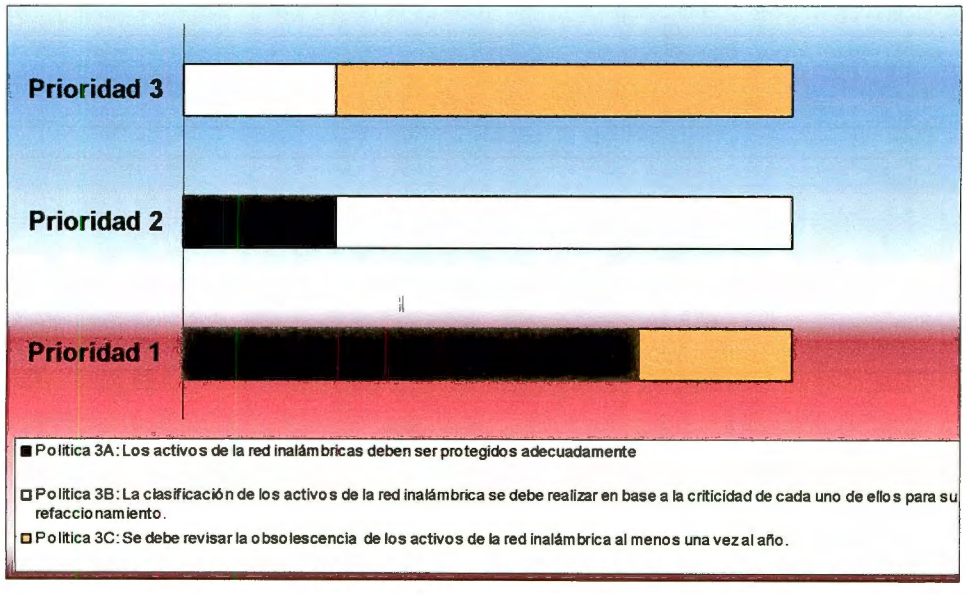


Figura 4.15. Resultados relacionados al control y clasificación de los activos.

4.3.4. Elemento de seguridad 4: Seguridad relacionada a los recursos humanos

Los responsables de los *hot spot* coinciden en que el personal involucrado en la prestación del servicio debe conocer la operación de los equipos, así como que el recurso humano que interactúa con el servicio de Internet público inalámbrico tenga los conocimientos necesarios del servicio para poder decidir como resolver el problema.

Los administradores mencionan que es responsabilidad directa del proveedor del servicio el punto de asegurarse que su personal conozca el nivel de criticidad de los equipos, ellos simplemente se limitan a reportar fallas del servicio, sin realizar ninguna revisión ya que ellos esta demasiado ocupados con sus verdaderas responsabilidades.

También ven mas como un asunto de mercadotecnia, más que de seguridad de la información, el hecho de que los empleados conozcan las perspectivas de crecimiento del servicio.

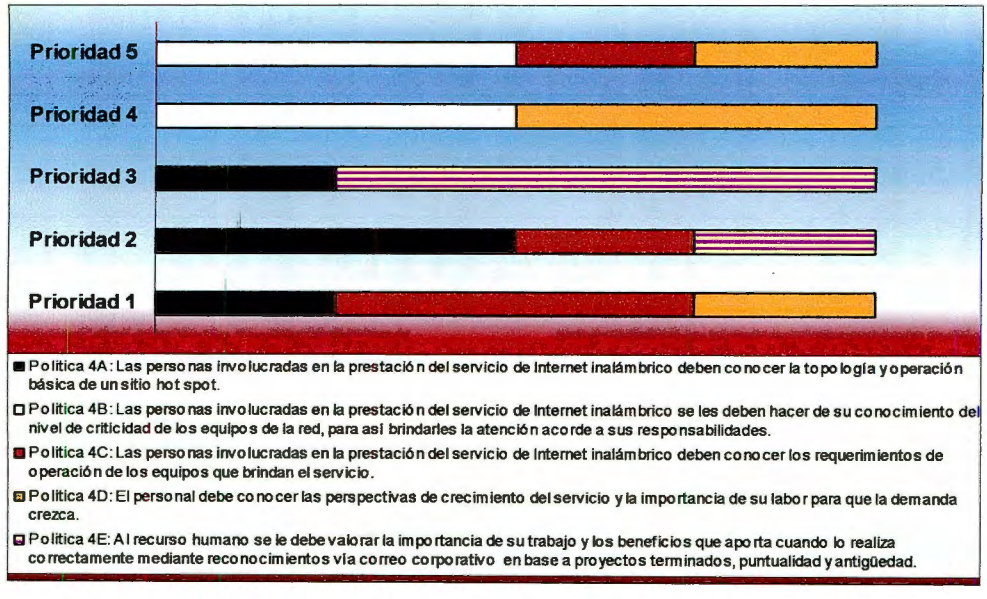


Figura 4.16. Resultados de las políticas de seguridad relacionadas al recurso humano.

4.3.5. Elemento de seguridad 5: Seguridad física y del entorno

Los encargados del negocio donde se encuentra el sitio *hot spot* concuerdan en la importancia de mantener el *site* de comunicaciones cerrado y el acceso a este debe estar plenamente controlado.

Los gerentes del negocio donde esta co-ubicado el *hot spot* coinciden en que el *site* de comunicaciones no sea utilizado como bodega, aunque en algunos casos el espacio del negocio es reducido, lo cual complica destinar un espacio único y aislado de algún área importante y necesaria del lugar, también consideran importante que cualquier persona que requiera tener acceso al *site* de comunicaciones deberá identificarse plenamente y deberá traer consigo alguna orden de trabajo autorizada por el área responsable de proveer del servicio.

Un punto que no reflejo ser tan importante es notificar a los responsables de los sitios *hot spot* la lista de personas autorizadas para acceder al *site* de comunicaciones por razones de mantenimiento del servicio, ya que ellos regularmente no tienen acceso a alguna cuenta de correo electrónico, por lo que regularmente ellos autorizan la entrada el *site* de comunicaciones al identificarse como se menciono en el punto anterior.

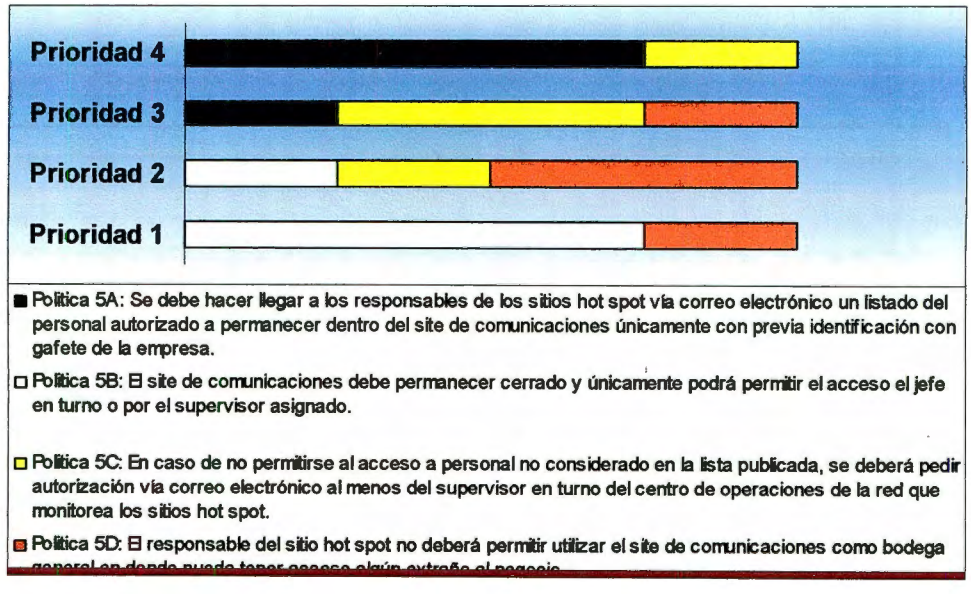


Figura 4.17. Resultados de los controles de la seguridad física y del entorno.

4.3.6. Elemento de seguridad 8: Administración de los incidentes de seguridad

Los encargados de los sitios *hot spot* opinan que debe ser responsabilidad total del proveedor del servicio llevar una bitácora de incidentes, ya que para ellos no es tan perceptible conocer cada estado de la red, además de que sus responsabilidades no les da tiempo de controlar este registro.

También ven como responsable a la subgerencia de seguridad la que se debe de encargar de definir y actualizar el formato y el contenido de la bitácora para el registro de los incidentes de seguridad, ya que finalmente ellos la utilizaran para mejorar el servicio.

Adicionalmente mencionan que aunque para su trabajo no tiene un impacto directo, consideran que la subgerencia de seguridad es la que debe de preparar y aplicar una estrategia para concientizar a las áreas usuarias, así como la importancia de llevar y mantener la bitácora de los incidentes de seguridad.

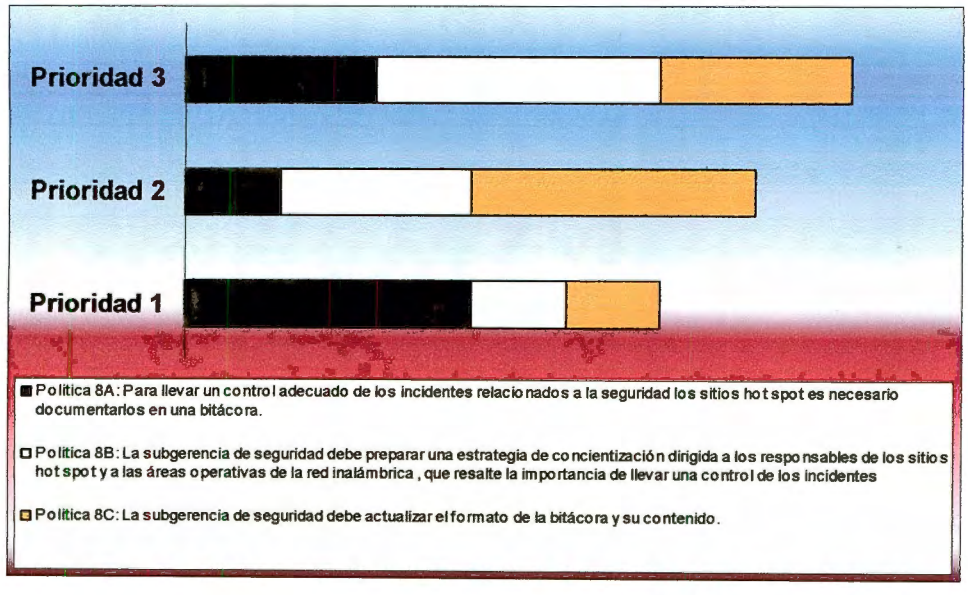


Figura 4.18. Resultados de la administración de los incidentes de seguridad.

4.3.7. Elemento de seguridad 9: Administración de la continuidad del negocio

Para los encargados del negocio donde se encuentra el *hot spot* es importante siempre tener un responsable sustituto en el sitio en caso de que él se ausente, ya que sus tareas lo requieren.

Los responsables están concientes en que un punto importante para mantener la continuidad del negocio el mantener el *site* de comunicaciones cerrado y bajo llave, también consideran importante la existencia de un plan de contingencia, así como la importancia de tener los equipos de comunicaciones del sitio alimentados por corriente ininterrumpida; A lo que no le dan mucha importancia es al lugar físico en donde se encuentre ubicado el *site* de comunicaciones dentro del *hot spot*, simplemente que lo haya..

También expresan que las antenas instaladas en los sitios las ubica el proveedor en donde él lo considere conveniente, de acuerdo a su estudio previo de cobertura, simplemente ellos cuidan que no bloqueen algún punto estratégico del negocio.

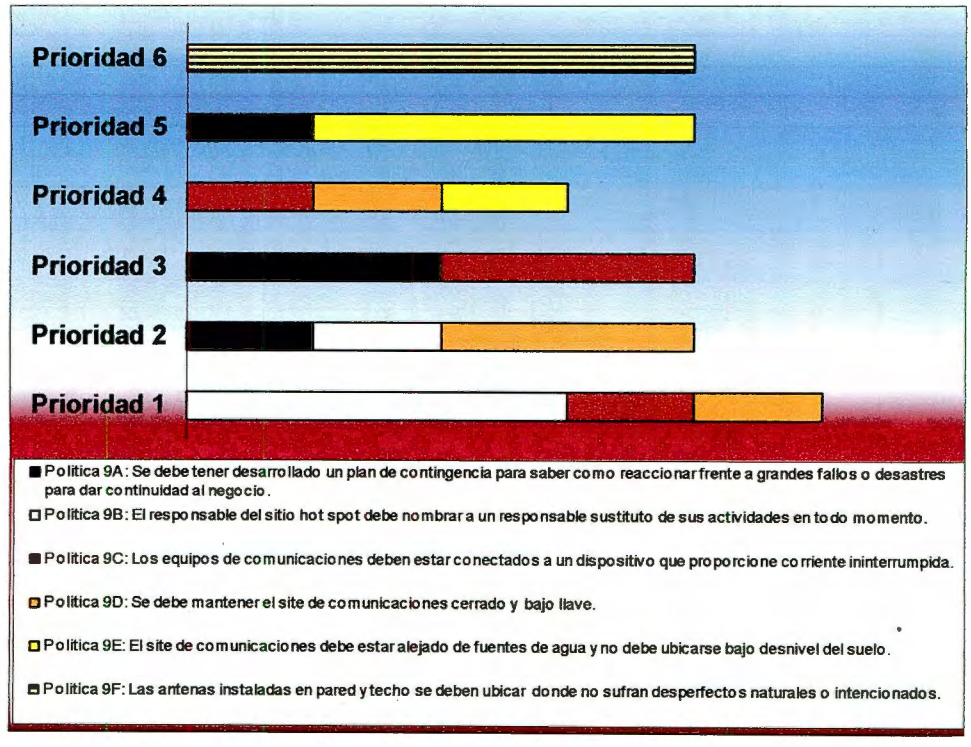


Figura 4.19. Resultados relacionados a la administración de la continuidad del negocio.

CAPÍTULO 5

Conclusiones

Primeramente se mencionarán algunas conclusiones concretas de las encuestas, para posteriormente dar las conclusiones generales del trabajo con respecto a que debe hacer o dejar de hacer el ISP para que la unidad de negocio del servicio inalámbrico sea rentable y de un valor agregado alto a los servicios que se ofrece.

Se comenzará por el resultado de la encuesta aplicada a los clientes de los sitios *hot spot*:

1. Reconocen que debe existir un compromiso de parte del proveedor del servicio para que exista una política de seguridad que garantice una estricta administración de las cuentas para acceder a los recursos de la red, lo cual debe ser considerado por el ISP con la finalidad de robustecer esta parte con la finalidad de tener a los clientes satisfechos y puedan permanecer cautivos en el uso del servicio.

2. Coinciden en su mayoría en que la empresa proveedora del servicio público de Internet inalámbrico cuente con políticas de seguridad, en las que esta dispuesto a formar parte, siempre y cuando estas sean difundidas por el área de seguridad de la empresa, para que están sean conocidas por todo el personal involucrado en el servicio.

3. Están dispuestos a formar parte de la política de seguridad con la finalidad de que la información que intercambian sea de manera segura, esto sin dejar fuera la responsabilidad de que el proveedor debe que vigilar la correcta aplicación de lo contenido en cada política de seguridad.

4. Están abiertos a cooperar en la seguridad de la información, siguiendo los lineamientos de seguridad que el proveedor les indique aplicar a sus dispositivos móviles, o sea que los aspectos organizativos de cómo mejorar la seguridad los indica el proveedor y los clientes están de acuerdo en aplicarlos.

5. Esperan que de forma natural el proveedor brinde el cuidado necesario a los activos de la red inalámbrica, para que estos se desempeñen de manera correcta y de acuerdo a sus funcionalidades, ya sean críticas o normales.

6. Exigen que el personal asignado a la atención de la red inalámbrica este capacitado para resolver cada contingencia de acuerdo a la clasificación del recurso afectado. Por otro lado los clientes no le dan gran importancia a la motivación que el proveedor del servicio de a sus empleados y esto podría frenar el crecimiento del servicio y el desarrollo de los empleados.

7. Le dan buen peso al sistema de autenticación para acceder a los equipos de la red y

definitivamente sobre este control de seguridad descansa la integridad de la información y recae totalmente en responsabilidad en el proveedor del servicio para que esto se proteja.

8. Identifican dentro de la estructura organizacional del ISP, una entidad exclusiva y responsable de la seguridad de la información, por lo que el ISP debe tomar en cuenta la importancia de las responsabilidades que recaen sobre esta área, por lo que debe justificarse de manera clara la existencia y la inversión que se haga en esta área.

9. Coinciden en el hecho de documentar los incidentes de la red, lo cual permitiría resolver problemas recurrentes de manera más rápida y también documentar casos aislados que pudieran evitarse en otro tiempo.

10. Concuerdan en que se deben respetar las leyes asociadas a la red inalámbrica, así como respetar acuerdos de confidencialidad de la información que pudieran generarse con el proveedor del servicio.

Ahora se analizaran los resultados de la encuesta aplicada a los responsables o administradores de los sitios hot spot con respecto a las políticas de seguridad desarrolladas para cuidar la confidencialidad, disponibilidad e integridad de la información:

I. Resulta importante resaltar que desde el punto de vista de los administradores, las necesidades con respecto a la seguridad de la información no son las mismas que para los clientes, de hecho son muy diferentes, ya que los administradores no ven la necesidad de la seguridad de la información como tal, sino que ven la parte de la seguridad solo como un servicio. Por lo anterior, de las políticas desarrolladas para algunos elementos de control del estándar varias no fueron consultadas con los administradores del hot spot, ya que ellos lo mencionaron, no tienen ningún marco referencia para opinar del porque algunas políticas serian mas importantes que otras.

II. Para los responsables de los sitios hot spot es muy importante que solo puedan acceder a la red inalámbrica los clientes autorizados por el proveedor del servicio, ya sea a través de un contrato o por medio de una tarjeta prepagada, por el hecho de que en el negocio donde se ubica el hot spot se realiza la venta de estas tarjetas de prepago.

III. También otro punto de vista de las políticas de seguridad es la cobertura de la señal inalámbrica, ya que para los responsables de los negocios si es muy importante que se establezcan estos limites, ya que solo así ellos pueden restringir lugares dentro del sitio que no son adecuados para que un cliente se estacione para estar navegando en Internet.

IV. Los administradores no saben y tampoco están interesados en conocer cual es la criticidad de cada uno de los equipos, pero lo que ellos si valoran es que el proveedor del servicio tome en cuenta esta clasificación, ya que esto se refleja en ofrecer un mejor servicio. También los administradores están concientes de que el personal involucrado el la prestación del servicio inalámbrico debe conocer la operación básica de los equipos de la red inalámbrica, ellos no se ven como personal involucrado en el servicio de Internet, ellos se ven únicamente como responsables del negocio y solo se encargan de pasar los reportes

de los clientes al proveedor del servicio respecto al servicio de Internet.

V. Los responsables de los sitios hot spot reconocen y toman en cuenta la seguridad física del *site* de comunicaciones, que aunque en ocasiones esta co-ubicado con otra área, ellos reconocen que es importante controlar al acceso, ya que finalmente esta dentro de sus instalaciones. También ellos consideran importante dejar un sustituto en caso de la ausencia del titular, aunque esto lo ven mas por sus responsabilidades dentro del negocio, que para atender cualquier contingencia del servicio inalámbrico.

Así, considerando los puntos de vista de los clientes y administradores de los sitios hot spot se concluye en los siguientes puntos, los cuales debe tomar en cuenta el proveedor del servicio público de acceso inalámbrico a Internet.

a. Se detecta como área de oportunidad el hecho de que los clientes están de acuerdo en hacer un frente común con el proveedor del servicio, para robustecer la seguridad del servicio inalámbrico.

b. El proveedor del servicio debe invertir recursos para involucrar a los responsables de los negocios en hacerlos concientes del valor agregado que les brinda ofrecer el servicio inalámbrico.

c. El proveedor del servicio debe revisar como esta trabajando el área dedicada a la seguridad de la información, con el fin saber hacia donde están apuntando los objetivos de esta y si en verdad están trabajando sobre la seguridad de la información.

d. El proveedor del servicio debe estar conciente que sobre él descansan políticas de seguridad con responsabilidades bien claras y que debe atender, las cuales van relacionadas a los controles del estándar siguientes:

    - Control y clasificación de los activos de la red
    - Control de acceso
    - Administración de la continuidad del negocio
    - Administración de los incidentes de seguridad
    - Conformidad con la legislación

e. El área de seguridad del proveedor del servicio debe complementar las políticas desarrolladas, para que estas sean alineadas a las perspectivas de los clientes, incluso deben ser incluidos en ellas como responsables de tareas que les tocaría realizar, si son concientes de la importancia de la seguridad de la información que intercambian en la red inalámbrica.

Apéndice A

Resumen de la norma oficial que rige las banda de frecuencia de *Wi Fi* en México

SCT. Norma Oficial Mexicana Emergente: NOM-EM-121-SCT1-1994
Instalación y operación de sistemas de radiocomunicación que emplean la técnica de espectro disperso en las bandas de 902-928 MHz, 2450-2483.5 MHz y 5725-5850 MHz.
Con fecha del 11 de Noviembre de 1994, la Secretaria de Comunicaciones y Transportes emite la Norma Oficial Emergente 121 (NOM-EM-121-SCT1-1994).

Introducción
El espectro disperso, es una técnica de transmisión en la cual los datos de interés ocupan un ancho de banda mayor del mínimo necesario para enviar tales datos. La dispersión del espectro se logra antes de transmitir la información a través del uso de un código que es independiente de la secuencia de datos. El mismo código es usado en el receptor (operando en sincronía con el transmisor) para comprimir la señal y así recobrar los datos originales.
Indican que se deben tener presente los artículos 124 y 125 del Reglamento de Telecomunicaciones de México, se hace alusión a los equipos para aplicaciones Industriales, Científicos y Médico [ICM (que no son de espectro disperso)] y, en particular, dichos equipos operan, entre otras, en las bandas de 902-928 MHz, 2400-2500 MHz y 5725-5875 MHz.
Por tanto, los equipos ICM que no son equipos de radiocomunicación, debido a que no transmiten información, deben convivir y ser protegidos, por parte de los sistemas de espectro disperso.
Los equipos ICM son dispositivos que producen una energía de radiofrecuencia, y que la utilizan internamente para generar efectos de tipo físico, mecánico, biológico y/o químico. Entre las aplicaciones ICM típicas tenemos las siguientes: Calefacción industrial en procesos de manufactura, diatermia médica terapéutica, aceleración de partículas cargadas, transductores electromecánicos para producir energía mecánica ultrasónica, humidificadores ultrasónicos domésticos, limpiadores domésticos de joyería. Por tanto, no es una telecomunicación.
Los equipos con técnica de espectro disperso son equipos de radiocomunicación que tienen aplicaciones internas (interiores de oficinas) y externas (intercomunicar edificios), dependiendo de la ocupación del espectro radioeléctrico en cada país.

Se identifican tres bandas de frecuencias factibles de operarse en México, siempre y cuando, cumplan con las regulaciones que se especifican en esta norma emergente. Tales bandas son 902-928 MHz, 2450-2483.5 MHz y 5725-5850 MHz.
La banda de frecuencias de 2400-2500 MHz está atribuida para los sistemas de espectro disperso. En México sólo se considera el segmento de 2450-2483.5 MHz como factible para la operación de esta clase de equipos. Lo anterior se debe a que la banda de 2300-2450 MHz se opera actualmente en México para sistemas de distribución múltiple de señales (enlaces punto-multipunto), para el servicio de telefonía en poblaciones rurales, cuyos repetidores se ubican en cerros altos a lo largo de nuestro país, y también, se aplica para la transmisión de datos dentro de

las ciudades más pobladas. Asimismo, la banda de 5725-5850 MHz puede ser utilizada para aplicaciones de espectro disperso.

Objetivo
La presente Norma va dirigida a la regulación de los sistemas de radiocomunicación que utilizan la técnica de espectro disperso en México.

Campo de aplicación
La técnica de espectro disperso es considerada como una tecnología clave en el desarrollo de las futuras redes de comunicaciones personales; las cuales se espera sean implantadas en esta década y tendrán un impacto directo en el campo de las telecomunicaciones a nivel internacional, particularmente en el área de las comunicaciones móviles, por lo que se espera que la normalización sea dinámica.

Área Local
Es un área de cobertura local, aquella en la que se pueden operar los equipos de espectro disperso usando una antena omnidireccional con una potencia radiada aparente (pra) máxima de 30 mWatts y/o un alcance máximo de 500 metros dentro de un mismo edificio.

Área Restringida
Es un área de cobertura restringida, aquella donde se utiliza una antena omnidireccional con una potencia radiada aparente de hasta un valor de 30 dBm, siempre y cuando las emisiones del usuario autorizado no se utilicen para enlazar equipos que impliquen el cruce de calles ni propiedades de terceros, por ejemplo: plantas industriales, centros comerciales, universidades, patios de carga y maniobras. Normalmente son enlaces no mayores de 500 metros que utilizan antenas omnidireccionales. Ocasionalmente se presentan casos que requieren enlazar equipos separados más de 500 metros utilizando para ello antenas direccionales.

Enlaces de Cobertura Amplia
Son aquellos enlaces punto a punto con una distancia entre extremos mayor a 500 metros, en donde se utilizan antenas direccionales, el alcance se determina con una potencia radiada aparente (pra) máxima de 36 dBm.

Especificaciones de transmisión aplicables a ambientes de operación en áreas locales (Bandas de 902-928 MHz, 2450-2483.5 MHz y 5725-5850 MHz).
Técnica de modulación de secuencia directa:
Ancho de banda de la señal transmitida: 500 kHz mínimo
Densidad de potencia en un segundo:< 8 dBm/3 kHz
Ganancia de procesamiento: 10 dB mínimo
Patrón de Radiación: Omnidireccional (para enlaces de hasta 500 metros)

Apéndice B

Encuesta aplicada

Esta en desarrollo un proceso de seguridad de la información para los sitios *hot spot*, el cual esta basado en el estándar ISO 27002. Cada elemento de este estándar esta compuesto por políticas especificas que se deben respetar con la finalidad de no comprometer la seguridad de la información.

Considerando su punto de vista y en orden de prioridad (la prioridad 1 es la más alta) como considera usted la importancia de implantación de cada una de las políticas para cada elemento del estándar.
Las prioridades no se deben repetir dentro del mismo elemento de control de la seguridad.

Elemento de Seguridad 1: Políticas de Seguridad:

Política 1.
Los usuarios del servicio inalámbrico publico deberán respetar el radio de cobertura del servicio inalámbrico dentro del sitio *hot spot*, con la finalidad de no degradar la calidad de la conexión.
Prioridad ( )

Política 2.
Los usuarios del servicio deben configurar su computadora de la manera como le indique el proveedor del servicio de Internet con la finalidad de tener mayor seguridad en su conexión.
Prioridad ( )

Política 3.
Solamente podrán conectarse a la red inalámbrica del sitio *hot spot* los clientes que cuentes con una clave de acceso a la red que haya sido proporcionada por el proveedor de servicio, la cual puede ser sido obtenida a través de una tarjeta de prepago o la realización de un contrato del servicio.
Prioridad ( )

Política 4.
La subgerencia de seguridad debe vigilar y fomentar la aplicación de todas las políticas de seguridad definidas.
Prioridad ( )

Elemento de Seguridad: Aspectos Organizativos para la Seguridad de los Sitios *hot spot*.

Política 5.

El proveedor del servicio debe anunciar el radio de cobertura de la señal de 45 metros, mediante señales luminosas.
Prioridad ( )

Política 6.
Cuando el cliente realice por primera vez su conexión a la red del sitio *hot spot* le debe aparecer un mensaje de invitación para configurar su dispositivo móvil utilizando el algoritmo de codificación sugerido por el proveedor del servicio, concientizandolo que este método de codificación le proporcionara una conexión segura a la red inalámbrica, protegiendo así la seguridad de la información que comenzara a intercambiar.
Prioridad ( )

Elemento de Seguridad 3: Clasificación y Control de los Activos.

Política 7.
Los activos de la red inalámbricas deben ser protegidos adecuadamente.
Prioridad ( )

Política 8.
La clasificación de los activos de la red inalámbrica se debe realizar en base a la criticidad de cada uno de ellos para su refaccionamiento.
Prioridad ( )

Política 9.
Se debe revisar la obsolescencia de los activos de la red inalámbrica al menos una vez al año.
Prioridad ( )

Elemento de Seguridad 4: Seguridad relacionada a los Recursos Humanos.

Política 10.
Las personas involucradas en la prestación del servicio de Internet inalámbrico deben conocer la topología y operación básica de un sitio *hot spot.*
Prioridad ( )

Política 11.
Las personas involucradas en la prestación del servicio de Internet inalámbrico se les deben hacer de su conocimiento la clasificación de los equipos referente al nivel de criticidad de estos dentro de la red, para así brindarles la atención acorde a sus responsabilidades.
Prioridad ( )

Política 12.
Las personas involucradas en la prestación del servicio de Internet inalámbrico deben conocer los requerimientos de operación de los equipos que brindan el servicio, como son condiciones

ambientales adecuadas en el cuarto de comunicaciones, interpretar etiquetado de los equipos.
Prioridad ( )

Política 13.
El personal debe conocer las perspectivas de crecimiento del servicio y que ellos son importantes para que la demanda crezca.
Prioridad ( )

Política 14.
Al recurso humano se le debe valorar la importancia de su trabajo y los beneficios que aporta cuando lo realiza correctamente mediante reconocimientos vía correo corporativo en base a proyectos terminados, puntualidad, antigüedad y capacitaciones.
Prioridad ( )

Elemento de Seguridad 5: Seguridad Física y del Entorno.

Política 15.
Se debe hacer llegar a los responsables de los sitios *hot spot* vía correo electrónico un listado del personal autorizado a permanecer dentro del *site* de comunicaciones únicamente con previa identificación con gafete de la empresa.
Prioridad ( )

Política 16.
El *site* de comunicaciones debe permanecer cerrado y únicamente podrá permitir el acceso el jefe en turno o por el supervisor asignado.
Prioridad ( )

Política 17.
En caso de no permitirse al acceso a personal no considerado en la lista publicada, se deberá pedir autorización vía correo electrónico al menos del supervisor en turno del centro de operaciones de la red que monitorea los sitios *hot spot*.
Prioridad ( )

Política 18.
El responsable en turno o supervisor del sitio *hot spot* no deberá permitir utilizar el *site* de comunicaciones como bodega general en donde pueda tener acceso algún extraño al negocio. En caso de que el *site* de comunicaciones sea compartido para otro fin, este deberá ser controlado internamente por el responsable del sitio *hot spot*.
Prioridad ( )

Elemento de Seguridad 6: Control de Acceso.

Política 19. Se debe proteger la conexión inalámbrica entre los equipos móviles (lap top, palm) y

las antenas del sitio *hot spot* mediante la aplicación de un procedimiento de configuración establecido para los equipos del cliente.
Prioridad ( )

Política 20. Se debe tener un sistema de autenticación robusto que impida tener acceso a las configuraciones de los equipos y sistemas que son accedidos por terceros, ya sea por asuntos de mantenimiento o actualizaciones.

Prioridad ( )

Elemento de Seguridad 7: Desarrollo y Mantenimiento de Sistemas.

Política 21.
El proceso desarrollado para administrar la seguridad de la información en los sitios de acceso público a Internet deberá mantenerse actualizado bajo la responsabilidad de la Subgerencia de Seguridad
Prioridad ( )

Política 22.
La subgerencia de seguridad debe asegurarse que todos los desarrollos que se integren a la red no pongan en riesgo la seguridad de la información.
Prioridad ( )

Política 23.
La subgerencia de seguridad debe mediante reuniones o boletines, concientizar a las áreas involucradas, la importancia de la seguridad de la información.
Prioridad ( )

Elemento de Seguridad 8: Administración de los Incidentes de Seguridad.

Política 24.
Para llevar un control adecuado de los incidentes relacionados a la seguridad los sitios *hot spot* es necesario documentarlos en una bitácora.
Prioridad ( )

Política 25.
La subgerencia de seguridad debe preparar una estrategia de concientización dirigida a los responsables de los sitios *hot spot* y a las áreas operativas de la red inalámbrica , que resalte la importancia de llevar una control de los incidentes que se presentan.
Prioridad ( )

Política 26.
La subgerencia de seguridad debe actualizar el formato de la bitácora y su contenido.
La bitácora de incidentes de Seguridad debe contener:

Fecha del Incidente.
Hora del Incidente.
Nombre de la persona que documento el incidente.
Nombre del sitio *hot spot* donde se presento el incidente
Descripción del Incidente.
Causa Probable del incidente.
Afectación provocada por el incidente.
Solución al incidente.
Incidente relacionado a otro caso.
Fecha y hora del cierre del incidente.
Prioridad ( )

Elemento de Seguridad 9: Administración de la continuidad del negocio.

Política 27.
Se debe tener desarrollado un plan de contingencia para saber como reaccionar frente a grandes fallos o desastres para dar continuidad al negocio.
Prioridad ( )

Política 28.
El responsable del sitio *hot spot* debe nombrar a un responsable sustituto de sus actividades en todo momento.
Prioridad ( )

Política 29.
Los equipos de comunicaciones deben estar conectados a un dispositivo que proporcione corriente ininterrumpida.
Prioridad ( )

Política 30
Se debe mantener el *site* de comunicaciones cerrado y bajo llave.
Prioridad ( )

Política 31.
El *site* de comunicaciones debe estar alejado de fuentes de agua y no debe ubicarse bajo desnivel del suelo.
Prioridad ( )

Política 32.
Las antenas instaladas en pared y techo se deben ubicar donde no sufran desperfectos naturales o intencionados.
Prioridad ( )

Elemento de Seguridad 10: Conformidad con la Legislación.

Política 33.
Se debe acatar la norma regulatoria del servicio inalámbrico en México. (121 SCT94)
Prioridad ( )

Política 34
Se debe respetar el contrato de trabajo de los empleados.
Prioridad ( )

Política 35.
Se debe respetar la confidencialidad de la información.
Prioridad ( )

Política 36
Se debe respetar la privacidad de las personas.
Prioridad ( )

Apéndice C

Resultado de la encuesta aplicada a los clientes de los *hot spot*

	1. Politica de Seguridad				2. Aspectos Organizativos de la Seguridad	
	Politica 1	Politica 2	Politica 3	Politica 4	Politica 5	Politica 6
Prioridad del Cliente 1	3	2	1	4	1	2
Prioridad del Cliente 2	3	2	1	4	2	1
Prioridad del Cliente 3	4	3	2	1	2	1
Prioridad del Cliente 4	4	3	2	1	2	1
Prioridad del Cliente 5	4	3	2	1	2	1
Prioridad del Cliente 6	3	2	1	4	2	1
Prioridad del Cliente 7	3	1	4	2	2	1
Prioridad del Cliente 8	4	2	1	3	2	1
Prioridad del Cliente 9	3	2	1	4	2	1
Prioridad del Cliente 10	4	2	3	1	2	1
Prioridad del Cliente 11	4	1	2	3	2	1
Prioridad del Cliente 12	2	4	1	3	2	1
Prioridad del Cliente 13	4	2	1	3	2	1
Prioridad del Cliente 14	4	3	2	1	2	1
Prioridad del Cliente 15	3	2	1	4	2	1
Prioridad del Cliente 16	4	3	1	2	2	1
Prioridad del Cliente 17	2	1	4	3	2	1
Prioridad del Cliente 18	2	4	1	3	2	1
Prioridad del Cliente 19	4	3	1	2	2	1
Prioridad del Cliente 20	4	1	2	3	2	1
Prioridad del Cliente 21	4	3	2	1	2	1
Prioridad del Cliente 22	4	2	3	1	2	1
Prioridad del Cliente 23	4	1	2	3	2	1
Prioridad del Cliente 24	2	4	1	3	2	1
Prioridad del Cliente 25	4	2	1	3	2	1
Prioridad del Cliente 26	4	3	2	1	2	1
Prioridad del Cliente 27	3	2	1	4	2	1
Prioridad del Cliente 28	4	3	1	2	2	1
Prioridad del Cliente 29	2	1	4	3	2	1
Prioridad del Cliente 30	2	4	1	3	2	1
Prioridad del Cliente 31	4	3	1	2	2	1
Prioridad del Cliente 32	4	1	2	3	2	1
Prioridad del Cliente 33	4	3	2	1	2	1
Prioridad del Cliente 34	3	2	1	4	1	2
Prioridad del Cliente 35	3	2	1	4	2	1
Prioridad del Cliente 36	4	3	2	1	2	1
Prioridad del Cliente 37	4	3	2	1	2	1
Prioridad del Cliente 38	4	3	2	1	2	1
Prioridad del Cliente 39	3	2	1	4	2	1
Prioridad del Cliente 40	3	1	4	2	2	1
Prioridad del Cliente 41	4	2	1	3	2	1
Prioridad del Cliente 42	3	2	1	4	2	1
Prioridad del Cliente 43	4	3	2	1	2	1
Prioridad del Cliente 44	4	1	2	3	2	1
Prioridad del Cliente 45	4	3	1	2	2	1
Prioridad del Cliente 46	2	4	1	3	2	1
Prioridad del Cliente 47	2	1	4	3	2	1
Prioridad del Cliente 48	4	3	1	2	2	1
Prioridad del Cliente 49	3	2	1	4	2	1
Prioridad del Cliente 50	4	3	2	1	2	1
Prioridad del Cliente 51	4	2	1	3	2	1
Prioridad del Cliente 52	2	4	1	3	2	1
Prioridad del Cliente 53	4	1	2	3	2	1
Prioridad del Cliente 54	3	2	1	4	1	2
Prioridad del Cliente 55	4	3	1	2	2	1
Prioridad del Cliente 56	4	1	2	3	2	1
Prioridad del Cliente 57	4	3	2	1	2	1

	3. Clasificacion y Control de Activos			4. Seguridad relacionada a los Recursos Humanos				
	Politica 7	Politica 8	Politica 9	Politica 10	Politica 11	Politica 12	Politica 13	Politica 14
Prioridad del Cliente 1	2	1	3	5	3	4	1	2
Prioridad del Cliente 2	1	2	3	1	3	2	4	5
Prioridad del Cliente 3	2	1	3	1	3	2	5	4
Prioridad del Cliente 4	1	2	3	1	3	2	4	5
Prioridad del Cliente 5	1	2	3	4	3	1	5	2
Prioridad del Cliente 6	1	2	3	1	3	2	4	5
Prioridad del Cliente 7	1	3	2	1	5	2	4	3
Prioridad del Cliente 8	1	2	3	2	3	1	5	4
Prioridad del Cliente 9	1	2	3	1	3	4	5	2
Prioridad del Cliente 10	1	3	2	2	3	1	4	5
Prioridad del Cliente 11	1	2	3	1	3	2	5	4
Prioridad del Cliente 12	2	3	1	1	2	4	3	5
Prioridad del Cliente 13	3	1	2	2	1	4	3	5
Prioridad del Cliente 14	1	3	2	3	2	1	4	5
Prioridad del Cliente 15	1	2	3	1	2	3	4	5
Prioridad del Cliente 16	3	1	2	1	3	2	4	5
Prioridad del Cliente 17	2	1	3	3	1	2	5	4
Prioridad del Cliente 18	1	2	3	1	3	2	5	4
Prioridad del Cliente 19	3	1	2	2	1	4	3	5
Prioridad del Cliente 20	3	2	1	3	1	2	4	5
Prioridad del Cliente 21	1	2	3	3	4	5	2	1
Prioridad del Cliente 22	1	3	2	2	3	1	4	5
Prioridad del Cliente 23	1	2	3	1	3	2	5	4
Prioridad del Cliente 24	2	3	1	1	2	4	3	5
Prioridad del Cliente 25	3	1	2	2	1	4	3	5
Prioridad del Cliente 26	1	3	2	3	2	1	4	5
Prioridad del Cliente 27	1	2	3	1	2	3	4	5
Prioridad del Cliente 28	3	1	2	1	3	2	4	5
Prioridad del Cliente 29	2	1	3	3	1	2	5	4
Prioridad del Cliente 30	1	2	3	1	3	2	5	4
Prioridad del Cliente 31	3	1	2	2	1	4	3	5
Prioridad del Cliente 32	3	2	1	3	1	2	4	5
Prioridad del Cliente 33	1	2	3	3	4	5	2	1
Prioridad del Cliente 34	2	1	3	5	3	4	1	2
Prioridad del Cliente 35	1	2	3	1	3	2	4	5
Prioridad del Cliente 36	2	1	3	1	3	2	5	4
Prioridad del Cliente 37	1	2	3	1	3	2	4	5
Prioridad del Cliente 38	1	2	3	4	3	1	5	2
Prioridad del Cliente 39	1	2	3	1	3	2	4	5
Prioridad del Cliente 40	1	3	2	1	5	2	4	3
Prioridad del Cliente 41	1	2	3	2	3	1	5	4
Prioridad del Cliente 42	1	2	3	1	3	4	5	2
Prioridad del Cliente 43	1	2	3	3	4	5	2	1
Prioridad del Cliente 44	3	2	1	3	1	2	4	5
Prioridad del Cliente 45	3	1	2	2	1	4	3	5
Prioridad del Cliente 46	1	2	3	1	3	2	5	4
Prioridad del Cliente 47	2	1	3	3	1	2	5	4
Prioridad del Cliente 48	3	1	2	1	3	2	4	5
Prioridad del Cliente 49	1	2	3	1	2	3	4	5
Prioridad del Cliente 50	1	3	2	3	2	1	4	5
Prioridad del Cliente 51	3	1	2	2	1	4	3	5
Prioridad del Cliente 52	2	3	1	1	2	4	3	5
Prioridad del Cliente 53	1	2	3	1	3	2	5	4
Prioridad del Cliente 54	2	1	3	5	3	4	1	2
Prioridad del Cliente 55	3	1	2	2	1	4	3	5
Prioridad del Cliente 56	3	2	1	3	1	2	4	5
Prioridad del Cliente 57	1	2	3	3	4	5	2	1

	5. Seguridad Fisica y del Entorno				6. Control de Acceso	
	Politica 15	Politica 16	Politica 17	Politica 18	Politica 19	Politica 20
Prioridad del Cliente 1	1	2	4	3	2	1
Prioridad del Cliente 2	1	3	2	4	2	1
Prioridad del Cliente 3	2	3	4	1	2	1
Prioridad del Cliente 4	1	3	2	4	2	1
Prioridad del Cliente 5	1	2	3	4	2	1
Prioridad del Cliente 6	1	2	3	4	1	2
Prioridad del Cliente 7	2	1	3	4	2	1
Prioridad del Cliente 8	2	1	3	4	2	1
Prioridad del Cliente 9	4	2	3	1	1	2
Prioridad del Cliente 10	3	1	2	4	2	1
Prioridad del Cliente 11	2	1	3	4	2	1
Prioridad del Cliente 12	3	2	4	1	2	1
Prioridad del Cliente 13	2	1	4	3	1	2
Prioridad del Cliente 14	3	1	2	4	2	1
Prioridad del Cliente 15	1	3	4	2	2	1
Prioridad del Cliente 16	1	2	3	4	2	1
Prioridad del Cliente 17	2	1	3	4	2	1
Prioridad del Cliente 18	3	1	4	2	2	1
Prioridad del Cliente 19	2	1	3	4	2	1
Prioridad del Cliente 20	1	3	2	4	2	1
Prioridad del Cliente 21	1	3	4	2	2	1
Prioridad del Cliente 22	3	1	2	4	2	1
Prioridad del Cliente 23	2	1	3	4	2	1
Prioridad del Cliente 24	3	2	4	1	2	1
Prioridad del Cliente 25	2	1	4	3	1	2
Prioridad del Cliente 26	3	1	2	4	2	1
Prioridad del Cliente 27	1	3	4	2	2	1
Prioridad del Cliente 28	1	2	3	4	2	1
Prioridad del Cliente 29	2	1	3	4	2	1
Prioridad del Cliente 30	3	1	4	2	2	1
Prioridad del Cliente 31	2	1	3	4	2	1
Prioridad del Cliente 32	1	3	2	4	2	1
Prioridad del Cliente 33	1	3	4	2	2	1
Prioridad del Cliente 34	1	2	4	3	2	1
Prioridad del Cliente 35	1	3	2	4	2	1
Prioridad del Cliente 36	2	3	4	1	2	1
Prioridad del Cliente 37	1	3	2	4	2	1
Prioridad del Cliente 38	1	2	3	4	2	1
Prioridad del Cliente 39	1	2	3	4	1	2
Prioridad del Cliente 40	2	1	3	4	2	1
Prioridad del Cliente 41	2	1	3	4	2	1
Prioridad del Cliente 42	4	2	3	1	1	2
Prioridad del Cliente 43	1	3	4	2	2	1
Prioridad del Cliente 44	1	3	2	4	2	1
Prioridad del Cliente 45	2	1	3	4	2	1
Prioridad del Cliente 46	3	1	4	2	2	1
Prioridad del Cliente 47	2	1	3	4	2	1
Prioridad del Cliente 48	1	2	3	4	2	1
Prioridad del Cliente 49	1	3	4	2	2	1
Prioridad del Cliente 50	3	1	2	4	2	1
Prioridad del Cliente 51	2	1	4	3	1	2
Prioridad del Cliente 52	3	2	4	1	2	1
Prioridad del Cliente 53	2	1	3	4	2	1
Prioridad del Cliente 54	1	2	4	3	2	1
Prioridad del Cliente 55	2	1	3	4	2	1
Prioridad del Cliente 56	1	3	2	4	2	1
Prioridad del Cliente 57	1	3	4	2	2	1

	7. Desarrollo y Mantto de Sistemas			8. Administracion de los incidentes de Seguridad		
	Politica 21	Politica 22	Politica 23	Politica 24	Politica 25	Politica 26
Prioridad del Cliente 1	1	2	3	1	3	2
Prioridad del Cliente 2	1	2	3	2	3	1
Prioridad del Cliente 3	2	1	3	1	3	2
Prioridad del Cliente 4	1	2	3	1	3	2
Prioridad del Cliente 5	1	3	2	1	2	3
Prioridad del Cliente 6	1	2	3	1	2	3
Prioridad del Cliente 7	2	1	3	3	2	1
Prioridad del Cliente 8	1	2	3	2	1	3
Prioridad del Cliente 9	2	1	3	1	3	2
Prioridad del Cliente 10	3	1	2	1	3	2
Prioridad del Cliente 11	1	2	3	1	3	2
Prioridad del Cliente 12	3	1	2	1	3	2
Prioridad del Cliente 13	1	2	3	1	2	3
Prioridad del Cliente 14	1	2	3	1	2	3
Prioridad del Cliente 15	1	3	2	1	2	3
Prioridad del Cliente 16	1	2	3	1	3	2
Prioridad del Cliente 17	1	2	3	3	2	1
Prioridad del Cliente 18	1	2	3	1	3	2
Prioridad del Cliente 19	1	2	3	1	3	2
Prioridad del Cliente 20	2	1	3	3	2	1
Prioridad del Cliente 21	1	2	3	2	1	3
Prioridad del Cliente 22	3	1	2	1	3	2
Prioridad del Cliente 23	1	2	3	1	3	2
Prioridad del Cliente 24	3	1	2	1	3	2
Prioridad del Cliente 25	1	2	3	1	2	3
Prioridad del Cliente 26	1	2	3	1	2	3
Prioridad del Cliente 27	1	3	2	1	2	3
Prioridad del Cliente 28	1	2	3	1	3	2
Prioridad del Cliente 29	1	2	3	3	2	1
Prioridad del Cliente 30	1	2	3	1	3	2
Prioridad del Cliente 31	1	2	3	1	3	2
Prioridad del Cliente 32	2	1	3	3	2	1
Prioridad del Cliente 33	1	2	3	2	1	3
Prioridad del Cliente 34	1	2	3	1	3	2
Prioridad del Cliente 35	1	2	3	2	3	1
Prioridad del Cliente 36	2	1	3	1	3	2
Prioridad del Cliente 37	1	2	3	1	3	2
Prioridad del Cliente 38	1	3	2	1	2	3
Prioridad del Cliente 39	1	2	3	1	2	3
Prioridad del Cliente 40	2	1	3	3	2	1
Prioridad del Cliente 41	1	2	3	2	1	3
Prioridad del Cliente 42	2	1	3	1	3	2
Prioridad del Cliente 43	1	2	3	2	1	3
Prioridad del Cliente 44	2	1	3	3	2	1
Prioridad del Cliente 45	1	2	3	1	3	2
Prioridad del Cliente 46	1	2	3	1	3	2
Prioridad del Cliente 47	1	2	3	3	2	1
Prioridad del Cliente 48	1	2	3	1	3	2
Prioridad del Cliente 49	1	3	2	1	2	3
Prioridad del Cliente 50	1	2	3	1	2	3
Prioridad del Cliente 51	1	2	3	1	2	3
Prioridad del Cliente 52	3	1	2	1	3	2
Prioridad del Cliente 53	1	2	3	1	3	2
Prioridad del Cliente 54	1	2	3	1	3	2
Prioridad del Cliente 55	1	2	3	1	3	2
Prioridad del Cliente 56	2	1	3	3	2	1
Prioridad del Cliente 57	1	2	3	2	1	3

	9. Administracion de la Continuidad del Negocio					
	Politica 27	Politica 28	Politica 29	Politica 30	Politica 31	Politica 32
Prioridad del Cliente 1	1	2	3	6	4	5
Prioridad del Cliente 2	1	6	5	4	3	2
Prioridad del Cliente 3	1	2	3	6	4	5
Prioridad del Cliente 4	2	3	6	1	5	4
Prioridad del Cliente 5	1	2	5	6	4	3
Prioridad del Cliente 6	3	2	4	1	6	5
Prioridad del Cliente 7	1	4	6	5	2	3
Prioridad del Cliente 8	5	6	3	4	1	2
Prioridad del Cliente 9	3	2	1	4	6	5
Prioridad del Cliente 10	1	5	2	4	3	6
Prioridad del Cliente 11	1	6	2	3	5	4
Prioridad del Cliente 12	5	4	1	6	2	3
Prioridad del Cliente 13	1	5	2	3	4	6
Prioridad del Cliente 14	6	3	5	1	2	4
Prioridad del Cliente 15	1	6	2	3	5	4
Prioridad del Cliente 16	1	6	2	4	5	3
Prioridad del Cliente 17	1	6	2	5	3	4
Prioridad del Cliente 18	1	6	5	2	3	4
Prioridad del Cliente 19	1	2	4	3	5	6
Prioridad del Cliente 20	3	1	6	2	4	5
Prioridad del Cliente 21	1	2	3	4	5	6
Prioridad del Cliente 22	1	5	2	4	3	6
Prioridad del Cliente 23	1	6	2	3	5	4
Prioridad del Cliente 24	5	4	1	6	2	3
Prioridad del Cliente 25	1	5	2	3	4	6
Prioridad del Cliente 26	6	3	5	1	2	4
Prioridad del Cliente 27	1	6	2	3	5	4
Prioridad del Cliente 28	1	6	2	4	5	3
Prioridad del Cliente 29	1	6	2	5	3	4
Prioridad del Cliente 30	1	6	5	2	3	4
Prioridad del Cliente 31	1	2	4	3	5	6
Prioridad del Cliente 32	3	1	6	2	4	5
Prioridad del Cliente 33	1	2	3	4	5	6
Prioridad del Cliente 34	1	2	3	6	4	5
Prioridad del Cliente 35	1	6	5	4	3	2
Prioridad del Cliente 36	1	2	3	6	4	5
Prioridad del Cliente 37	2	3	6	1	5	4
Prioridad del Cliente 38	1	2	5	6	4	3
Prioridad del Cliente 39	3	2	4	1	6	5
Prioridad del Cliente 40	1	4	6	5	2	3
Prioridad del Cliente 41	5	6	3	4	1	2
Prioridad del Cliente 42	3	2	1	4	6	5
Prioridad del Cliente 43	1	2	3	4	5	6
Prioridad del Cliente 44	3	1	6	2	4	5
Prioridad del Cliente 45	1	2	4	3	5	6
Prioridad del Cliente 46	1	6	5	2	3	4
Prioridad del Cliente 47	1	6	2	5	3	4
Prioridad del Cliente 48	1	6	2	4	5	3
Prioridad del Cliente 49	1	6	2	3	5	4
Prioridad del Cliente 50	6	3	5	1	2	4
Prioridad del Cliente 51	1	5	2	3	4	6
Prioridad del Cliente 52	5	4	1	6	2	3
Prioridad del Cliente 53	1	6	2	3	5	4
Prioridad del Cliente 54	1	2	3	6	4	5
Prioridad del Cliente 55	1	2	4	3	5	6
Prioridad del Cliente 56	3	1	6	2	4	5
Prioridad del Cliente 57	1	2	3	4	5	6

	10. Conformidad con la Legislacion.			
	Politica 33	Politica 34	Politica 35	Politica 36
Prioridad del Cliente 1	1	4	2	3
Prioridad del Cliente 2	3	4	1	2
Prioridad del Cliente 3	1	4	2	3
Prioridad del Cliente 4	1	4	2	3
Prioridad del Cliente 5	1	2	4	3
Prioridad del Cliente 6	1	4	3	2
Prioridad del Cliente 7	1	3	2	4
Prioridad del Cliente 8	3	4	1	2
Prioridad del Cliente 9	4	3	1	2
Prioridad del Cliente 10	3	4	1	2
Prioridad del Cliente 11	1	4	2	3
Prioridad del Cliente 12	3	4	1	2
Prioridad del Cliente 13	1	4	2	3
Prioridad del Cliente 14	3	4	1	2
Prioridad del Cliente 15	1	4	2	3
Prioridad del Cliente 16	1	4	3	2
Prioridad del Cliente 17	2	4	1	3
Prioridad del Cliente 18	1	2	3	4
Prioridad del Cliente 19	4	3	1	2
Prioridad del Cliente 20	1	4	2	3
Prioridad del Cliente 21	1	3	2	4
Prioridad del Cliente 22	3	4	1	2
Prioridad del Cliente 23	1	4	2	3
Prioridad del Cliente 24	3	4	1	2
Prioridad del Cliente 25	1	4	2	3
Prioridad del Cliente 26	3	4	1	2
Prioridad del Cliente 27	1	4	2	3
Prioridad del Cliente 28	1	4	3	2
Prioridad del Cliente 29	2	4	1	3
Prioridad del Cliente 30	1	2	3	4
Prioridad del Cliente 31	4	3	1	2
Prioridad del Cliente 32	1	4	2	3
Prioridad del Cliente 33	1	3	2	4
Prioridad del Cliente 34	1	4	2	3
Prioridad del Cliente 35	3	4	1	2
Prioridad del Cliente 36	1	4	2	3
Prioridad del Cliente 37	1	4	2	3
Prioridad del Cliente 38	1	2	4	3
Prioridad del Cliente 39	1	4	3	2
Prioridad del Cliente 40	1	3	2	4
Prioridad del Cliente 41	3	4	1	2
Prioridad del Cliente 42	4	3	1	2
Prioridad del Cliente 43	1	3	2	4
Prioridad del Cliente 44	1	4	2	3
Prioridad del Cliente 45	4	3	1	2
Prioridad del Cliente 46	1	2	3	4
Prioridad del Cliente 47	2	4	1	3
Prioridad del Cliente 48	1	4	3	2
Prioridad del Cliente 49	1	4	2	3
Prioridad del Cliente 50	3	4	1	2
Prioridad del Cliente 51	1	4	2	3
Prioridad del Cliente 52	3	4	1	2
Prioridad del Cliente 53	1	4	2	3
Prioridad del Cliente 54	1	4	2	3
Prioridad del Cliente 55	4	3	1	2
Prioridad del Cliente 56	1	4	2	3
Prioridad del Cliente 57	1	3	2	4

Apéndice D

Resultado de las encuestas aplicadas a los administradores de los sitios *hot spot*

	1. Politica de Seguridad				2. Aspectos Organizativos de la Seguridad	
	Politica 1	Politica 2	Politica 3	Politica 4	Politica 5	Politica 6
Prioridad del Administrador 1	1	2	3	4	2	1
Prioridad del Administrador 2	2	3	1	4	2	1
Prioridad del Administrador 3	2	3	1	4	2	1
Prioridad del Administrador 4	4	3	1	2	1	2
Prioridad del Administrador 5	1	2	1	4	2	1
Prioridad del Administrador 6	1	2	1	4	2	1
Prioridad del Administrador 7	2	3	1	4	2	1
Prioridad del Administrador 8	1	2	3	4	2	1
Prioridad del Administrador 9	4	3	1	2	1	2
Prioridad del Administrador 10	2	3	1	4	2	1

	3. Clasificacion y Control de Activos			4. Seguridad relacionada a los Recursos Humanos				
	Politica 7	Politica 8	Politica 9	Politica 10	Politica 11	Politica 12	Politica 13	Politica 14
Prioridad del Administrador 1	1	2	3	1	4	2	5	3
Prioridad del Administrador 2	1	2	3	2	5	1	4	3
Prioridad del Administrador 3	1	2	3	2	4	5	1	3
Prioridad del Administrador 4	2	3	1	3	5	1	4	2
Prioridad del Administrador 5	1	2	3	1	5	1	4	3
Prioridad del Administrador 6	1	2	3	1	5	1	4	3
Prioridad del Administrador 7	1	2	3	2	4	5	1	3
Prioridad del Administrador 8	1	2	3	1	4	2	5	3
Prioridad del Administrador 9	2	3	1	3	5	1	4	2
Prioridad del Administrador 10	1	2	3	2	5	1	4	3

	5. Seguridad Fisica y del Entorno				6. Control de Acceso	
	Politica 15	Politica 16	Politica 17	Politica 18	Politica 19	Politica 20
Prioridad del Administrador 1	4	1	3	2	No Aplico	No Aplico
Prioridad del Administrador 2	4	1	3	2	No Aplico	No Aplico
Prioridad del Administrador 3	4	1	2	3	No Aplico	No Aplico
Prioridad del Administrador 4	1	2	3	4	No Aplico	No Aplico
Prioridad del Administrador 5	4	1	3	2	No Aplico	No Aplico
Prioridad del Administrador 6	4	1	3	2	No Aplico	No Aplico
Prioridad del Administrador 7	4	1	2	3	No Aplico	No Aplico
Prioridad del Administrador 8	4	1	3	2	No Aplico	No Aplico
Prioridad del Administrador 9	1	2	3	4	No Aplico	No Aplico
Prioridad del Administrador 10	4	1	3	2	No Aplico	No Aplico

	7. Desarrollo y Mantto de Sistemas			8. Administracion de los incidentes de Seguridad		
	Politica 21	Politica 22	Politica 23	Politica 24	Politica 25	Politica 26
Prioridad del Administrador 1	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 2	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 3	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 4	No Aplico	No Aplico	No Aplico	3	2	1
Prioridad del Administrador 5	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 6	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 7	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 8	No Aplico	No Aplico	No Aplico	1	3	2
Prioridad del Administrador 9	No Aplico	No Aplico	No Aplico	3	2	1
Prioridad del Administrador 10	No Aplico	No Aplico	No Aplico	1	3	2

	9. Administracion de la Continuidad del Negocio					
	Politica 27	Politica 28	Politica 29	Politica 30	Politica 31	Politica 32
Prioridad del Administrador 1	2	1	3	4	5	6
Prioridad del Administrador 2	3	1	4	2	5	6
Prioridad del Administrador 3	5	1	3	2	4	6
Prioridad del Administrador 4	3	2	1	4	5	6
Prioridad del Administrador 5	3	1	4	2	5	6
Prioridad del Administrador 6	3	1	4	2	5	6
Prioridad del Administrador 7	5	1	3	2	4	6
Prioridad del Administrador 8	2	1	3	4	5	6
Prioridad del Administrador 9	3	2	1	4	5	6
Prioridad del Administrador 10	3	1	4	2	5	6

	10. Conformidad con la Legislacion.			
	Politica 33	Politica 34	Politica 35	Politica 36
Prioridad del Administrador 1	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 2	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 3	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 4	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 5	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 6	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 7	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 8	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 9	No Aplico	No Aplico	No Aplico	No Aplico
Prioridad del Administrador 10	No Aplico	No Aplico	No Aplico	No Aplico

Bibliografía

[ADSL-07] Consulta en internet
http://www.adslnet.es/index.php/2007/08/21/conexion-inalambrica-en-el-hogar-como-instalar-y-proteger-una-red-wi-fi/
Fecha de consulta: 05-diciembre-2007

[ALI-05] Aligning COBIT, ITIL and ISO 17799 for Business Benefit
LexisNexis™ Academic
Copyright 2005 PR Newswire Europe Limited.
All Rights Reserved.
PR Newswire Europe
November 9, 2005 Wednesday
LENGTH: 467 words
HEADLINE: Aligning COBIT, ITIL and ISO 17799 for Business Benefit
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 16-marzo-2007

[ANK-05] LexisNexis™ Academic Copyright 2005 by PRIMEDIA Business.
Copyright 2005 by PRIMEDIA Business Magazines & Media, Inc.
All Rights Reserved
Telephony
January 31, 2005
SECTION: WIRELESS; Pg. 26 ISSN: 0040-2656
LENGTH: 1779 words
HEADLINE: On the Verge of Convergence
BYLINE: by Jason Ankeny
Fecha de consulta: 31-octubre-2006

[BUS-06] Business Editors; Health/Medical Writers.
LexisNexis™ Academic
Copyright 2006 Business Wire, Inc.
Business Wire
January 24, 2006 Tuesday 12:00 PM GMT
DISTRIBUTION: Business Editors; Health/Medical Writers
LENGTH: 436 words
HEADLINE: Cereplex Completes Security Assessment: Compliance with ISO Standard Insuring Data Integrity for Automated Surveillance Clients
DATELINE: GERMANTOWN, Md. Jan. 24, 2006
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 30-abril-2007

[CAR-04] J.A. Carballar, Wi-Fi. Como construir una red inalámbrica. Alfa Omega, México, DF., 2004, Pg.

[CAR-05] Simeon, Carrie Higbie, Infosel News,
Publication: Infosel News
Provider: Terra Networks México S.A. de C.V.
Date: February 28, 2006 (17:09)
Fuente: GRUPO REFORMA Lilia Chacón Redacción México (55) 5628 7351 Fax (55) 5628 7349/7359 E-mail: monitoreoif@reforma.com
Any redistribution of this information is strictly prohibited.
Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007 Internet Securities, Inc. (trading as ISI Emerging Markets), all rights reserved.
A Euromoney Institutional Investor company.
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 17-septiembre, 2007.

[CHA-06] Lilia Chacon, Infosel News, http://biblioteca.itesm.mx/nav/
Publication: Infosel News
Provider: Terra Networks México S.A. de C.V.
Date: June 21, 2007 (23:11)
Fuente: GRUPO REFORMA Lilia Chacón Redacción México (55) 5628 7343 Fax (55) 5628 7349/7359 E-mail: monitoreoif@reforma.com
Fecha de consulta: 17-septiembre, 2007

[CHA-05] Lilia Chacon, Agencia Reforma Negocios
Publication: Reforma - Negocios
Provider: Agencia Reforma
Date: February 28, 2006
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 13-octubre-2007

[CHE-05] Chennai
LexisNexis™ Academic
Copyright 2005 Financial Times Information
All Rights Reserved
Global News Wire - Asia Africa Intelligence Wire
Copyright 2005 Kasturi & Sons Ltd (KSL)
Business Line
August 24, 2005
Fecha de consulta: 10-noviembre-2006

[EDN-04] LexisNexis™ Academic
Copyright 2004 Reed Business Information, US, a division of Reed Elsevier Inc.
All Rights Reserved
EDN
November 11, 2004

SECTION: FEATURES; Design Feature; Pg. 67
LENGTH: 5718 words
HEADLINE: Power and wireless options extend Ethernet's reach;
Ethernet's power-delivery and wireless abilities offer new application potential that hugely extends the reach of the IEEE's 802.x series of standards.
BYLINE: By David Marsh, Contributing Technical Editor
Fecha de consulta: 10-noviembre-2006

[ENG-05] A. Engst, G. Fleishman, Introducción a las redes inalámbricas. Anaya Multimedia, México, D.F., 2005, Pg.

[ERN-07] 9ª Encuesta Global de Seguridad de la Información 2006, Mancera, S. C. Integrante de Ernst&Young Global, Pg. 26
www.ey.com/mx
Fecha de consulta 30-abril-2007.

[FUN-05] Ignacio Funes, Crain Communications
Publication: Crain Communications - Crain's de México
Provider: Crain's Communications, S. de R.L. de C.V.
Date: February 14, 2005
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 20-septiembre-2007

[GAS-06] Prevén en este año liberar permiso para TV de Telmex
Verónica Gascón. El Norte. Monterrey, Mexico: Jul 23, 2007. pg. 7
http://0-proquest.umi.com.millenium.itesm.mx/pqdlink?index=0&did=1308594891&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1197323447&clientId=23693
Fecha de consulta: 04-junio-2007

[INE-07] Pagina web INEGI
http://www.inegi.org.mx/prod_serv/contenidos/espanol/bvinegi/productos/encuestas/especiales/endutih/endutih2004.pdf
Fecha de consulta: 06/diciciembre/2007

[INT-07] Intranet Telmex/Red Uno
Fecha de consulta: 25-mayo-2007

[ISO-05] ISO-17799-1 2005
International Standard ISO/IEC FDIS ISO 27002:2005 (E), Information Technology-Security Techniques-Code of Practice for information security management, 2005.

[KHA-05] Khalfan Al Mazrouei, IT Manager of ADSM.
LexisNexis™ Academic
Copyright 2006 AME Info FZ, LLC.

All Rights Reserved
Middle East Company News Wire
May 22, 2006 Monday 3:29 PM GMT
LENGTH: 608 words
HEADLINE: ADSM aims to become first UAE exchange to achieve ISO 17799
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 12-marz0-2007

[MIM-05] Michael S. Mimoso, NEWSCAN; Standards; Pg. 18, LexisNexis™
LexisNexis™ Academic
Copyright 2005 Trusecure Corporation
Information Security
August, 2005
SECTION: NEWSCAN; Standards; Pg. 18
LENGTH: 260 words
HEADLINE: A Fresh Take on ISO 17799, BS7799
BYLINE: MICHAEL S. MIMOSO
LOAD-DATE: August 18, 2005
http://biblioteca.itesm.mx/nav/
Fecha de consulta: 12-marzo-2007

[PEN-03] R. Peña, R. Baeza-Yates, J.V. Rodriguez, Gestión Digital de la Información. Alfa Omega, México, DF., 2003, Pg.

[PRO-05] Documento interno de la empresa NET, Arquitectura_Funcional_Prodigy_Movil
Creado 21 Noviembre, 2002 por H. Zamora, Pg. 5-14
Fecha de consulta: 07-noviembre-2006.

[REI-04] N. Reid, R. Seide, 802.11 WIFI Manual de redes inalámbricas. McGraw Hill, México, DF., 2004, Pg.

[STA-04] Standards IEEE "Get IEEE 802": Wireless (IEEE 802.11)
http://standards.ieee.org/getieee802/802.11.html
Fecha de consulta: 10-noviembre-2006

[TMX-07] Pagina web telmex
http://www.telmex.com/mx/negocio/in_pdgyMovil_TerminoCondicion.html
Fecha de consulta: 05/diciembre/2007

[WIF-06] Wi-fi Alliance, Get to know the alliance.
http://www.wi-fi.com/about_overview.php
Fecha de consulta: 15-octubre-2006