Estudio de Metodologías para la Implantación de la Seguridad en Redes Inalámbricas de Área Local

AUTOR: JESUS ENRIQUE MÉNDEZ ÁLVAREZ
TUTOR: VINCENZO MENDILLO

Caracas, Junio de 2006
DERECHO DE AUTOR

Yo, JESUS ENRIQUE MENDEZ ALVAREZ; titular de la Cédula de Identidad número V-12.422.877, cedo a la Universidad Metropolitana el derecho de reproducir y difundir el presente trabajo titulado con las únicas limitaciones que establece la legislación vigente en materia de derecho de autor.

En la ciudad de Caracas, a los once días del mes de junio de 2006.

__________

Autor
APROBACIÓN DEL TUTOR

Quien suscribe VINCENZO MENDILLO, Tutor del Trabajo de Grado Estudio de las metodologías de implantación de la seguridad en redes inalámbricas de área local, elaborado por JESUS ENRIQUE MENDEZ ALVAREZ, para optar al título de Especialista en Gerencia en Tecnología y Telecomunicaciones, considera que el mismo reúne los requisitos exigidos por el Decanato de Postgrado de la Universidad Metropolitana, y tiene méritos suficientes como para ser sometido a la presentación y evaluación por parte del jurado examinador.

En la ciudad de Caracas, a los once días del mes de junio de 2006.

VINCENZO MENDILLO

[Signature]

Tutor
RESUMEN

Las redes locales inalámbricas están siendo instaladas por organizaciones de todo el mundo, quienes han reconocido su valor y por ende han comenzado a utilizar estas tecnologías para incrementar la productividad de su fuerza de trabajo y mejorar la calidad de los servicios que están ofreciendo a los usuarios. Sin embargo, ese tipo de red está plagada de vulnerabilidades de seguridad, lo cual ha impuesto la necesidad de contar con esquemas integrales que garanticen la seguridad y por ende le permitan a las organizaciones alcanzar sus objetivos claves. Ha sido necesario entonces tomar las medidas necesarias para mitigar los riesgos en las potenciales áreas críticas de cada organización, dado que los mecanismos básicos de seguridad de las redes locales inalámbricas hasta la fecha se han hecho insuficientes para proteger los activos de información. En tal sentido, se investigaron las metodologías de seguridad más cercanas a lo especificado en los estándares internacionales de la seguridad, las cuales se aplicaron al problema de la investigación, logrando como resultado dos esquemas metodológicos complementarios, contentivos de las mejores prácticas de seguridad tanto para el ámbito global de la organización como para el entorno específico de las redes inalámbricas de área local, mediante una combinación integral de las perspectivas necesarias para la implantación de una cultura de seguridad organizacional.
INDICE

RESUMEN............................................................................................................................... i

LISTA DE TABLAS Y FIGURAS............................................................................................ iii

INTRODUCCIÓN.................................................................................................................... 1

Capítulo 1. El Problema de la investigación........................................................................... 3

1.2 Formulación del problema................................................................................................. 5
1.3 Justificación de la Investigación........................................................................................ 5
1.4 Objetivos............................................................................................................................. 7
  1.4.1 Objetivos Generales........................................................................................................ 7
  1.4.2 Objetivos específicos...................................................................................................... 7
1.5 Alcance............................................................................................................................... 7
1.6. Limitaciones..................................................................................................................... 8

Capítulo 2. Fundamentos del trabajo....................................................................................... 9

2.1. Bases teóricas................................................................................................................... 9
  2.1.1 Redes inalámbricas de área local (WLAN, Wireless Local Area Network)............... 9
  2.1.1.1 ¿Qué es una red inalámbrica de área local o WLAN?......................................... 9
  2.1.1.2 Origen de las redes inalámbricas locales............................................................ 10
  2.1.1.3. Medios de transmisión inalámbrica .................................................................... 11
  2.1.1.4. Como trabajan las WLAN .............................................................................. 16
  2.1.1.5 Infraestructura WLAN....................................................................................... 17
  2.1.1.6. Estándares en WLAN....................................................................................... 19
  2.1.1.7. Futuro de las redes inalámbricas de área local............................................... 24
  2.1.1.8. Vulnerabilidades más comunes en la seguridad de las WLAN .................... 26
  2.1.1.9. Seguridad en WLAN....................................................................................... 32
  2.1.1.10. Protocolos de seguridad en WLAN .............................................................. 32
  2.1.1.10.1. Protocolos de seguridad en WLAN......................................................... 57

2.2 Marco metodológico ....................................................................................................... 60
  2.2.1. Consideraciones Generales...................................................................................... 60
  2.2.2. Tipo de Investigación............................................................................................... 60
  2.2.3. Área de Investigación............................................................................................... 61
  2.2.4. Descripción de la Metodología.............................................................................. 61
  2.2.5. Diseño de la Investigación....................................................................................... 62
  2.2.6. Instrumentos de recolección de información....................................................... 62
  2.2.7. Técnicas documentales........................................................................................... 63

Capítulo 3. Metodologías de implantación de la seguridad en WLAN................................. 65

3.1. Estándar ISO/IEC 17799................................................................................................. 67
3.2. Cobit (Objetivos de control de información y tecnologías relacionadas)..................... 72
3.3. Aspectos a cubrir para la implantación de la seguridad de una WLAN....................... 84
  3.3.1. Cobit como metodología de implantación de seguridad en WLAN..................... 85
    3.3.1.1. Cuadro de mando integral a partir de Cobit............................................... 97
  3.3.2. ISO 17799 metodología de implantación de la seguridad en WLAN.................. 98

CONCLUSIONES..................................................................................................................... 121

RECOMENDACIONES ........................................................................................................... 124

Bibliografía.............................................................................................................................. 125

Glosario de Términos ............................................................................................................. 127
LISTA DE TABLAS Y FIGURAS

TABLAS
Tabla 1. Resumen de tecnologías de cifrado de datos WLAN ......................................................... 57
Tabla 2. Indicadores de Gestión del dominio de Soporte y servicios según Cobit ....................... 78
Tabla 3. Indicadores de gestión del dominio Monitoreo según Cobit ............................................. 82
Tabla 4. Metodología de implantación de la seguridad en WLAN aplicando Cobit ...................... 86

FIGURAS
Figura 1. Comunicación Cliente – punto de acceso - Red cableada. ................................................ 16
Figura 2. Configuración típica de WLAN corporativas ................................................................. 17
Figura 3. Proyección de crecimiento de usuarios WLAN .............................................................. 25
Figura 4. Inversión en WLAN distribuida por tipo de usuario ..................................................... 26
Figura 5. Codificación en WEP .................................................................................................... 35
Figura 6. Decodificación en WEP ................................................................................................ 35
Figura 7. Modos de autenticación WEP ....................................................................................... 36
Figura 8. Clave compartida en WEP ........................................................................................... 39
Figura 9. Proceso de autenticación 802.1X en WPA/WPA2 .......................................................... 41
Figura 10. Proceso de cifrado TKIP/WPA .................................................................................... 45
Figura 14. Cálculo del valor MIC usado por AES CBC-MAC ....................................................... 56
Figura 15. Mapa de presencia de seguridad ................................................................................ 65
Figura 17. Dominios de control Norma UNE-ISO/IEC 17799 ..................................................... 68
Figura 19. Modelo de Gestión de la seguridad del SIGS en la UNE/ISO-IEC 17799 ...................... 71
Figura 20. Interrelación de los cuatro dominios de COBIT ......................................................... 74
Figura 21. Componentes de la Planificación en TI ................................................................. 75
Figura 22. Etapas de la adquisición e implantación ................................................................. 76
Figura 23. Elementos a considerar para un adecuado Soporte .................................................. 77
Figura 24. Principios de Cobit .................................................................................................. 85
Figura 25. Cuadro de mando integral a partir de los dominios de Cobit ...................................... 97
INTRODUCCIÓN

La creciente necesidad de acceso a los servicios informáticos a través de las redes de comunicaciones, como medio por excelencia para optimizar los tiempos de producción de bienes y servicios, mejorar los procesos claves de las organizaciones e incrementar los niveles de calidad de servicio, se ha convertido hoy por hoy, en la principal preocupación de los líderes de las empresas altamente competitivas. Sin lugar a dudas, las redes inalámbricas representan un medio para desarrollar nuevos negocios, hacer más productiva y efectiva la labor de los miembros de la organización, lo cual se traduce, en un incremento del valor tangible tanto para clientes como para accionistas.

Sin embargo, las vulnerabilidades de seguridad acompañan muy de la mano a dichas redes; estudios realizados por reconocidos entendidos en la materia en los Estados Unidos estiman que “para el año 2008 la seguridad de las redes inalámbricas locales, será el mayor problema que enfrentarán las empresas de ese país”¹ y la causa primordial de esta situación es la dificultad de controlar el tráfico en estas redes, vale decir, por primera vez en la historia de la computación no se puede conocer donde se encuentran en la red ni el dispositivo ni el usuario y como no es posible conocer donde esta el usuario tampoco se sabe quién es. A partir del año 1999 se han ido publicando documentos en Internet, donde se mencionan las mejores prácticas para la implantación de redes inalámbricas locales, sin embargo, mientras estas prácticas estén lejos del alcance del usuario final, es casi nada lo que se puede hacer para disminuir las intrusiones en las redes de este tipo.

En este sentido, la presente investigación bibliográfica (no experimental), estudia las distintas maneras, formas y mecanismos de implantar la seguridad en las redes inalámbricas de área local y coloca a disposición de las personas

---

¹ “Wireless LANs (WLANs) will be the largest growing wireless security problem faced by enterprises through 2008.” (Gartner Group).
interesadas en el tema, las mejores prácticas metodológicas para la puesta en funcionamiento de la seguridad de dichas redes, independientemente del ámbito en el cual se encuentren.

Para alcanzar estos objetivos, la investigación está conformada de tres grandes capítulos que se describen a continuación:

En el capítulo 1 se desarrolla el planteamiento del problema, objetivos, y el alcance que permiten abordar el problema dentro de un marco conceptual y metodológico adecuado.

En el capítulo 2 se encuentran los antecedentes del estudio, así como las bases teóricas y metodológicas utilizadas para orientar al lector en cuanto a las teorías y metodologías aplicadas durante la investigación.

En el capítulo 3 se describen las metodologías seleccionadas para la implantación de la seguridad de las redes inalámbricas de área local y los resultados de la aplicación de las mismas al problema de la investigación.

Por último, se mencionan un conjunto de conclusiones y recomendaciones, producto del desarrollo de la investigación.
Capítulo 1. El Problema de la investigación

En la actualidad, garantizar la seguridad de la información de una organización es una decisión crítica, sobre todo por la creciente necesidad de acceso a los servicios informáticos a través de las redes de comunicaciones, como medio por excelencia para optimizar los tiempos de producción de bienes y servicios, mejorar los procesos claves de las organizaciones e incrementar los niveles de calidad de servicio esperados por los clientes, siempre urgidos de nuevas e innovadoras soluciones para satisfacer sus necesidades. En este sentido, las empresas hoy en día reconocen el valor de las redes inalámbricas y están utilizando estas tecnologías para garantizar la productividad de su fuerza de trabajo y el servicio a sus usuarios. Sin embargo, existe la preocupación de que las redes inalámbricas están plagadas de vulnerabilidades de seguridad, por lo que hay que tener muy presentes estas dificultades al momento de implantar una solución de red basada en estas tecnologías. Desde que se detectaron los primeros puntos débiles en la seguridad en las redes inalámbricas de área local (WLAN, Wireless Local Area Network) de primera generación, analistas y empresas dedicadas a la seguridad en las redes han procurado resolver estos problemas. Algunos de estos esfuerzos han contribuido de manera significativa a la causa de la seguridad inalámbrica. Otros han participado de los defectos: algunos introducen un conjunto distinto de vulnerabilidades de seguridad; otros precisan hardware propietario costoso; otros evitan la cuestión de la seguridad de WLAN por completo protegiéndose con otra tecnología de seguridad potencialmente compleja como es la de las redes privadas virtuales (VPN); y otros aplican enfoques híbridos.

Paralelamente, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), junto con otros organismos normativos y consorcios, ha vuelto a definir y ha mejorado con diligencia los estándares de seguridad inalámbrica para permitir que las WLAN hagan frente al entorno de seguridad hostil de principios del siglo
veintiuno. Gracias a los esfuerzos de los organismos normativos y los líderes del sector, las palabras "seguridad WLAN" han dejado de ser contradictorias. Las WLAN pueden implantarse y utilizarse actualmente con un gran nivel de confianza en su seguridad. A pesar de todas las ventajas que pueden ofrecer estas tecnologías de red, una serie de preocupaciones acerca de la seguridad de las WLAN ha frenado su adopción, sobre todo en los sectores más conscientes de la importancia de la seguridad, como son el de las finanzas o los gubernamentales. Aunque parece obvio el riesgo que supone transmitir sin proteger los datos de una red a cualquiera que se encuentre en las cercanías, existe un número sorprendente de WLAN que se han instalado sin ninguna característica de seguridad activada. La mayoría de las empresas han implantado algún tipo de seguridad inalámbrica; no obstante, suele tratarse de características básicas de primera generación, que no ofrecen una protección adecuada según los estándares actuales.

Cuando se desarrollaron los primeros estándares para WLAN, la seguridad no constituía un tema tan preocupante como lo es hoy. El nivel y la sofisticación de las amenazas era muy inferior y la adopción de la tecnología inalámbrica estaba todavía dando sus primeros pasos. Es, en ese momento, cuando surge el esquema de la seguridad de las WLAN de primera generación, conocido como privacidad equivalente al cable (WEP, Wired Equivalent Privacy). La WEP subestimó las medidas necesarias para "igualar" la seguridad del aire a la seguridad del cable. En contraposición, los métodos de seguridad de WLAN modernos se diseñaron para trabajar en un entorno hostil como el aire donde no existen unos perímetros físicos o de red claros. Los puntos débiles de seguridad descubiertos en la WEP estática implican que las WLAN protegidas por ella son vulnerables a diversos tipos de amenazas. Algunas herramientas de "auditoria" disponibles hasta de forma gratuita, logran que sea posible introducirse con facilidad en redes inalámbricas protegidas por WEP. Las WLAN que no han sido protegidas se encuentran expuestas obviamente a las mismas amenazas también;
la diferencia radica en que se precisan menos conocimientos, tiempo y recursos para llevar a cabo los ataques.

Hoy en día existen esquemas modernos de seguridad disponibles para la implantación de WLAN que permiten alcanzar niveles suficientemente buenos de seguridad para los activos de la organización, sin embargo, también es ampliamente conocido que la difusión de estos métodos, mejores prácticas y nuevos esquemas de implantación de la seguridad está apenas al alcance de algunos, razón por la cual es altamente recomendable que los responsables de las áreas de informática, seguridad y/o telecomunicaciones cuenten con la información que les permita identificar los elementos necesarios para la implantación de esquemas de seguridad para WLAN, mediante el uso de las mejores prácticas metodológicas disponibles a fin de garantizarle a la organización a la cual pertenecen, alcanzar sus metas y objetivos exitosamente, apalancados en las tecnologías que ofrecen las redes inalámbricas.

1.2 Formulación del problema

En función de lo antes expuesto surge la pregunta:

¿Cuáles son los elementos que se deben considerar, siguiendo las mejores prácticas existentes, para llevar a cabo la implantación de la seguridad de una WLAN, de tal forma que la organización pueda alcanzar su más alto nivel de productividad mediante el logro de sus metas?

1.3 Justificación de la Investigación

Hoy por hoy, los administradores de red necesitan conceder a los usuarios finales, libertad y movilidad sin que los intrusos puedan acceder a la WLAN o a la información que se envía y recibe en la red inalámbrica. En una WLAN, los datos transmitidos se difunden por el aire a través de ondas de radio que viajan entre los dispositivos clientes (estaciones) y los puntos de acceso (AP) que conectan las
Estaciones a la red. Esto significa que cualquier dispositivo cliente de WLAN que esté dentro del área de servicio de un punto de acceso, puede recibir los datos transmitidos al punto de acceso (AP) (o desde éste).

Es muy factible entonces, que los datos que se transmiten a través de la red inalámbrica puedan llegar a destinatarios no deseados de otras oficinas, pisos o, incluso, fuera del edificio en el que se encuentra ubicado el punto de acceso o sencillamente ser espiados desde algún tipo de antena de gran alcance; en una WLAN los límites de la red han cambiado; sin estrictas medidas de seguridad, la instalación de una WLAN puede ser el equivalente a colocar puertos de red alámbricos por todas partes, incluyendo por ejemplo el estacionamiento.

En tal sentido, los administradores de red necesitan tener la total seguridad de que cuentan con soluciones que protegen sus WLAN de las posibles vulnerabilidades.

Sin embargo, al igual que en las redes tradicionales, es imposible garantizar un entorno de red completamente seguro que impida cualquier tipo de penetración en todo momento. La protección de la seguridad es dinámica, no estática. Tanto los administradores de red como los fabricantes de WLAN necesitan ir un paso por delante de los piratas informáticos. Por tal motivo, los expertos en seguridad recomiendan a las empresas instalar varias capas de defensa en la red para combatir las amenazas; adicionalmente los administradores de red pueden reducir el riesgo si diseñan e instalan inteligentemente sus redes inalámbricas, implantan medidas de seguridad reconocidas y utilizan productos y software desarrollados por expertos en seguridad de redes.

Por todo lo anteriormente expuesto es imperativo estudiar los mecanismos para implantar la seguridad en la WLAN y colocar en un documento a disposición de los administradores de redes y especialistas en seguridad, información de las mejores prácticas metodológicas para la puesta en funcionamiento de la seguridad de sus redes WLAN, independientemente del ámbito en el cual se encuentren.
1.4 Objetivos

1.4.1 Objetivos Generales

- Estudiar las diferentes metodologías de implantación de la seguridad en redes inalámbricas locales.

- Difundir las mejores prácticas para la implantación de seguridad en redes inalámbricas locales.

- Proveer a la comunidad académica y profesional un estudio amplio de las distintas metodologías existentes para la implantación de la seguridad en redes inalámbricas locales, que pueda servir de guía práctica para la puesta en marcha de este tipo de tecnologías de comunicación de datos en las organizaciones.

1.4.2 Objetivos específicos

- Realizar una investigación para identificar las metodologías de implantación de la seguridad en WLAN.

- Identificar los elementos claves que deben formar parte de una implantación de seguridad en WLAN.

- Estudiar los diferentes estándares y protocolos que conforman las WLAN.

- Recolectar información de los desarrollos más relevantes de soluciones para WLAN en lo que a las metodologías de implantación de seguridad se refiere..

- Aplicar las metodologías expuestas en la investigación al problema objeto de estudio.

1.5 Alcance

La presente investigación ha sido desarrollada con el propósito de dar a conocer las metodologías de implantación de seguridad en WLAN más populares en la actualidad, por lo que, la audiencia de esta investigación son especialmente...
administradores de redes, gerentes de informática/sistemas y profesiones afines, cuyo interés principal esté orientado a conocer los aspectos más resaltantes que deben tenerse en consideración al momento de implantar la seguridad de sus WLAN.

El estudio de las diferentes metodologías se concentra en las distintas opciones técnicas que desde el punto de vista operativo se deben tener en cuenta para implantar una solución de seguridad para una WLAN. Así mismo se sugieren algunas consideraciones desde el punto de vista de la planificación de un proyecto tipo para la implantación de la seguridad en WLAN. Los aspectos institucionales, económicos, financieros, ambientales y administrativos no han sido considerados en el presente trabajo de investigación.

1.6. Limitaciones

Debido a que la información disponible sobre este tema está cambiando continuamente, además de ser muy reciente, la obtención de bibliografía impresa actualizada fue un poco difícil, por lo que la mayor parte de las referencias pertenece a materiales publicados en Internet por organizaciones dedicadas a la elaboración de estándares, la investigación tecnológica y el desarrollo de soluciones de este tipo. (Dichas referencias se encuentran debidamente identificadas en la bibliografía, la cual provee toda la información necesaria para ubicar las fuentes de información referenciadas).
Capítulo 2. Fundamentos del trabajo

2.1. Bases teóricas

2.1.1 Redes inalámbricas de área local (WLAN, Wireless Local Area Network)

2.1.1.1 ¿Que es una red inalámbrica de área local o WLAN?

Las redes inalámbricas de área local son sistemas de comunicación de datos alternativos a las redes de área local (Local Area Network, por sus siglas en inglés) cableadas, cuyas características principales son la flexibilidad, el uso del aire mediante la tecnología de radiofrecuencias como medio de transmisión de los datos entre un cliente y otro en la red. Ellas representan una opción adicional a las redes de datos tradicionales ya que nos permiten darle conectividad de red a localizaciones físicamente remotas y aisladas donde es poco factible y costoso instalar cualquier forma de infraestructura cableada. Estas particulares características de las WLAN permiten a los usuarios finales moverse de un lado a otro dentro del espectro de alcance de la red inalámbrica, manteniéndose permanentemente conectados a los servicios y aplicaciones que existan en la red a la cual se encuentra conectado, así como también ofrecen a los administradores la portabilidad física de la red, lo cual permite trasladar las redes con sus usuarios al lugar que sea requerido dentro de la organización.

En su forma más simple, una WLAN está conformada por un transceptor, denominado punto de acceso (Access Point, AP por sus iniciales en inglés) y un dispositivo cliente, como se muestra en la figura 1. Estos AP están localizados en ubicaciones físicas distribuidas a lo largo de la organización y funcionan como centros de comunicaciones. Los clientes de red que cuenten en sus equipos terminales con un adaptador de red inalámbrico tendrán la posibilidad de transmitir datos desde y hacia los AP y, en consecuencia, desde el cliente hasta el servidor. Otro elemento importante es que se pueden incorporar más AP cerca de las fronteras de las áreas de cobertura de la WLAN, para así ampliar el alcance de la...
red. Las WLAN, haciendo la analogía con las redes de telefonía celular, se comunican mediante un conjunto de celdas, que al ser solapadas en sus periféricos, ofrecen la posibilidad a los administradores de la red de extender las áreas de cobertura. [11]

2.1.1.2 Origen de las redes inalámbricas locales

El origen de las redes de área local inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, que consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de dicha tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro esparcido, siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, la Comisión Federal de Comunicaciones (FCC, Federal Communications Comission), que es la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas Industrial, Científica y Médica (ISM, Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en espectro esparcido. ISM son unas bandas para uso comercial sin licencia: es decir, la FCC simplemente reserva la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. Para eso hay otras instancias.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN comenzaran a dejar el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando profundamente en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban
la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea
considerada realmente una red de área local. [10]

2.1.1.3. Medios de transmisión inalámbrica

Las redes inalámbricas de área local realizan la transferencia de datos entre
un punto de la red y otro haciendo uso de ondas electromagnéticas del espectro
de radiofrecuencia e infrarrojo. Los entes reguladores de las telecomunicaciones
en cada país, responsables de controlar la concesión de licencias para el uso del
espectro radioeléctrico, han dispuesto un conjunto de frecuencias para ser
utilizadas comercialmente sin necesidad de una licencia para ello. Como ya se
mencionó, estas bandas de frecuencia han sido identificadas con las siglas en
inglés ISM (bandas de uso industrial, científico y médico) e incluyen las bandas
900 MHz, 2.4 GHz y 5 GHz, ampliamente usadas por la mayoría de los
dispositivos de comunicación inalámbrica comerciales. Adicionalmente a estas
bandas de frecuencia están en estudio y prueba en algunos países, las bandas de
40-60 GHz, cuyas prestaciones se estiman son mucho más elevadas que las
bandas actualmente disponibles.

Para transferir datos mediante ondas electromagnéticas, existen distintos
tipos de medios de transmisión cada uno de los cuales tiene ventajas, desventajas
y limitaciones de los cuales haremos mención a continuación:

Sistemas Infrarrojos

Este tipo de sistemas no permiten ser utilizados para desarrollar soluciones
para redes inalámbricas de área local corporativas, por lo cual, su uso es
relativamente limitado. Los sistemas infrarrojos (IR) transmiten datos
aprovechando las frecuencias ubicadas cerca del espectro electromagnético de
luz visible, aunque por debajo de las frecuencias de ésta. La limitación más
importante que tiene este medio de transmisión es similar a la de la luz visible, en
el sentido de que no pueden penetrar objetos opacos como paredes, suelos y
techos. Esta característica restringe el alcance de este medio de transmisión inalámbrica de datos, a lo sumo dentro un mismo ambiente (habitación, oficina). Otra limitación de este sistema es que el dispositivo emisor y el receptor deben tener línea de vista sin interrupciones de ningún tipo para lograr la transmisión exitosa de los datos. Ambas características son la causa del limitado crecimiento de este tipo de sistemas. [11]

**Sistemas de radio de banda estrecha**

Estos sistemas envían y reciben datos de una única frecuencia de radio específica. Los usuarios de este tipo de sistema de transmisión se comunican en frecuencias distintas para evitar posibles interferencias en sus comunicaciones. En estos sistemas particularmente, el equipo receptor está configurado solamente para escuchar la frecuencia designada y se filtran las restantes. Estas características imponen a este sistema una limitación cuando otro transceptor hace uso de la misma frecuencia y dentro del mismo rango de cobertura donde otro usuario en el mismo momento esté realizando una transmisión, se producirá una interferencia y en consecuencia los datos se pierden o se corrompen. Adicionalmente, en algunos países existen regulaciones legales que implican la tramitación de una licencia ante las respectivas autoridades, para hacer uso de las tecnologías de banda estrecha. [11]

**Sistemas de radio de banda ancha: espectro expandido**

Este sistema de transmisión recorre la banda completa de frecuencias disponibles en el espectro (canal) para transmitir los datos de manera confiable y segura, así mismo la señal se distribuye de manera uniforme sobre una amplia gama de frecuencias, con lo que se consume más ancho de banda a expensas de alcanzar una mayor confiabilidad, integridad y seguridad de las comunicaciones. Esta manera de transmitir las señales disminuye, más no evita a los dispositivos la posibilidad de interferencias y los ruidos en las comunicaciones originados por la
presencia de otras señales, a diferencia del sistema de banda estrecha. Por supuesto que estas bondades tienen su costo relacionado dada la naturaleza del sistema de transmisión. Estos costos se reflejan a través de la presencia de mayores niveles de ruido y en consecuencia son señales más difíciles de detectar. Este sistema de bandas puede operar sin requerir licencia en las bandas 902 MHz hasta 928 MHz, 2.4 GHz hasta 2.48 GHz ó en el espectro de bandas comprendido entre las frecuencias que van desde 5.725 GHz hasta 5.850 GHz. Otra características de estos sistemas es que tienen un alcance de rango medio (aproximadamente de 30 hasta 300 metros) y una baja capacidad de transmisión (típicamente 0.1 Watt). Así mismo, las comunicaciones pueden ser significativamente más rápidas que el sistema de radio de banda estrecha, alcanzando hasta 54 Megabits por segundo de velocidad de transmisión de datos a 2.4 GHz ó 5.8 GHz.

Existen dos tipos de expansión de espectro, Expansión de Espectro por Salto de Frecuencia (FHSS, Frecuency-Hopping Spread Spectrum) y la Expansión de Espectro por Secuencia Directa (DSSS, Direct-Sequence Spread Spectrum). La primera más económica de implantar, sin embargo, la secuencia directa tiene un potencial superior importante de utilización debido a que provee mayores velocidades de transmisión de los datos, posee una gama más amplia de cobertura y cuenta con unas elevadas capacidades para la corrección de errores con respecto al sistema por salto de frecuencia. [11]

**Expansión de espectro por salto de frecuencia (FHSS, por sus siglas en ingles)**

En este sistema se hace uso de una señal portadora a la cual son asociados los datos, con lo que se mitigan exitosamente los efectos de las interferencias sobre la señal. Esta portadora modulada en función del tiempo va saltando por toda la banda de una frecuencia a otra. Existe en cada transductor un código programado que define el orden y el valor de las frecuencias que son utilizadas para el salto. Tanto el receptor como el emisor de la señal deben estar
configurados con el mismo código de salto para garantizar la comunicación y el envío correcto de señales en el momento y frecuencia adecuada. El resultado creado por los transceptores funcionando en total sincronía en la práctica, es un canal lógico de comunicaciones (en la banda de 2.4 a 2.48 GHz) con velocidades de transmisión de datos de hasta 2 ó 3 Mbps y un rango de alcance de hasta 300 metros, sin necesidad de repetidores

Para que se presente una interferencia en la comunicación de una señal de un sistema de banda estrecha, será necesario difundir dicha señal en la misma frecuencia y al mismo tiempo que la señal que está saltando.

En el FHSS, cuando se producen errores en la transmisión en una frecuencia en particular, se retransmite la señal usando una frecuencia distinta en el salto que sigue a continuación. Cuando los receptores no están programados con códigos de salto similares las transmisiones de señales FHSS se asemejan a ruidos de breve duración. Dentro de una WLAN, se pueden utilizar diferentes códigos de salto para diferenciar las distintas subredes de la red y evitar que las señales interfieran entre sí.

Las redes inalámbricas basadas en el sistema FHSS son altamente recomendables cuando la pauta sea la facilidad de instalación en instalaciones donde se requieren muchos clientes, independientemente si la instalación se realiza al aire libre o en áreas interiores relativamente abiertas. [11]

Expansión de espectro por secuencia directa (DSSS, por sus siglas en inglés)

La expansión de espectro por secuencia directa es una técnica de modulación de señales para sistemas de comunicación inalámbrica en la que se incorpora un patrón de bits para cada bit que es transferido durante una comunicación (bits redundantes). Estos bits son denominados chirps o también código de chip. Cuando este patrón de bit redundante se incluye en la
comunicación, un receptor es capaz de realizar la recuperación de datos dañados sobre las señales que han sido transmitidas, las cuales están basadas en técnicas de análisis estadístico. Por consiguiente, al hacer uso de una mayor cantidad de bits en el código de chirp, disminuye la probabilidad de que se vea afectada la información a causa de interferencias en la comunicación.

Sin embargo, al incrementar la cantidad de información que se requiere transmitir, DSSS requiere un ancho de banda mayor para llevar a cabo la transmisión de los datos, generalmente haciendo uso de dos de tres frecuencias que no están solapadas para realizar la comunicación. Esta particularidad relativa a la corrección de errores evita que estos sistemas deban retransmitir los datos que puedan haberse visto afectados mientras transitaban a través del medio. Así mismo esta importante característica permite que mediante esta tecnología se alcancen velocidades de transmisión de hasta 11 Mbps y rangos de varios kilómetros de cobertura. [11]

**División de frecuencia por multiplexación ortogonal (OFDM, por sus siglas en inglés)**

Es una técnica de modulación FDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio. OFDM divide la señal de radio en muchas sub-portadoras que son transmitidas simultáneamente hacia el receptor en diferentes frecuencias. OFDM reduce la diafonía (efecto de acoplamiento entre canales) durante la transmisión de la señal.

Normalmente la modulación se realiza tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos durante la transmisión, entonces esta modulación se denomina COFDM, del inglés Coded OFDM. Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras equiespaciadas que forman una modulación de este tipo, los procesos de modulación y demodulación se
realizan en tiempo discreto mediante la aplicación de funciones matemáticas avanzadas (Transformada Discreta del Coseno DCT, IDCT, entre otras).

Esta técnica de transmisión de señales inalámbricas se utiliza en 802.11a WLAN, 802.16, WiMAX (Worldwide Interoperability for Microwave Access) y, en Europa, en PLC (Power Line Communications). [3]

2.1.1.4. Como trabajan las WLAN

Para enviar y recibir datos de un extremo al otro de la conexión, se utilizan ondas de radio o infrarrojos para utilizando el aire como medio de transmisión. Los datos a transmitir se superponen a la señal portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Para extraer los datos, el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de red de área local (LAN) sin cable los puntos de acceso (AP), se conectan a la red cableada de un lugar fijo mediante cableado. Seguidamente, el punto de acceso recibe la información, la almacena y la transmite desde la WLAN hacia la red LAN alámbrica. Ver figura 1.


Los AP pueden manejar un grupo pequeño o grande de usuarios y funcionar en un rango de cobertura desde al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en el cual se obtenga la cobertura de radio deseada según el requerimiento de la instalación.
El usuario final accede a la red WLAN a través de adaptadores de red inalámbricos, los cuales utilizan los protocolos de comunicación IEEE 802.11.

Estos dispositivos activos de red proporcionan una interfaz entre el sistema de operación de red del cliente y las ondas electromagnéticas, vía una antena. [3]

2.1.1.5 Infraestructura WLAN


Puntos de acceso inalámbrico (AP, Access Point): Este elemento de red permite a los dispositivos inalámbricos el acceso a la red cableada corporativa. Los AP son colocados generalmente detrás del firewall\(^2\) corporativo, es decir, fuera del dominio de colisión de la red interna, para así permitir el acceso conveniente a la red, sin embargo se incrementa con esta acción la vulnerabilidad de la red a ataques de seguridad. Los AP disponibles en la actualidad soportan

---

\(^2\) Firewall es un elemento de hardware o software utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.
diferentes tipos de WLAN, por ejemplo 802.11g, algunos inclusive están habilitados para soportar hasta los 3 estándares vigentes (802.11b/g/a).

**Dispositivos móviles: Asistentes personales digitales** (PDA, por sus siglas en inglés), computadores portátiles, computadores portátiles tipo tabla, teléfonos inalámbricos para voz sobre IP y muchos otros dispositivos similares que brindan a los usuarios la posibilidad de moverse con su equipo inalámbrico sin dejar de hacer sus labores de trabajo en la organización. Sin embargo, deben ser dispositivos que soporten la interacción con redes inalámbricas para que puedan funcionar dentro de las WLAN.

**Tarjeta con interfaz a la red inalámbrica:** Para comunicar los dispositivos móviles con los AP dispuestos a lo largo de la organización, se requiere una tarjeta de red que sea capaz de establecer contacto con el AP, mediante señales de radio frecuencia en las bandas establecidas por el estándar WLAN seleccionado para operar en la red. De igual forma que en las redes LAN, las tarjetas de red inalámbrica cuentan con un identificador físico único denominado MAC Address, el cual generalmente se utiliza para procesos de autenticación del dispositivo en la red. Así mismo como existen AP duales, también existen tarjetas de red con interfaz inalámbrica duales.

El cuarto elemento que conforma la infraestructura de la WLAN son los **servidores de seguridad**, quienes son responsables de gestionar las políticas de seguridad establecidas por la organización, para asegurar el control de los activos de información, de manera que los usuarios tengan acceso a la información corporativa que se adapte mejor a su perfil de cargo y por ende a sus alcances y responsabilidades dentro de estructura de la institución a la cual pertenezca. Adicionalmente en estos servidores reposa generalmente la responsabilidad de brindar servicios de autenticación, autorización y contabilidad/auditoría (AAA) a usuarios y/o clientes externos al dominio de la red interna de la organización, por
lo cual este elemento es clave para garantizar la seguridad de los activos de información de la organización. En estos servidores, también suelen colocarse herramientas de software sofisticadas y de propósito específico para incrementar la seguridad tales como Redes Privadas Virtuales (VPN, Virtual Private Network), Sistema de Detección de Intrusos (IDS, Intrusion Detection System) Sistema de Prevención de Intrusos (IPS, Intrusion Prevention System), Corta fuegos (Firewall), entre otros.

2.2.1.6. Estándares en WLAN

En el área de los estándares para WLAN, instituciones como el IEEE\(^3\), la Wi-Fi Alliance\(^4\), han trabajado fuertemente sobre las diferentes características que la seguridad debe cumplir, como parte de las especificaciones de las WLAN. Sin embargo, se ha descrito siempre la seguridad en los diferentes estándares para WLAN, como una opción y esto se debe fundamentalmente al hecho de que principalmente ha sido percibida como un obstáculo para incrementar la velocidad de transmisión de los datos, por lo cual se ha venido dejando en segundo plano, a pesar de estar en conocimiento que representa un mecanismo apropiado y necesario para la protección de la red. Esto origina una situación peligrosa, debido al hecho de dejar en manos del usuario final, la responsabilidad de velar por la seguridad de las comunicaciones inalámbricas, donde los avances alcanzados en los estándares aún son insuficientes. En tal sentido, en la presente investigación se hace referencia de forma resumida a los estándares que sustentan las WLAN; sin embargo se hace énfasis especialmente en los mecanismos de seguridad utilizados para cada situación.

El siguiente cuadro resume los estándares de WLAN y sus características principales en lo que respecta a velocidad de transferencia, banda de frecuencia que utiliza, esquema de modulación de frecuencias, seguridad, ventajas y

---

\(^3\) IEEE Instituto de Ingenieros Eléctricos y Electrónicos
\(^4\) Wi-Fi Alliance Grupo de trabajo con su propia marca (Wireless Fidelity, Wi-Fi)
desventajas de cada uno, así como algunas otras informaciones relevantes:

<table>
<thead>
<tr>
<th>Estándar</th>
<th>Tasa de Transferencia</th>
<th>Esquema de Modulación</th>
<th>Seguridad</th>
<th>Ventajas/Desventajas y otras informaciones</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>Hasta 2Mbps en la banda de 2.4GHz</td>
<td>IR, FHSS ó DSSS</td>
<td>WEP y WPA</td>
<td>Esta especificación ha sido extendida también para el estándar 802.11b.</td>
</tr>
<tr>
<td>IEEE 802.11b (Wi-Fi)</td>
<td>Hasta 11Mbps en la banda de los 2.4GHz</td>
<td>DSSS con CCK</td>
<td>WEP y WPA</td>
<td>Los equipos que utilizan el estándar, no interoperan con los equipos configurados con el 802.11a. Se necesitan menos AP que en 802.11a para cubrir largos espacios. Permite gran velocidad de acceso a los datos hasta los 100 metros desde el equipo hasta la estación base. Dispone de 14 canales en la banda de frecuencia de 2.4GHz, solamente con tres canales en los que no se solapan las señales.</td>
</tr>
<tr>
<td>IEEE 802.11g (Wi-Fi)</td>
<td>Hasta 54Mbps en la banda de los 2.4GHz</td>
<td>OFDM above 20Mbps, DSSS con CCK below 20Mbps</td>
<td>WEP y WPA</td>
<td>Ha reemplazado al estándar 802.11b. Adiciona facilidades de seguridad sobre 802.11. Compatible con 802.11b. 14 canales disponibles (de acuerdo al continente: USA 1-11, Europa 1-13, Japón 14 canales) en la banda de los 2.4GHz con tres canales en los que no es posible solapar las señales.</td>
</tr>
<tr>
<td>IEEE 802.11i (Wi-Fi)</td>
<td>Es el estándar que proporciona seguridad adicional a las redes WLAN.</td>
<td>No aplica</td>
<td>WPA y WPA2</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------</td>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
</tbody>
</table>

Especifica mejoras en la seguridad de las redes de área local (LAN) inalámbricas. En el estándar WPA se requiere autenticación 802.1x. En el estándar 802.11, la autenticación 802.1x era opcional. En entornos sin una infraestructura de servicio de usuario de acceso telefónico de autenticación remota (RADIUS), WPA admite el uso de una clave compartida previamente. En los entornos con una infraestructura RADIUS, se admiten el Protocolo de Autenticación Extensible (EAP) y RADIUS. Para el estándar 802.11, el cifrado de Privacidad Inalámbrica Equivalente al cable (WEP) es opcional. Para WPA, se requiere el cifrado con el protocolo TKIP. El protocolo TKIP sustituye a WEP con un algoritmo de cifrado nuevo más seguro. Con WPA, un método conocido como Michael especifica un nuevo algoritmo que calcula un código de integridad de mensaje (MIC) de 8 bytes con las utilidades de cálculo disponibles en los dispositivos inalámbricos existentes. WPA define el uso del estándar de cifrado avanzado (AES) como sustituto adicional para el cifrado de WEP. [10]
IEEE 802.1X | Especifica los mecanismos de control de acceso a la red. | No aplica | No aplica | Utiliza Protocolo de Autenticación Extensible (EAP), el cual soporta múltiples métodos de autenticación. Especifica como EAP debe ser encapsulado en las tramas LAN. Define tres elementos principales que son: Dispositivos inalámbricos (solicitantes de autenticación en la red, se denominan “Suplicantes”), Puntos de Acceso Inalámbricos (Actúan como intermediarios en el proceso de autenticación, se denominan “Autenticador”) y Servidor de Autenticación (es el responsable de llevar a cabo la autenticación). Se caracteriza por renovar las claves de autenticación periódicamente. Provee autenticación solamente del lado del cliente. No protege adecuadamente la WLAN de ataques como “hombre en el medio”. [11]

<table>
<thead>
<tr>
<th>Estándar</th>
<th>Tasa de Transferencia</th>
<th>Esquema de Modulación</th>
<th>Seguridad</th>
<th>Ventajas/Desventajas y otras informaciones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth</td>
<td>&lt;1 Mbps en la versión 1.1 y asta 3Mbps en la versión 2.2 de Bluetooth, en la banda de los 2.45GHz</td>
<td>FHSS</td>
<td>PPTP, SSL ó VPN</td>
<td>No soporta IP en su forma nativa, por lo que tampoco soporta bien TCP/IP ni aplicaciones WLAN. Funciona muy bien para interconectar dispositivos móviles como PDA, teléfonos celulares y PCs en intervalos de distancia cortos.</td>
</tr>
<tr>
<td>Radiointerface</td>
<td>Speed Capacity</td>
<td>Frequency Band</td>
<td>Encryption/Authentication</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Radio Frecuencia Local (HomeRF)</td>
<td>Hasta los 10Mbps en la banda de los 2.4GHZ</td>
<td>FHSS</td>
<td>Direcciones IP independientes para cada red, los datos son enviados con un algoritmo de encriptamiento de al menos 56 bits.</td>
<td>HomeRF no está ampliamente soportado por los fabricantes o grupos de trabajo. Se utiliza generalmente en casa y no en empresas. Su rango de cobertura es de 50 metros solamente desde la estación base. Los costos para implantarlo y mantenerlo son mínimos. La calidad de la voz es siempre buena, debido que continuamente reserva una porción del ancho de banda para servicios de voz. Responde bien a las interferencias debido al sistema de transmisión de señales que lo soporta.</td>
</tr>
<tr>
<td>HiperLAN/1 (Europa)</td>
<td>Hasta los 20Mbps en la banda de los 5,8GHz</td>
<td>CSMA/CA</td>
<td>Encriptamiento y autenticación individual encada sesión.</td>
<td>Se utiliza solamente en Europa. HiperLAN es totalmente ad-hoc, no necesita configuración ni un controlador principal para funcionar. Relativamente costoso para operarlo y mantenerlo. No garantiza el ancho de banda.</td>
</tr>
<tr>
<td>HiperLAN/2 (Europa)</td>
<td>Hasta 54Mbps en la banda de los 5,8GHz</td>
<td>OFDM</td>
<td>Cuenta con características muy fuertes de seguridad que soportan sesiones individuales de autenticación y claves de encriptación para cada sesión.</td>
<td>Se utiliza solo en Europa. Está diseñado para transportar celdas ATM, paquetes IP, paquetes Firewire (IEEE 1394) y voz digital (de teléfonos celulares). Mejor calidad de servicio que HiperLAN/1 y garantiza el ancho de banda.</td>
</tr>
</tbody>
</table>

OpenAir | Protocolo | CSMA/CA con | OpenAir no | OpenAir es un

---

Estudio de metodologías de implantación de la seguridad en redes inalámbricas de área local
Universidad Metropolitana, Postgrado de la Facultad de Ingeniería, Caracas - Venezuela
24

| antecesor al 802.11, usando FHSS. Alcanza entre 0.8 y 1.6 Mbps | retransmisión de MAC | implanta ningún tipo de encriptamiento en la capa de física pero genera identificadores de red basados en un password. | protocolo propietario de Proxim. Todos los productos OpenAir están basados en módulos Proxym. |

2.2.1.7. Futuro de las redes inalámbricas de área local

Imagínese en una conferencia, lejos de su puesto de trabajo, pero urgido de una información que requiere para completar la presentación que le corresponde. Usted cuenta con un computador portátil el cual dispone de una tarjeta de red inalámbrica segura. Seguidamente se conecta a la intranet de su organización, ubica la información que necesita, la imprime y se la muestra a su cliente el cual queda gratamente impresionado por la efectividad y la manera simple como usted consiguió la información, sin importar mucho su ubicación física dentro del campus de la organización.

Ahora imagine que usted es un doctor o algún otro profesional de la salud con un paciente en cama y en ese momento le corresponde recetarle un medicamento a su paciente para lo cual debe consultar la historia médica, los tratamientos previos, las veces que ha asistido a su consulta.

Usted cuenta con un computador portátil tipo tablet con acceso a la red inalámbrica por lo cual, de forma inmediata acaba de usar su computador para hacer todas esas acciones de solicitud, búsqueda e ingreso de información, allí, al lado de su paciente, al que usted le ha ahorrado minutos y quizás horas de espera interminable en cama y le ha brindado al centro de salud la oportunidad de multiplicar el valor de esa cama al colocarla próximamente disponible, sólo por el hecho de hacer uso de la WLAN.
Suponga ahora que se encuentra en el piso o en el cuarto de control de una planta industrial pero necesita en tiempo real información relacionada con el inventario disponible de alguna de las piezas que produce su planta o el estado de la producción de sus equipos industriales. Sencillamente a través de la WLAN usted podrá conectarse a sus sistemas y rápidamente ubicar esta información y así tomar una decisión que le permitirá a su organización elevados niveles de competitividad en el sector de mercado en el que se encuentre su industria.

Y así como estas tres situaciones hipotéticas, existe una diversidad considerable de situaciones en las que el uso de las WLAN es ampliamente recomendable por lo que se ha venido incrementando vertiginosamente su presencia en la vida cotidiana de hoy. Un estudio de Gartner Group del año 2002 proyecta que el uso de las WLAN en los Estados Unidos será más del doble para el año 2006 y es sencillo visualizar el porqué de este fenómeno. [3]

![Figura 3. Proyección de crecimiento de usuarios WLAN](image)

En los inicios las áreas de venta, distribución y manufactura adoptaron las WLAN en una mayor cantidad. Sin embargo, el crecimiento proyectado señala un cambio en esta tendencia inicial que apunta hacia el mercado de las corporaciones y empresas, el sector de las telecomunicaciones y los proveedores de acceso a servicios públicos.

---

5 Gartner Group (compañía de investigación de Tecnologías de Información a nivel mundial).
Sin embargo, estas facilidades relativas a la flexibilidad y movilidad conllevan a inherentes amenazas de seguridad, a pesar de proporcionar un esquema de conectividad muy versátil y utilizable tanto para usuarios como para los sistemas, debido a que los datos son enviados haciendo uso de rutas aéreas, la interceptación de los datos y el acceso a los recursos de la red, representan potenciales riesgos para la seguridad del entorno de la WLAN.

2.2.1.9. Vulnerabilidades más comunes en la seguridad de las WLAN

Esta situación ha sido una de las causas principales de la limitada expansión de las WLAN, ya que la mayoría de los responsables de las áreas de tecnología en las empresas, evitan dar el salto hacia las redes inalámbricas porque tienen alguna de las siguientes percepciones:

- WLAN no es seguro.
- WLAN es muy complicado.
- WLAN es inestable.
- WLAN es costoso.

Dichas percepciones están basadas en que la mayoría de las
implantaciones de WLAN han sido realizadas con miras a disfrutar de los beneficios que la movilidad ofrece a los usuarios; también se ha asumido, en algunos casos, que todo aquel que accede a la red inalámbrica es de confianza puesto que forma parte de la organización. En la realidad no siempre es así. En general, las organizaciones dan por sentado que sus redes son seguras, lo cual es un grave error. A pesar de contar con soluciones de seguridad para encriptamiento de los datos y autenticación de usuarios y servicios, aún así el riesgo permanece, sobre todo porque el porcentaje más común de huecos en la seguridad son creados precisamente por los llamados “bien conocidos e interesados empleados” de la organización.

A continuación se listan las vulnerabilidades de seguridad más comunes en comunicaciones WLAN:

**Accesos no autorizados:** Intrusos con malas intenciones intentan penetrar mediante diferentes tipos de ataques de seguridad, en la WLAN. Entre los ataques más utilizados, se tiene:

“**Sniffing**”: Se utiliza este término cuando el tráfico de la red está siendo monitoreado. En las WLAN la información trasmitida por los AP es fácil de monitorear debido a que los datos muchas veces viajan como texto en claro y completamente desprotegidos. En el momento en el que un intruso obtiene datos vitales que comprometen la seguridad de la WLAN, pueden hacerse pasar como usuarios de la organización para robar información vital de la empresa.

“**Spoofing**”: Significa suplantación. Sucedé cuando un intruso se hace pasar por un dispositivo de la red robando sus credenciales. Por ejemplo, el intruso hace espionaje de la red, ubica la “DIRECCIÓN MAC” de un verdadero dispositivo en la WLAN y luego intenta interactuar desde otro equipo diferente pero con la MAC robada con el AP haciéndole pensar que en verdad es un usuario autorizado.
“Jamming”: Se introducen interferencias con señales de radio que dejan al AP inhabilitado para atender peticiones de los dispositivos de la WLAN, perturbando aquellas áreas de la organización que hagan uso de la WLAN para sus actividades del día a día. El estándar 802.11 es susceptible a este tipo de ataques debido a la banda de frecuencia en la cual opera. Pueden ser intencionales o accidentales.

“Session Hijacking”: En este tipo de ataque el intruso intenta aparecer como un usuario legítimo de la WLAN, que se está conectando en ese momento con el AP debido a que recientemente fue desconectado. En el interín de la negociación, el intruso se conecta a la WLAN, dejando tanto al administrador de la red como al verdadero usuario en total oscuridad.

Negación de Servicio: Una vez que el intruso ha logrado ingresar a la red, puede fácilmente inundar la WLAN con tráfico basura, el cual, eventualmente ocasionará la caída de la WLAN. Este ataque puede ser realizado de muchas formas, por ejemplo mediante continuas solicitudes de acceso a la WLAN, luego de haber recibido con anticipación la respuesta de aprobación de acceso.

Hombre en el medio: En este caso, el intruso cambia los valores de configuración de su dispositivo inalámbrico para convertirlo en un falso AP. Todo el tráfico proveniente de los dispositivos de los usuarios autorizados es forzado a viajar a través de este dispositivo, quien actúa como un pseudo-AP. De esta manera, el intruso puede ver todas las credenciales de los usuarios y luego hacer spoofing a la WLAN. Esto es posible gracias a que las especificaciones para WLAN proveen sólo autenticación del lado del cliente. La autenticación en el AP está desactivada o no configurada por defecto, por lo que no hay manera para el cliente de asegurarse que está conectándose a uno de los AP legítimos de la WLAN.
La cobertura física de los servicios de la WLAN, dependen de la especificación utilizada. En muchos casos, la cobertura excede las fronteras físicas de la organización, lo cual, permite a los intrusos realizar ataques inclusive desde los propios estacionamientos de las organizaciones. Es conocido por mucha gente que se pueden utilizar antenas hechas en casa para detectar el tráfico que proviene de los AP y que éstas pueden estar colocadas a mucha distancia, con lo cual se puede penetrar y acceder gratis, por ejemplo, a Internet.

**WLAN Rogue:** Los AP son el medio a través del cual los dispositivos inalámbricos pueden obtener información de la red corporativa de la organización. Así mismo, los AP son el último elemento cableado de la red corporativa de la organización y el comienzo de la red inalámbrica, por decirlo de alguna manera. Por tal razón, todos los puntos de acceso de la red inalámbrica deben ser conocidos, controlados e inventariados por el administrador de la red, dado el bajo costo de estos dispositivos, cualquier empleado puede adquirir uno, instalarlo y levantar su propia WLAN no autorizada, con lo cual, dadas las vulnerabilidades por las configuraciones de fábrica que por defecto tienen los AP, automáticamente se abren a través de ellos dispositivos brechas de seguridad en la red.

El problema más grave de estas vulnerabilidades es que si no se logran detectar estos dispositivos, pueden convertirse en una puerta abierta para la salida de información clave de la organización, debido a que los intrusos generalmente van más allá del libre y gratuito acceso a Internet, tomando ventaja de la situación para extraer inclusive información confidencial. Por tanto, es imperativo identificar, descubrir y eliminar estos dispositivos de la WLAN y tomar las medidas necesarias para mitigar el riesgo al máximo.

Un método para detectar AP no autorizados es mediante radio frecuencia y analizadores de espectro o sniffing. Este método obliga al personal de seguridad a caminar alrededor de la ubicación física de la WLAN implantada e intentar detectar
los AP no autorizados localizando el punto de emisión de las señales de radio frecuencia. Sin embargo, esta estrategia es poco práctica en edificaciones extensas.

Otra manera de identificar los AP no autorizados es utilizando soluciones de software, lo cual, es una vía más práctica y dinámica para identificar la ubicación y estado de los AP de la WLAN, y determinar cuales están autorizados y cuales no, usando políticas previamente implantadas para ejecutar, por ejemplo, el apagado del puerto en el switch de la red LAN donde está conectado el AP no autorizado.

También se pueden combinar ambas metodologías para obtener mejores resultados en aquellos casos donde sea posible.

Es recomendable que los administradores de la WLAN establezcan mecanismos y medidas apropiadas en sitio para detectar y prevenir el uso de AP no autorizados en las organizaciones.

**Dispositivos inalámbricos y seguridad de usuario:** Los dispositivos inalámbricos móviles, en muchos casos, son propiedad de los usuarios. En tal sentido, los administradores de la seguridad deben garantizarle a la organización que sólo aquellos dispositivos aprobados podrán ser utilizados en la WLAN y únicamente el personal autorizado tendrá permitido usar esos dispositivos.

**Recuperación desde dispositivos y pérdidas de información:** Los dispositivos inalámbricos, tales como computadores portátiles, agendas electrónicas portátiles (PDA) y teléfonos celulares, entre otros, tienen un alto riesgo de extraviarse, perderse o ser robados, precisamente por su naturaleza portátil. Sin embargo, el costo de remplazar el dispositivo es menor que el generado por la perdida de la información en ellos contenida. En tal sentido, es recomendable adoptar medidas para implantar la autenticación de los dispositivos inalámbricos y la protección de la información en ellos almacenada, mitigando así
los riesgos de seguridad relacionados, evitando de esta manera que la información llegue a manos equivocadas. Para ello, las aplicaciones responsables de la administración de los dispositivos deben proveer una forma remota de bloquear los dispositivos cuando no estén siendo utilizados. Así mismo, una vez que es recuperado un dispositivo o cuando se incorpora un equipo a la WLAN, los datos deben ser restaurados a su estado original, tal y como estaba antes del extravío del dispositivo.

Dispositivos en desuso: La distribución de software hacia los dispositivos móviles debe realizarse de manera segura a través de la red, de tal forma de mantener al día las versiones de software que ejecutan los usuarios en sus equipos terminales. En tal sentido, es recomendable que los administradores de red tengan la posibilidad de consultar, cuando así lo deseen, los inventarios de hardware y software de los dispositivos existentes a fin de poder garantizar el uso apropiado y el respectivo control de los dispositivos de la institución. De esta forma, si una aplicación ha sido instalada sin autorización, los administradores de la red podrían recibir una alerta de esta anomalía y proceder a desinstalar dicho software remotamente. Así mismo, sucede en el caso contrario cuando se dañe, corrompa o accidentalmente se borre una aplicación, se podría realizar la reinstalación remotamente y reestablecer el equipo a su estado original.

Control de acceso según en el contexto: La seguridad en WLAN forma parte de la política integral de una organización, por lo que es crucial contar tanto con un inventario de los dispositivos y sus credenciales como con la información de los usuarios que utilizan dichos dispositivos y la relación existente entre ellos. Esta clase de información generalmente es almacenada en un directorio, donde se aplican políticas de seguridad y control de acceso a los recursos de acuerdo al contexto del dispositivo y del usuario dentro de la institución.

Ataques por virus y códigos maliciosos: Día tras día, la contaminación de las aplicaciones con códigos maliciosos o virus se ha convertido en una
vulnerabilidad de seguridad importante de las redes corporativas. Sin embargo, hasta la fecha son pocos los virus y códigos maliciosos que han afectado las plataformas de las agendas electrónicas portátiles (PDA), pero es razonable esperar que esta situación cambie radicalmente en el tiempo a medida que incremente la popularidad de estos sistemas móviles como resultado de la presencia de WLAN en las empresas. Por tal motivo, debe tenerse en cuenta que al momento de sincronizar estos dispositivos con los equipos de escritorio, existe la posibilidad de transferir archivos contaminados que luego pudieran infectar la red corporativa. En consecuencia, deben existir mecanismos, herramientas y procedimientos para proteger los activos de información de este tipo de ataques por virus y códigos maliciosos.

2.2.1.10. Seguridad en WLAN

A pesar de todas estas vulnerabilidades, las WLAN cuentan hoy en día con un conjunto de herramientas y mecanismos de seguridad bastante diverso y amplio. Sin embargo, para garantizar la seguridad de una red son necesarios no solamente los controles técnicos sino un conjunto de elementos entre los que están políticas, normas y procedimientos de seguridad, ética y competencia tanto de las personas que se encargan de la red como de las que pueden acceder a ella. En este sentido, en las siguientes secciones de este capítulo, se exponen en detalle cada uno de los elementos que conforman la seguridad en las WLAN, protocolos de seguridad, seguridad física, mecanismos para proveer seguridad y algunas metodologías disponibles para implantar la seguridad en estas redes.

2.2.1.10.1. Protocolos de seguridad en WLAN

El medio de transmisión de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las
mismas precauciones que se tienen para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Conscientes de este problema, el IEEE [15] publicó un mecanismo opcional de seguridad, denominado privacidad equivalente a la provista por cable (WEP, Wired Equivalent Privacy), en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.

Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i, que permitiera dotar de suficiente seguridad a las redes WLAN, la cual, fue publicada en junio de 2004.

El problema de 802.11i fue su tardanza para ser publicado. Algunas empresas en vista de que el protocolo WEP (de 1999) era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías como redes privadas virtuales (VPN, Virtual Private Network) para asegurar los extremos de la comunicación (por ejemplo, mediante IPSec, es decir IP Seguro). La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. Pero la tecnología VPN es quizás demasiado costosa en recursos para su implantación en redes WLAN.

En tal sentido y no ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi, decidió lanzar un mecanismo de seguridad intermedio de transición hasta que estuviese disponible 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados del desarrollo de la norma. El resultado, en el año 2003, fue el protocolo de fidelidad inalámbrica con acceso protegido (WPA, Wifi Protected Access). Posteriormente en junio de 2004, justo antes de la aprobación del estándar IEEE 802.11i, surgió el protocolo de fidelidad inalámbrica con acceso protegido versión 2 (WPA2, Wi-Fi Protected Access) en el que se combinan las diferentes técnicas que mitigan los problemas de WEP que
comprenden las áreas de autenticación (IEEE 802.1X, EAP), chequeo de integridad de datos (TKIP) y chequeo de integridad de mensaje (MIC).

A continuación se analizan las características de los mecanismos de seguridad anteriormente mencionados:

**Especificación original IEEE 802.11**

La especificación original del estándar IEEE 802.11 utiliza tres mecanismos para proporcionarle seguridad a la WLAN que son identificador de servicio (SSID), filtrado con dirección MAC (Control de acceso al medio) y WEP (Wired Equivalent Privacy, su traducción en inglés).

- **SSID (Identificador de Servicio):** El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste de un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

  Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (Basic Service Set Identifier), mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (SSID extendido). Se puede referir a cada uno de estos tipos como SSID en términos generales. Generalmente el SSID se le conoce como nombre de la red.

- **Filtrado con dirección MAC (Control de Acceso al Medio):** restringe el acceso a computadoras donde la dirección MAC de su adaptador de red (NIC), está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico.
**WEP (Wired Equivalent Privacy):** diseñado para proporcionar privacidad a las comunicaciones inalámbricas de extremo a extremo, similar a que se usa en una conexión cableada. Este protocolo funciona compartiendo una clave secreta entre los distintos dispositivos inalámbricos y el punto de acceso, con la cual los datos son cifrados mediante el algoritmo RC4 y se usa código de redundancia cíclica (CRC) de 32 bits para chequear la codificación. La clave secreta está compuesta de dos elementos: una clave WEP de 40 o 104 bits y un número aleatorio de 24 bits denominado vector de inicialización (IV). El cifrado funciona tanto para claves de 64 bits como para claves de 128 bits. La clave resultante se inserta en un generador de números seudoaleatorios generando un flujo de clave. Antes de enviar la clave al receptor, el emisor combina el flujo de clave emitida por el generador con el texto en claro que se va a enviar, haciendo una operación XOR, obteniendo como resultado el texto cifrado que será transmitido al receptor.

![Figura 5. Codificación en WEP](image1)

![Figura 6. Decodificación en WEP](image2)
Cuando el receptor recibe el texto cifrado, este utiliza el vector de inicialización y una copia propia de la clave secreta para generar un flujo de clave idénticamente igual al generado por el emisor. Seguidamente el receptor combina el flujo de clave con el texto cifrado recibido y obtiene como resultado el texto en claro originalmente enviado por el emisor.

**Autenticación en WEP**

Los dos niveles de autenticación WEP son:

- **Sistema abierto**: Este esquema permite que todos los usuarios ingresen a la red inalámbrica.
- **Autenticación con clave compartida**: Este es el modo más seguro que controla acceso a la LAN inalámbrica y busca evitar que piratas informáticos ingresen en la red.

![Figura 7. Modos de autenticación WEP](image)

La autenticación con clave compartida usa una clave secreta que es compartida por todos los usuarios y puntos de acceso a la red inalámbrica.
Cuando un usuario intenta conectarse a un punto de acceso, se le responde con una solicitud de autenticación. La estación de trabajo inalámbrica utiliza su clave secreta compartida para codificar este texto, responderle al punto de acceso y así autenticarse en la WLAN. Luego, el punto de acceso decodifica la respuesta utilizando la misma clave compartida y compara el resultado con el texto enviado inicialmente.

**Imperfecciones del protocolo WEP**

Sin embargo, es bien sabido que WEP tiene muchas fallas de seguridad, lo que pone en tela de juicio las afirmaciones sobre la seguridad que ofrece. A continuación se mencionan algunas de las imperfecciones más conocidas del protocolo, con lo cual queda bastante claro que es muy probable que WEP sólo sea recomendable usarlo en el futuro en conjunto con las redes privadas virtuales (VPN).

- **Claves inseguras:** La inseguridad con las claves se debe a que se comparten entre todas las estaciones y puntos de acceso en la red, por lo que su distribución es un problema. Cuando se utiliza la misma clave y se comparte con un número de usuarios, dicha clave ya no será secreta. La inseguridad de claves se resuelve configurando cada una de las estaciones inalámbricas con la clave secreta, en lugar de permitir que los usuarios ejecuten este procedimiento.

Sin embargo no hay garantía del 100% para esta solución debido a que la clave se almacena en la computadora del usuario. La mejor manera para defenderse contra las claves inseguras es migrar a una configuración del sistema que asigne una clave única para cada usuario en la computadora; las contraseñas deben de cambiarse regularmente, porque nunca se sabe cuando se comprometerá esa clave.
- **A mayor nivel de encriptación menor ancho de banda:** Como puede deducirse, agregar niveles de encriptación a la red reducirá el ancho de banda y la velocidad de conexión. Es importante cuantificar exactamente lo que cada nivel de seguridad cuesta en términos de velocidad:

1. La encriptación a 40 bits reduce el ancho de banda por lo menos en 1 Mbps.
2. La encriptación a 128 bits reduce el ancho de banda por casi 2 Mbps.

- **Clave comunitaria:** Todo usuario en la red inalámbrica puede usar la misma clave compartida, pero aún con autenticación, autorizar solamente un individuo no es posible porque todos son considerados un grupo usando la misma clave compartida para ingresar a la red. Si se tienen varios en la organización, esta “clave comunitaria” puede ser adquirida fácilmente y hay una gran posibilidad de que un usuario no autorizado ingrese a los recursos de la red. En la mayoría de los casos, la clave utilizada para autenticar usuarios es la misma que la usada para codificar datos. Esto puede constituirse en un gran agujero de seguridad para cualquier usuario inalámbrico, sin importar la plataforma. Cuando un pirata informático posee una copia de la “clave compartida” puede usarla para ingresar a la red y ver el tráfico de otros usuarios. Esto ocasiona aún más problemas. La mejor defensa contra este tipo de ataques es enviar claves separadas para autenticación y encriptación en el sistema.

- **Autenticación del mensaje:** El código de redundancia cíclica (CRC) elegido para la autenticación es débil debido a que fue diseñado para el control de errores y no para autenticación. Es posible modificar un mensaje tal que el CRC sea válido para el mensaje, pero no será el mensaje enviado. También pueden inyectarse mensajes en otros de la misma manera.
Reutilización de clave compartida: Debido a que la clave compartida es estática y raramente cambiada, la aleatoriedad de la clave compartida depende del valor del vector de inicialización (VI). Por tanto, cuando se reutiliza un vector de inicialización (VI), se tienen dos mensajes codificados con la misma clave compartida. A esto se denomina colisión. Teniendo en cuenta que el tamaño del vector de inicialización (VI) es de 24 bits, se producirán colisiones cada $2^{24}$ paquetes, es decir, se repetirá la clave compartida aproximadamente cada 16 millones de paquetes, por lo que puede montarse un tipo de ataque para obtener esa clave compartida utilizada.

Ataque por reutilización de la clave compartida: Lo primero es enviar un paquete conocido y cuando se recibe la respuesta se obtiene el texto cifrado y el vector de inicialización (VI). Por tanto, se cuenta con el texto en claro y el texto cifrado, por lo que es posible calcular la clave compartida de la siguiente forma $K = P \oplus C$. Ahora basta con crear una base de datos indexada por el vector de inicialización (VI) conteniendo las diversas claves compartidas obtenidos y, para cada mensaje visto en el futuro, el atacante tendrá la clave compartida con la que decodificará dicho mensaje.
- **Algoritmo de manejo de clave de RC4:** El principal problema es una debilidad en el modo en el que el algoritmo de encriptación RC4 se implanta en el WEP. El problema es que tener un texto conocido impregnado en la clave (por ejemplo el VI) conduce a claves débiles que generan texto cifrado conocido mediante el motor del algoritmo RC4, lo que permite al atacante crear un “motor inverso” que genere la clave a través de un texto cifrado conocido. Además, claves de mayor tamaño no solucionan el problema debido a que el ataque recupera cada byte de la clave por separado, ya que intenta decodificar la clave como un entero. Por tanto, el ataque crece linealmente y no exponencialmente como crecería la clave al aumentarla de tamaño.
Especificación del estándar IEEE 802.11i

Fidelidad Inalámbrica con Acceso Protegido (WPA, Wi-Fi Protected Access)

El acceso protegido para Wi-Fi o WPA, es una combinación de técnicas de autenticación (mediante la especificación establecida por el IEEE 802.1X), chequeo de cifrado de datos (mediante el uso del protocolo de integridad de clave temporal TKIP) y de mensaje (el protocolo de chequeo de integridad del mensaje Michael MMIC).

Autenticación IEEE 802.1X

802.1X es un mecanismo de control de acceso que funciona tanto para redes cableadas como inalámbricas. Se usa el protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) en combinación con RADIUS para autenticar clientes y distribuir claves. Básicamente el proceso de autenticación sucede a groso modo como se muestra en la figura 9.

Figura 9. Proceso de autenticación 802.1X en WPA/WPA2

El estándar IEEE 802.1X especifica cómo el protocolo EAP debe encapsular las tramas y también define tres miembros principales en la configuración:
1. **802.1X Solicitante** ("Supplicant"): representado por el dispositivo inalámbrico que solicita autenticación para acceder a la red.

2. **802.1X Autenticador** ("Authenticator"): representado por el punto de acceso (AP) que actúa como intermediario en el proceso de autenticación.

3. **802.1X Servidor de Autenticación** ("Authentication Server"): representado por el servidor que conduce el proceso de autenticación.

Una conexión WLAN usando 802.1X procede de la siguiente manera:

1. El usuario ("solicitante") solicita conectarse a la WLAN a través de un punto de acceso ("autenticador").

2. Seguidamente el punto de acceso ("autenticador") solicita la identidad del usuario y la transmite al "servidor de autenticación" usando el protocolo (RADIUS, Remote Authentication Dial-In User Service).

3. El "servidor de autenticación" le solicita al punto de acceso ("autenticador") una prueba de identidad del usuario. El punto de acceso ("autenticador") desempaqueta el mensaje IP y lo encapsula dentro de un paquete con formato EAPOL (EAP sobre LAN) y luego lo envía al cliente. De acuerdo al método de autenticación (PAP, CHAP, EAP) utilizado puede variar el mensaje enviado como la cantidad de mensajes enviados al cliente.

4. A continuación el cliente responde a esta petición de identidad enviando sus credenciales al "servidor de autenticación" mediante el "autenticador".

5. Si son correctas las credenciales, se le otorga un acceso al cliente a la WLAN, acorde a las políticas de seguridad establecidas en el servidor de autenticación.

La implantación es abierta, por lo que las organizaciones pueden utilizar el método de autenticación más conveniente, y tampoco existen restricciones en particular para el servidor de autenticación.
Protocolo de Autenticación Extensible (EAP): Originalmente diseñado para el protocolo PPP, es uno de los mecanismos utilizados por las redes 802.11 para intentar proporcionar un cierto nivel de seguridad en el cifrado de los datos que se transmiten entre el cliente y el punto de acceso. Este mecanismo genérico de transmisión de datos de autenticación puede ser materializado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5, que basa la autenticación del cliente en el uso de login y password, o EAP-TLS, que se basa en el uso del protocolo TLS y permite autenticación mutua entre los dos extremos. [13]

RADIUS (Remote Access Dial-In User Server): Es un protocolo de autenticación, autorización y accounting (AAA) para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un Proveedor de Servicios de Internet (ISP, Internet Service Provider) mediante módem, DSL, MODEM de cable, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS mediante el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autoriza el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.
**Imperfecciones de 802.1X**

Debido a que la especificación trata solamente sobre la autenticación, el método de cifrado de las comunicaciones debe ser robusto. Muchas WLAN utilizan WEP como método de cifrado de las comunicaciones, pero las claves secretas son estáticas. Al contrario de 802.1X que actualiza automáticamente las claves de autenticación, las claves secretas WEP deben ser modificadas manualmente en cada uno de los dispositivos para así garantizar que el sistema de cifrado funcione bien y sea robusto. Así mismo, los servidores de autenticación pueden ser usados para dar el acceso a la WLAN a través de VPN, mecanismo que le provee a la comunicación un alto nivel de seguridad. Algunas organizaciones también desearían utilizar Advanced Encryption Standard (AES) para lograr cifrado de datos de 128,154 y hasta 256 bits. Sin embargo, se necesitan equipos de red adicionales para facilitar esta actividad y evitar que el rendimiento de la WLAN se vea comprometido, dada la reducción de ancho de banda a consecuencia del cifrado de los datos. Otra imperfección considerable del 802.1X es que a manudo sólo se configura para proveer autenticación del lado del cliente, con lo que, ataques como el del “hombre en el medio” son altamente probables que ocurran.

**Limitaciones del 802.1X**

Es importante saber que tanto el cliente (“solicitante”) como el punto de acceso (“autenticador”) deben estar configurados con el mismo método de autenticación para que se pueda efectuar la comunicación y el cliente logre el acceso a la WLAN.

El hecho de que 802.1X no es un estándar obligatorio, limita su espectro de acción, por lo que quizás operará solo en algunas WLAN privadas, y no en WLAN tipo hotspots y públicas.
Protocolo de Integridad de Clave Temporal (TKIP)

A pesar de que con el IEEE 802.1X se le da solución a los problemas de autenticación presentes en WEP, aún siguen sin solventar los inconvenientes de seguridad relacionados con las claves de cifrado débiles y la alta probabilidad de que se pueda averiguar la clave WEP. En tal sentido, el protocolo de integridad de clave temporal TKIP logra darle solución efectiva a estas vulnerabilidades de WEP. TKIP utiliza claves de cifrado de 256 bits las cuales son generadas mediante un proceso muy elaborado, más robusto y fuerte que los métodos antecesores. TKIP combina tres elementos para cifrar los datos que envía el emisor:

256 bits

48 bits

128 bits

TKIP=MAC Address del cliente + Vector de Inicialización (IV) + Clave temporal
(Única para todos los clientes)

Con la inclusión de esta clave temporal única para todos los clientes, se garantiza que la clave de cifrado sea realmente única, valga la redundancia. Cada 10.000 paquetes transmitidos se cambia la clave temporal a fin de evitar que los atacantes logren decodificar los paquetes y descifrar la clave de cifrado, fortaleciendo la seguridad de la red.

802.1X + TKIP/SSN CHEQUEO

Figura 10. Proceso de cifrado TKIP/WPA
Chequeo de Integridad de Mensaje Michael (MMIC)

Este chequeo se realiza con el fin de garantizar la integridad del mensaje transmitido. Para ello, el transmisor de un paquete agrega aproximadamente 30 bits (el MIC) al paquete antes de cifrarlo y transmitirlo. El receptor lo descifra y verifica el MIC (con base en un valor derivado de la función MIC) antes de aceptar el paquete. Si el MIC no concuerda, se descarta el paquete. Con el MIC se garantiza que se desecharán los paquetes modificados y que los atacantes no podrán falsificar mensajes para persuadir a los dispositivos de red de que los autentiquen.
Enmienda de Seguridad 802.11i ó Wi-Fi Protected Access 2 (WPA2)

En enero de 2001 fue creado el grupo de trabajo en la IEEE para mejorar la seguridad en la autenticación y la encriptación de datos en WLAN. Dos años más tarde, en abril de 2003, la Wi-Fi Alliance (una asociación que promueve y certifica Wi-Fi) elaboró una recomendación para responder a las preocupaciones empresariales ante la seguridad inalámbrica. Sin embargo, estaban conscientes de que los usuarios no querrían cambiar sus equipos, por lo cual continuaron investigando y trabajando para resolver las vulnerabilidades de seguridad persistentes, hasta junio de 2004, cuando fue adoptada la edición final del estándar 802.11i que recibe el nombre comercial WPA2 por parte de la alianza Wi-Fi.

La especificación 802.11i está compuesta los siguientes elementos:

![Diagrama de Arquitectura de capas 802.11i](image)

Figura 11. Arquitectura de capas 802.11i
Cambios introducidos por el estándar IEEE 802.11i

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

La nueva arquitectura para las redes inalámbricas se denomina Robust Security Network (RSN) y utiliza autenticación 802.1X, distribución de claves robustas y nuevos mecanismos de integridad y privacidad. Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica. Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red de transición de seguridad – Transitional Security Network (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro. Si el proceso de autenticación o asociación entre estaciones utiliza el llamado 4-way handshake, la asociación recibe el nombre de RSNA (Robust Security Network Association).

El establecimiento de un contexto seguro de comunicación consta de cuatro fases (ver Figura 13):

- Fase 1: Acuerdo sobre la política de seguridad.
- Fase 2: Autenticación 802.1X.
- Fase 3: Derivación y distribución de las claves.
- Fase 4: Confidencialidad e integridad de los datos RSNA.

Fase 1: Acuerdo sobre la política de seguridad

En esta etapa tanto el dispositivo cliente (“solicitante”) como el punto de acceso (“autenticador”) deben ponerse de acuerdo en relación a la política de seguridad a
utilizar. Este proceso se realiza a través del intercambio de un grupo de mensajes que se listan a continuación:

1. (Solicitante): Solicitud de políticas de seguridad del punto de acceso.
2. (Autenticador): Respuesta contentiva de políticas de seguridad al solicitante.
3. (Solicitante): Solicitud de autenticación abierta estándar.
5. (Solicitante): Envía al autenticador una solicitud de asociación con los datos que se listan; políticas de seguridad, método(s) de autenticación soportados (802.1X, PSK), protocolos de seguridad para tráfico punto a punto (unicast) y punto-multipunto (multicast) (CCMP, TKIP, etc), datos acerca del soporte para la pre-autenticación de tal manera de evitar retrasos en el funcionamiento en la red, en caso de cambio de punto de acceso.

**Fase 2: Autenticación 802.1X**

Esta etapa del proceso corresponde a la autenticación 802.1X basada en el Protocolo de Autenticación Extensible (EAP) y adicionalmente en el método de autenticación seleccionado:

- EAP/TLS, uso de certificados tanto en el cliente como en el servidor (requiere claves públicas funcionando en ambos lados)
- EAP/TTLS ó PEAP, para autenticación híbrida. Uso de certificados sólo del lado del servidor.
Esta fase se realiza mediante el intercambio de un conjunto de mensajes en secuencia, tal y como se menciona a continuación:

   (Solicitante): responde al “autenticador” indicando el método de autenticación preferido.
2. (Autenticador): usando el protocolo RADIUS, realiza una petición de autenticación al servidor de autenticación, indicando método de autenticación del cliente (“solicitante”).
3. (Servidor de autenticación): Intercambia mensajes EAP con el cliente (“solicitante”) para generar una clave maestra común (MK, Master Key).
4. (Solicitante): Intercambia mensajes EAP con el servidor de autenticación para generar una clave maestra común (MK).
5. (Servidor de autenticación): Envía un mensaje de Aceptación RADIUS al punto de acceso (“autenticador”) y distribuye la clave maestra común MK.
6.(Autenticador): Envía un mensaje EAP exitoso al cliente (“solicitante”).

**Fase 3. Jerarquía y distribución de claves**

Un aspecto fundamental del estándar IEEE 802.11i es que sustenta la seguridad de la conexión en las claves secretas. En arquitecturas de contexto seguro de comunicación, la vida de las claves secretas es finita y limitada; así mismo la seguridad del sistema se realiza mediante un grupo de claves organizadas de acuerdo a una jerarquía de claves establecida. Luego que el autenticador envía el mensaje de autenticación exitosa al cliente, dependiendo de si se está utilizando un servidor de autenticación (clave maestra común, MK) ó si se está en redes domesticas o pequeñas empresas que no cuentan con servidor de autenticación (clave pre-compartida (PSK)), se deriva la clave maestra por parejas (PMK) y se crean dos grupos de claves temporales de sesión actualizables, la clave transitoria por parejas (PairWise Transient key (PTK)), y la clave transitoria de grupo (Group Transient Key, (GTK)) a partir de la primera clave...
(MK) o la segunda (PSK), según sea el caso. La PMK se usa para generar la PTK, cuya longitud depende del protocolo de cifrado utilizado (TKIP) 512 bits, (CCMP\(^6\)) 384 bits.

La PTK está compuesta como se muestra en la figura 14.

![PTK](diagrama PTk.png)

**Figura 12. Composición clave transitoria por parejas PTK**

- **KCK (Key Confirmation Key):** clave para la autenticación de mensajes (MIC) durante el la negociación de 4 pasos (4-Way Handshake) y la negociación de clave grupal (Group Key Handshake).

- **KEK (Key Encryption Key):** clave que garantiza la confidencialidad de los datos durante la negociación de 4 pasos (4-Way Handshake\(^7\)) y la negociación de clave grupal (Group Key Handshake).

- **TEK (Temporary Encryption Key):** clave temporal para cifrado de datos utilizada por los métodos de cifrado TKIP y CCMP.

- **TMK (Temporary MIC Key):** clave temporal para la autenticación cuando se aplica Michael en TKIP.

---

\(^6\) CCMP: Modo contador/ Protocolo de código de cifrado de bloques de mensajes de autenticación (Counter-Mode /Cipher Block Message Authentication Code Protocol)

\(^7\) 4-Way Handshake: Negociación en cuatro pasos.
Luego de haber aclarado los conceptos relativos a las claves que intervienen en el proceso de jerarquías de claves y obtenida las clave maestra por parejas (PMK) de la cual se derivan la clave transitoria por parejas (PTK) y la clave transitoria de grupo (GTK), se listan a continuación los pasos que siguen en el proceso de contexto de seguro de comunicación pendientes en esta fase:

1. El punto de acceso, luego de haber derivado la clave maestra (MK) enviada por el servidor de autenticación, deriva y distribuye la clave transitoria por parejas (PTK) y la clave transitoria por grupo (GTK) hacia los clientes (“solicitantes”).

2. El punto de acceso (“autenticador”) da inicio a la negociación en cuatro pasos con el(los) cliente(s) (“solicitante(s”)”. En este paso, se valida que el cliente conozca la clave maestra por parejas (PMK), se deriva una nueva clave transitoria por parejas (PTK), se instalan en el cliente (“solicitante”) y en el punto de acceso (“autenticador”) las claves de cifrado e integridad, se cifra el transporte de la clave transitoria de grupo (GTK), se convalida el esquema de cifrado y se intercambian 4 mensajes de clave EAPOL entre el cliente (“solicitante”) y el punto de acceso (“autenticador”) en lo que se denomina negociación en cuatro pasos.

3. Cuando el último mensaje de clave EAPOL es enviado, significa que ha finalizado el proceso de negociación con lo que el cliente (“solicitante”) procede a instalar a clave y se da inicio al proceso de cifrado.

4. Cuando el punto de acceso (“autenticador”) recibe este mensaje, instala las claves propias.

5. En este punto el contexto seguro de comunicación ha obtenido, calculado e instalado las claves de cifrado e integridad para que se comuniquen de forma segura el dispositivo móvil y el punto de acceso.
Tratamiento especial para el tráfico punto-multipunto

Este tipo de tráfico utiliza la clave transitoria de grupo (GTK) para protegerse, la cual, ha sido derivada de una clave maestra de grupo (GMK), una cadena fija, la “dirección MAC” del punto de acceso (“autenticador”) y un número aleatorio llamado GNonce. El tamaño de la clave transitoria de grupo (GTK) va a depender del protocolo de cifrado, TKIP 256 bits y CCMP 128 bits.

La GTK está compuesta de un grupo de claves temporales dedicadas que son:

![Diagrama de la Clave Transitoria de Grupo (GTK)](image)

Figura 13. Composición de la Clave Transitoria de Grupo (GTK)

Luego de obtenida la clave transitoria de grupo (GTK), el punto de acceso (“autenticador”) inicia un proceso de negociación de la clave de grupo con el cliente (“solicitante”), durante el cual se usan las claves temporales (KCK y KEK) generadas en la negociación de cuatro pasos antes mencionada.

Negociación de clave de grupo

Esta negociación se necesita para desasociar un cliente o para renovar la clave transitoria de grupo (GTK).

1. El punto de acceso (“autenticador”) calcula una nueva clave transitoria de grupo (GTK) usando un número aleatorio denominado GNonce.
2. Se envía cifrada la clave transitoria de grupo con la clave de cifrado (KEK) para garantizar la confidencialidad de los datos, el número de secuencia de la clave transitoria de grupo (GTK) y usando la clave de autenticación para mensajes MIC\textsuperscript{8} se calcula el MIC y se envía al cliente (“solicitante”).

3. El cliente (“solicitante”) al recibir el mensaje, verifica el código de integridad del mensaje (MIC) y descifra la clave transitoria de grupo (GTK).

4. Seguidamente para verificar la culminación de la negociación de clave de grupo, el cliente (“solicitante”) envía un mensaje al punto de acceso (“autenticador”) con el próximo número de secuencia de clave transitoria de grupo (GTK) y el código de integridad del mensaje (MIC) calculado. El autenticador verifica la MIC recibida e instala la nueva clave transitoria de grupo (GTK).

**Fase 4: Confidencialidad e integridad de datos**

Para llevar a cabo estas actividades fundamentales se utilizan los siguientes protocolos de cifrado e integridad:

- TKIP con RC4
- CCMP con AES\textsuperscript{9}
- WRAP con AES

**TKIP con RC4**: este esquema se divide en dos fases: la primera se encarga de los datos estáticos mediante la clave de cifrado temporal (TEK), la MAC Address del trasmisor (para evitar colisiones a causa del vector de inicialización IV) y los 32 bits más significativos del vector de inicialización. En la segunda fase, se toma el resultado de la primera fase más los 16 bits menos significativos del vector de inicialización, modificando todos los bits del campo clave por paquete para cada

---

\textsuperscript{8} MIC: Código de Integridad de mensajes. (Messages Integrity Code)

\textsuperscript{9} AES Estándar de cifrado avanzado (Advanced Encryption Standard)
nuevo vector de inicialización. El resultado de la segunda fase y una parte del vector de inicialización representan la entrada para el algoritmo RC4, el cual crea un flujo de clave que luego se opera con la expresión matemática XOR más el MPDU (MAC Protocol Data Unit), el MIC calculado a partir de la MPDU y el ICV o CRC de WEP. Seguidamente, Michael produce un valor de comprobación de 8 octetos denominado MIC y lo incluye a la MSDU (MAC Service Data Unit) previo a la transmisión.

**CCMP con AES:** utiliza el algoritmo AES CBC-MAC, que está diseñado para proporcionar una sólida integridad de los datos. El algoritmo CBC-MAC calcula un valor de 128 bits y utiliza los 64 bits de orden superior como un código de integridad de mensaje (MIC) y el modo contador de AES para cifrar la carga 802.11 y el MIC.

Para calcular un valor de MIC, AES CBC-MAC usa el siguiente proceso:

1. Se cifra un bloque inicial de 128 bits con AES y la clave de integridad de datos. Esto produce un resultado de 128 bits (Resultado1).

2. Se realiza una operación exclusiva OR (XOR) entre Resultado1 y los próximos 128 bits de los datos sobre los cuales se calcula el MIC. Esto produce un resultado de 128 bits (XResultado1).

3. Se cifra el valor de XResultado1 con AES y la clave de integridad de datos. Esto genera el valor Resultado2.

4. Se realiza una operación XOR entre el valor de Resultado2 y los siguientes 128 bits de los datos. Esto genera XResultado2

5. Se repiten los pasos 3 y 4 para los bloques adicionales de 128 bits de los datos. Los 64 bits de orden superior del resultado final constituyen el MIC de CCMP.
WRAP (Wireless Robust Authenticated Protocol) con AES: Este protocolo utiliza el esquema de cifrado autenticado de cifrado y autenticación en la misma operación (OCB (Offset Codebook Mode)). Este esquema de cifrado fue el elegido por el grupo de trabajo de la IEEE 802.11i, pero fue descartado a posteriori por problemas con la propiedad intelectual y el licenciamiento.

Cuadro resumen

En la tabla 1 se resumen las características más relevantes de las tecnologías de cifrado de datos existentes en WLAN.

<table>
<thead>
<tr>
<th>Resumen Tecnologías de Cifrado de Datos WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>**</td>
</tr>
<tr>
<td>Algoritmo de cifrado</td>
</tr>
<tr>
<td>Tamaño de la clave</td>
</tr>
<tr>
<td>Vida de la clave</td>
</tr>
</tbody>
</table>
Tabla 1. Resumen de tecnologías de cifrado de datos WLAN

<table>
<thead>
<tr>
<th>Clave de paquete</th>
<th>Concatenada</th>
<th>No es requerida</th>
<th>No es requerida</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integridad: Encabezado; Datos</td>
<td>Ninguno, CRC-32</td>
<td>Michael, Michael</td>
<td>CCMP, CCMP</td>
</tr>
<tr>
<td>Respuesta</td>
<td>Ninguna</td>
<td>Utiliza Vector de Inicialización</td>
<td>Utiliza Vector de Inicialización</td>
</tr>
<tr>
<td>Administración de clave</td>
<td>Ninguna</td>
<td>Basado en EAP</td>
<td>Basado en EAP</td>
</tr>
</tbody>
</table>

2.1.10.2. Seguridad a nivel físico de la WLAN.

Una de las consideraciones más importantes que debe tener en cuenta una organización al momento de implantar una WLAN son las políticas, normas y procedimientos relativos al cuidado, prevención y control de los componentes físicos que la componen en caso de accidentes, inclemencias meteorológicas y actos vandálicos.

Estas acciones deben estar en consonancia con tres factores que son:

1. Riesgo al que pueden estar expuestos los componentes.
2. Probabilidad de ocurrencia del riesgo.
3. Impacto de la ocurrencia del riesgo en la operación.

Puntos de acceso y antenas

Si su ubicación es interna, los AP deben ser colocados en lugares seguros, preferiblemente a una altura donde puedan ser fácilmente administrables por el personal técnico, lejos de posibles fuentes de interferencia (hornos microondas y otros transmisores). En caso de estar ubicados en lugares externos, se recomienda protegerlos de los vientos fuertes, nieve, hielo, lluvia. Preferiblemente deben estar en sitios que eviten su exposición directa a los cambios climatológicos. Disponer de pararrayos en caso de tormentas. En relación al
cableado que permite la interacción con la red cableada, se recomienda que sea ubicado en cubiertas protectores alejados preferentemente de tuberías y depósitos de agua, los cuales deben ser revisados periódicamente en caso de estar cercanos al cableado para prevenir derrames por fugas accidentales.

En cuanto a la seguridad física de estos componentes, se recomienda colocarlos en áreas que cuenten con mecanismos tales como, cerraduras y puertas, sistemas de control de acceso, preferiblemente no accesibles al público. Si se cuenta con sistemas de vigilancia, se recomienda dedicar recursos a aquellos componentes de mayor incidencia y criticidad para la operación del negocio.

En cuanto a la identificación y documentación, es fundamental etiquetar cada componente de la WLAN y mantener un control de inventario de la ubicación física de cada uno de ellos, permanentemente actualizado y siguiendo lo establecido en los procedimientos para control de inventario con los que cuente la organización. Se recomienda también establecer una lista de personal autorizado para el mantenimiento de estos componentes y el seguimiento permanente mediante el registro de las acciones que impliquen cambios físicos de los componentes que incidan sobre el sistema de seguridad física implantado en la organización.

**Dispositivos móviles**

Los equipos móviles son bastante atractivos para ser hurtados o extraviados en la organización, dadas sus características físicas. En tal sentido, es recomendable utilizar mecanismos de cierre para garantizar la permanencia en el tiempo de estos dispositivos dentro de la organización, casa o sitio remoto. Generalmente se usan en estos casos candados que bloquean físicamente el retiro del equipo del lugar físico donde se encuentran. Otro mecanismo a
considerar es la correlación entre el usuario y el equipo móvil en una base de
datos, preferiblemente un directorio, que pueda ser consultado por todos los
miembros de la organización y que permita al personal de seguridad autorizar la
entrada o salida de equipos sólo por aquellos usuarios autorizados o con equipos
assignados de acuerdo a la información contenida en esos directorios. Así mismo,
hoy en día se encuentran disponibles dispositivos de control de acceso
inalámbrico mediante sistema de comunicación infrarrojo, que funcionan
combinando un dispositivo que es colocado en el equipo móvil, el cual emite una
señal de código infrarrojo con los datos del equipo y del usuario propietario, un
sistema de control de acceso inalámbrico de señales infrarrojo ubicado en las
áreas de acceso de cada oficina o grupo de oficinas, un sistema de alarmas y
alertas que se activa cuando un equipo móvil es trasladado fuera de su ubicación
física por un usuario diferente al propietario y el personal de seguridad que
monitorea continuamente las alertas y alarmas movilizándose físicamente al lugar
donde se disparó la alerta en cuestión, para así detener al sujeto y validar el
motivo del traslado no autorizado del equipo móvil.

Tanto para puntos de acceso y antenas como para dispositivos móviles, la
organización debe contar con una política de seguridad física conocida, divulgada
y aprobada por todos los miembros de la institución. Allí deben concentrarse todos
los procesos, normativas y recomendaciones que permitan garantizar el éxito de la
seguridad física de los componentes de la WLAN. En este mismo orden de ideas,
es fundamental educar al usuario y hacerlo parte del sistema de seguridad física,
dándole a entender la relevancia e implicaciones del cumplimiento de lo
establecido por el sistema de seguridad y su corresponsabilidad como miembro
ejecutor de los lineamientos establecidos.
2.2 Marco metodológico

2.2.1. Consideraciones Generales

Hasta el momento, en el presente documento se han venido describiendo las tecnologías, protocolos, estándares y esquemas de las redes inalámbricas de área local, haciendo particular énfasis en las considerables vulnerabilidades de seguridad que existen en sus distintos componentes. Precisamente sobre este respecto se ha considerado que la metodología de implantación de la seguridad representa el aspecto de mayor significación para garantizar el control sobre los activos de información de las organizaciones. En tal sentido, la investigación pretende dilucidar, sugerir y proponer a través del estudio de las mejores prácticas metodológicas internacionales, un esquema de trabajo genérico e independiente del tipo de organización, basado en el análisis comparativo de cada una de estas metodologías, que pueda ser de utilidad para las comunidades de interés relacionadas con el tema.

Esta investigación es del tipo no experimental y por tanto, los contenidos aquí propuestos se dejan expuestos para futuras investigaciones donde se pueda demostrar la efectividad de la metodología de implantación sugerida como resultado del estudio.

2.2.2. Tipo de Investigación

El estudio de las metodologías de implantación de la seguridad en WLAN, se aborda con el propósito de llevar a cabo una investigación del tipo bibliográfica amplia. En tal sentido, a continuación se refieren algunas citas bibliográficas que describen las características relevantes de una investigación de este tipo:

− “Cuando los datos ya han sido recolectados en otras investigaciones y son conocidos mediante los informes correspondientes, nos referimos a datos secundarios, porque han sido obtenidos por otros y nos llegan elaborados y procesados de acuerdo con los fines de quienes inicialmente los obtuvieron y
manipularon. Como estas informaciones proceden siempre de documentos escritos (ésa es la forma en que se emiten los informes científicos), damos a estos diseños el nombre de bibliográficos.” (Carlos A. Abino, El Proceso de Investigación).

− “La investigación bibliográfica o búsqueda de información bibliográfica, es aquella etapa de la investigación científica donde se explora qué se ha escrito en la comunidad científica sobre un determinado tema o problema”. (Gloria Rojas, Universidad Católica de Maule, Chile).

Dado el nivel de la investigación, se considera que es de tipo no experimental y que está diseñada para ofrecer una propuesta metodológica sustentada en el estudio de las mejores prácticas internacionales en el área de investigación.

2.2.3. Área de Investigación

El estudio se llevó a cabo recolectando la información de la bibliografía referenciada en el presente documento, disponible a nivel mundial.

2.2.4. Descripción de la Metodología

La metodología propuesta se desagrega por etapas, una propuesta conforme a una serie de pasos: elección del tema, planteamiento del problema, recopilación de datos, análisis e interpretación de datos, comunicación de resultados, formulación de recomendaciones e implantación.

Dicho marco permite identificar claramente los factores bajo estudio y analizar en forma ordenada y sistemática sus componentes del modo más racional utilizando las técnicas más adecuadas de investigación.
2.2.5. Diseño de la Investigación

En el marco de la investigación planteada, referido al estudio de las metodologías de implantación de la seguridad en redes inalámbricas de área local, el diseño de la investigación utilizado corresponde al de tipo bibliográfico, en el cual la información procede siempre de documentos elaborados y escritos por otros (ésa es la forma en que se emiten los informes científicos) [12]. Así mismo, dicho diseño se fundamenta en enfoques amplios y versátiles de las fuentes de información. Esto incluye el uso de fuentes primarias y secundarias de información, observación, entrevistas con expertos y entrevistas de grupo con especialistas. El objetivo es resumir las mejores prácticas obtenidas del proceso de investigación en base a las metodologías estudiadas a fin de extraer las mejores alternativas identificadas.

El estudio propuesto se adecua a los propósitos de la investigación no experimental descriptiva, donde no se ha planteado hipótesis, pero sí se ha definido un conjunto de variables. Se trata de un estudio descriptivo, en la medida que el fin último es el de describir con precisión, las características de las metodologías de implantación de la seguridad de redes inalámbricas locales.

2.2.6. Instrumentos de recolección de información

En base a los objetivos establecidos en la presente investigación, donde se plantea el estudio de las metodologías de implantación de la seguridad en redes inalámbricas de área local, ubicado dentro de la modalidad de los denominados proyectos factibles. Se emplean un conjunto de instrumentos y técnicas de recolección de la información, orientados de manera esencial a alcanzar los fines propuestos. Para seguir este lineamiento, hay que cumplir con tres fases básicas: la primera tiene que ver con la delimitación de todos los aspectos teóricos de la investigación, vinculada a la formulación y delimitación del problema, objeto de estudio, elaboración del marco teórico, etc. La segunda es relativa a la realización
de un estudio de las vulnerabilidades de seguridad presentes en las redes inalámbricas de área local y sus implicaciones en las organizaciones. Y por último, la tercera fase está ligada al análisis de las metodologías de implantación de seguridad en este tipo de redes y la propuesta metodológica como resultado del estudio realizado.

Dada la naturaleza del estudio y en función de los datos que se requieren, tanto del momento teórico, como del momento metodológico de la investigación, así como con la presentación del trabajo escrito, en primer lugar, se sitúan las denominadas técnicas y protocolos instrumentales de la investigación documental. Dentro de ese ámbito, también se usarán una serie de técnicas operacionales para manejar las fuentes documentales, desde una dimensión estrictamente técnica y común a todas las ciencias, a saber: de subrayado, fichaje, bibliográficas, de citas y notas de referencias bibliográficas y de ampliación de texto, construcción y presentación de índices, presentación de cuadros, gráficos e ilustraciones, presentación del trabajo escrito, etc. Debido a que la investigación es del tipo no experimental, no ha sido factible aplicar el uso de técnicas de observación directa, no participante y sistemática en la realidad objeto de estudio.

2.2.7. Técnicas documentales

Anteriormente se ha señalado que la dimensión de la investigación es documental; se emplean diversas técnicas e instrumentos de recolección de la información que contienen principios sistemáticos y normas de carácter práctico, muy rigurosas e indispensables para ser aplicados a los materiales bibliográficos que se consultan a través de todo el proceso de investigación, así como en la organización del trabajo escrito que se producirá al final del mismo.

Para el análisis de las fuentes documentales se utilizan las técnicas de: observación documental, presentación resumida, resumen analítico y análisis crítico. A partir de la observación documental como punto de partida en el análisis
de las fuentes bibliográficas mediante una lectura general de los textos y de las sitios consultados, se inicia la búsqueda y observación de los hechos presentados en los materiales escritos consultados que son de interés para la investigación. La técnica de presentación resumida asume un papel importante en la construcción de los contenidos teóricos de la investigación. De igual manera, la técnica de resumen analítico, se incorpora para descubrir la estructura de las páginas y textos consultados.
Capítulo 3. Metodologías de implantación de la seguridad en WLAN

El capítulo 2 del presente documento hace referencia a los elementos que conforman una configuración de red inalámbrica de área local tradicional, con especial énfasis en las vulnerabilidades que históricamente han venido arrastrando consigo estas tecnologías. Sin embargo, es claro y notorio el avance que desde el punto de vista tecnológico se ha logrado, en lo que respecta a los mecanismos de seguridad de las tecnologías inalámbricas, las cuales abarcan tanto los aspectos relativos a la seguridad del lado del cliente como del lado del servidor; inclusive se han incorporado componentes adicionales a la arquitectura de red para incrementar los niveles de seguridad de los datos y los equipos en este tipo de redes. Por tanto, justo en este punto es válido evaluar, sí se están considerando todos los aspectos relativos a la seguridad de un entorno de red inalámbrico, pero antes en la figura 15, se muestra un gráfico con los elementos que según la literatura componen el mapa de seguridad de un entorno de red:

![Figura 15. Mapa de presencia de seguridad](image)

En esta figura se puede visualizar claramente que la seguridad de un entorno
de red inalámbrico se compone de:

- Seguridad de la información
- Procesos de seguridad
- Tecnologías de seguridad para Internet
- Seguridad de las comunicaciones
- Seguridad del entorno inalámbrico
- Seguridad física

En tal sentido, el tema de la seguridad de las tecnologías de información y comunicación comprende un conjunto de elementos que interactúan entre sí, que se solapan, se comunican y se complementan constituyendo un sistema de relaciones que debe regirse por un conjunto de normas y procesos que esquemáticamente permitan garantizar el adecuado funcionamiento de sus partes.

Aunado a esto, el avance progresivo de la tecnología (sistemas operativos, bases de datos, aplicaciones, comunicaciones, correo electrónico, Internet, etc.) y el nacimiento de las diferentes necesidades de cada organización, ha requerido que un importante número de profesionales se dediquen a analizar y diseñar normas para la administración y gestión de las diferentes plataformas informáticas, lo cual en definitiva, ha ido llevando a la conformación de un estándar de seguridad internacional, del que se han derivado ciertas metodologías para la implantación de la seguridad específicamente en entornos de redes inalámbricas.

Visto todo esto, a continuación se mencionan los elementos más importantes que conforman el estándar internacional de seguridad ISO/IEC\textsuperscript{10} 17999, como marco referencial de las metodologías de implantación de seguridad para redes inalámbricas ISO/IEC 17999, y Cobit 4.0, que son objeto de estudio de la investigación.

\textsuperscript{10} IEC Comisión Electrónica Internacional, International Electrotechnical Comission
3.1. Estándar ISO/IEC 17799

En el año 1995 el Instituto Británico de Estándares (BSI, British Standard Institute), publicó la norma (BS7799), contentiva de un conjunto de buenas prácticas para la administración de seguridad de los sistemas de información. Luego de una revisión por parte este organismo, en mayo de 1999, se publicó la segunda versión, la cual fue adoptada principalmente por algunos países de Europa, África y Oceanía. Seguidamente en el año 2000, fue adoptada por la Organización Internacional de Estándares (ISO, por sus siglas en ingles), como la norma ISO 17799 [14]. En el año 2002 la norma se adoptó como Una Norma Española (UNE) y finalmente en el 2004 se estableció la norma UNE 71502 basada en el estándar ISO 17999.

La norma UNE – ISO/IEC 17799 es una compilación de recomendaciones sobre prácticas exitosas de seguridad, aplicable en toda organización independientemente de su tamaño, sector, y sistemas informáticos utilizados. Dicha norma fue redactada para que fuese flexible intencionalmente y nunca indujo a la aplicación de una solución de seguridad específica para lograr su cumplimiento. Uno de los principales objetivos de la norma UNE- ISO/IEC 17799,
es proteger la confidencialidad, integridad y disponibilidad de la información escrita, almacenada, y transferida. La misma consta de diez dominios de control que cubren todos los aspectos relativos a la gestión de la seguridad de la información; consta de más de 36 objetivos de control y alrededor de 134 controles.

![Figura 17. Dominios de control Norma UNE-ISO/IEC 17799](image)

Desde su publicación por parte de la Organización Internacional de Estándares (ISO, por sus siglas en inglés), se ha consolidado como la norma técnica de seguridad de la información reconocida a nivel mundial, como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información". [6]

**De las recomendaciones**

En la norma se hacen recomendaciones independientes a la tecnología, es intencional la flexibilidad e imprecisión de la misma, por lo que se hace difícil contar con una norma que funcione en una variedad de entornos de tecnología de
la información y que sea capaz de desarrollarse con el cambiante mundo tecnológico. Simplemente la norma ofrece un conjunto de reglas basado en un enfoque de mejores prácticas más que en un método efectivo para diseñar, comunicar y mantener las políticas y procedimientos de seguridad, frente a las necesidades actuales de usuarios, administradores, especialistas de seguridad, entre otros.

Sistema de Gestión de la Seguridad de la Información (UNE 71502)

La norma UNE/ISO-IEC 17799 propone el Sistema de Gestión de la Seguridad de la Información (SGSI) tipificada en la norma (UNE 71502), en la cual, se especifican las consideraciones para establecer, implantar, documentar y evaluar de dicho sistema de gestión.

El SGSI es el sistema que comprende las políticas, procedimientos, procesos, estructura organizativa y recursos requeridos para implantar la gestión de la seguridad de la información. Así mismo, abarca lo relativo a los aspectos organizativos, físicos, lógicos y legales entre otros. Es aplicable en cualquier tipo de organización al ser independiente de marcas, plataformas tecnológicas y mecanismos específicos y se caracteriza por su profundo contenido documental.

![Figura 18. Estructura del SGSI](image-url)
El SGSI utiliza el modelo PHVA (Planificar, Hacer, Verificar y Actuar) para llevar a cabo la gestión de la seguridad de la información.

**Planificar:** Esta es la fase inicial del modelo de gestión donde se define la política de la seguridad, se realiza un análisis de riesgos y se seleccionan los respectivos controles. En la práctica, se realizan tres preguntas que permiten establecer el plan de acción en función del logro de los objetivos que se desea alcanzar. La primera pregunta es ¿Cuál es el estado actual de la seguridad de la organización? La segunda es ¿A qué estado de seguridad desea llegar la organización? La tercera pregunta es ¿Cómo se desea alcanzar el estado de seguridad objetivo?. Un aspecto crucial es la participación de los más altos niveles directivos de la organización en esta etapa de definición del sistema.

**Hacer:** En esta etapa se realizan la implantación del SGSI y la operación del mismo. Durante la fase de implantación del SGSI se ponen en funcionamiento los controles técnicos y no técnicos (procesos, procedimientos, normas y políticas); se establecen pautas para la verificación de los controles implantados a fin de determinar la efectividad de los mismos. Adicionalmente, al finalizar la fase de implantación de controles, comienza la operación de los mismos y se comienzan a dar respuesta a los incidentes de seguridad que puedan suscitarse.

**Verificar:** Se audita el SGSI mediante indicadores de rendimiento que permitan verificar el comportamiento en función de los objetivos previamente establecidos. Se verifican tanto la eficacia del SGSI como la eficiencia y si se adecua a lo estipulado en la planificación, si esta funcionando bien y se ha mantenido correctamente. También se descarta la aparición de nuevos riesgos y los cambios que puedan afectar al sistema de gestión.

**Actuar:** Este estadio del sistema indica la revisión continua de la eficacia del SGSI por parte de la organización mediante auditorías periódicas y permanentes.
revisiones de la seguridad, de tal forma de evaluar los indicadores de los procesos, verificar los objetivos de seguridad establecidos con el propósito de aplicar medidas correctivas sobre las debilidades detectadas en el SGSI y determinar las acciones preventivas para evitar potenciales causas de no conformidades en el SGSI.

Figura 19. Modelo de Gestión de la seguridad del SIGS en la UNE/ISO-IEC 17799

Referencia obligada

Por todo lo antes mencionado, la adopción de un programa de seguridad para la protección de la información en cualquier organización basado en las áreas de dominio que alcanza cubrir la norma, puede ser de muchísimo provecho como insumo para definir y guiar la preparación de una política de seguridad de alto nivel. En todo caso, el objetivo final de las organizaciones en general es simplemente cumplir de la mejor manera sus respectivos procesos de negocio, para lo cual las mejores prácticas representan la vía más utilizada por las instituciones de mayor éxito mundial.

Haciendo referencia por un instante al problema de la presente investigación, destaca el hecho de que uno de los beneficios que ofrece la aplicación de un esquema de protección de seguridad basado en la norma UNE-ISO/IEC 17799 es y se cita: “... al adoptar estándares y marcos de referencia comunes, las organizaciones pueden construir una arquitectura de seguridad que les permita minimizar las brechas que se puedan registrar entre las amenazas
detectadas y los controles existentes, mitigando el riesgo asociado a una eventual ocurrencia de dicha amenaza … “[6], lo cual, representa una respuesta general al problema de la investigación.

En consecuencia, para brindar altos niveles de seguridad a las redes inalámbricas es en definitiva una excelente recomendación, adoptar metodologías de implantación apegadas a los estándares internacionales regidos por las mejores prácticas y recomendaciones establecidas por los expertos en la materia.

En tal sentido y según los resultados de la investigación bibliográfica realizada durante el presente trabajo, existen un conjunto de metodologías que pueden ser aplicadas para la implantación de la seguridad en las redes inalámbricas, entre las cuales tenemos:

- Objetivos de Control de información y tecnologías relacionadas (Cobit, por sus siglas en inglés).
- La propia norma UNE/ISO-IEC 17799

A continuación se aplica lo establecido en ambas metodologías al problema de la investigación objeto de estudio.

3.2. Cobit (Objetivos de control de información y tecnologías relacionadas)

Esta metodología según su taxonomía, consta de una colección de documentos que pueden ser clasificados como mejores prácticas generales para el gobierno, control y seguridad de las Tecnologías de Información y Comunicación.

La primera edición de la metodología, fue publicada por ISAF11 en el año

---

11 ISAF Fuerza de Asistencia Internacional de seguridad (International Security Assistance Force)
1996. En el año 1998, se publicó la segunda edición con objetivos de control adicionales y el conjunto de herramientas de implantación. En el año 2000, el ITGI\textsuperscript{12} publicó la tercera edición incorporando una guía de administración y varios objetivos de control adicionales. Para el año 2005, la ITIG culminó una exhaustiva reconstrucción de los contenidos de la metodología y publicó la versión actual de Cobit 4.0.

Este conjunto de lineamientos y estándares internacionales establece un patrón de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro “dominios” principales, a saber:

- Planificación y organización
- Adquisición e implantación
- Soporte y servicios
- Monitoreo y evaluación

Estos dominios agrupan objetivos de control de alto nivel, que abarcan tanto los aspectos de información, como de la tecnología que los soporta. Estos dominios y los objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Asimismo, se deben tomar en cuenta los recursos que proporcionan las tecnologías de Información y comunicación, tales como: datos, sistemas de aplicación, tecnologías (plataformas), instalaciones y el recurso humano.

La interacción de los dominios con los objetivos del negocio, información y recursos de tecnologías de información y comunicación, se muestra en la figura 20.

A continuación se describen cada uno de los dominios de la metodología de

\textsuperscript{12} ITIG Instituto gubernamental de Tecnologías de Información (IT Governance Institute)
control de Objetivos de información y Tecnologías Relacionadas, CobiT.

**Dominio: Planificación y Organización**

Este dominio se refiere a cómo las tecnologías de información y comunicación pueden contribuir al cumplimiento de los objetivos del negocio, desde el punto de vista estratégico y táctico.

![Diagrama de interrelación de los cuatro dominios de COBIT]

**Figura 20.** Interrelación de los cuatro dominios de COBIT.

En este sentido, el dominio de planificación y organización debe cumplir con una serie de procesos, entre los cuales se destacan la definición de un plan estratégico de sistemas, de la arquitectura de la información y de la organización y sus relaciones. Destaca también la administración de las inversiones en tecnología de información y de los recursos humanos que le compete. Debe considerarse igualmente en este dominio, la evaluación de los riesgos, y cuáles son los controles a establecer con el fin de mitigar estos riesgos.

Como base fundamental, la definición del plan estratégico debe comprender una serie de componentes que se muestran en la figura 21.
Se pueden establecer una serie de indicadores de gestión, que permitan medir la efectividad del cumplimiento de los procesos establecidos en el dominio. Para esto, pueden definirse indicadores tanto cuantitativos como cualitativos, por ejemplo para la administración de la inversión en tecnología de información, se pueden tener indicadores como presupuesto por área, porcentaje del cumplimiento de este presupuesto al final del período, problemas solventados con las inversiones realizadas, entre otros.

La importancia de los indicadores de gestión, aparte de medir la efectividad del cumplimiento de los procesos, es identificar las posibles desviaciones para aplicar los correctivos necesarios únicamente en las áreas que merezcan ser atendidas. De esta manera, se dedican recursos de inversión, tiempo y humanos a la atención de estas situaciones puntuales.

Adicionalmente, permiten la identificación de controles no aplicados, que pueden dar origen a las desviaciones identificadas. En este sentido, ubicar estas situaciones permitirá la toma de decisiones, tales como fortalecer los controles establecidos o la implantación de controles alternos.
**Dominio: Adquisición e Implantación**

Se refiere a la adquisición, desarrollo e implantación de soluciones de tecnología de información y comunicación, que permitan llevar a cabo la estrategia definida en el dominio de planificación y organización. Ver figura 22.

Uno de los factores más importantes a considerar en este dominio, es cómo las soluciones de tecnología de información y comunicación se adaptan a los procesos del negocio, y si estas soluciones llevan consigo riesgos que obliguen a establecer nuevos controles en dichos procesos.

![Figura 22. Etapas de la adquisición e implantación](image.png)

La medición de esta adaptabilidad, de los riesgos y controles existentes, es realizada igualmente mediante indicadores de gestión. Por ejemplo, se pueden medir los eventos ocurridos en un período determinado y el impacto de estos eventos; el número de quejas y solicitudes adicionales realizadas por los usuarios...
para la modificación a las soluciones; o el porcentaje de modificaciones efectivas realizadas a los sub-módulos del sistema de información implantado.

**Dominio: Soporte y servicios**

Esta actividad hace referencia a la entrega de los servicios de tecnología de información y comunicación, abarcando las operaciones, entrenamiento, seguridad, continuidad de los sistemas y planes de contingencia: vale decir, que los procesos de soporte a estas operaciones deben estar definidos y documentados. Una vez que una solución de red inalámbrica ha sido implantada en una organización, bien sea una solución adquirida de un proveedor externo o una solución desarrollada en la propia organización, tanto los sistemas para su gestión como la plataforma que la soporta, van a requerir un adecuado soporte que permita garantizar su adecuada operación y adaptación a los nuevos requerimientos que surjan de la dinámica operativa diaria de la organización. En la figura 23 se pueden observar los elementos a considerar para un adecuado soporte.

El soporte debe considerar un conjunto de procesos, que faciliten el control de todas las actividades relacionadas; vale decir: definición de acuerdos de niveles de servicios, administración de servicios prestados por terceros, administración del

![Figura 23. Elementos a considerar para un adecuado Soporte](image)
desempeño y capacidad, aseguramiento del servicio continuo, garantía de la seguridad de sistemas, identificación y asignación de costos, educación y entrenamiento a los usuarios, apoyo y soporte a los usuarios, administración de la configuración, administración de problemas e incidentes, administración de los datos, administración de instalaciones y administración de las operaciones.

En cada uno de los procesos antes mencionados se pueden establecer indicadores de gestión que permitan mantener un adecuado control de las actividades del dominio. Estos indicadores permitirán aplicar los correctivos necesarios en caso de ocurrir alguna desviación importante. Ejemplo de estos indicadores son:

**Tabla 2. Indicadores de Gestión del dominio de Soporte y servicios según Cobit**

<table>
<thead>
<tr>
<th>Proceso IT</th>
<th>Objetivo</th>
<th>Indicadores de desempeño</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definir y gestionar niveles de servicio</td>
<td>Definir, documentar y satisfacer los requerimientos en cuanto a niveles de servicio.</td>
<td>• Tiempo de resolución de asuntos relacionados a los niveles de servicio.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fondos adicionales requeridos para alcanzar los niveles de servicio acordados.</td>
</tr>
<tr>
<td>Gestionar servicios prestados por terceros</td>
<td>Asegurar que los proveedores de servicios se adhieren a los roles y responsabilidades acordados y que satisfacen los requerimientos.</td>
<td>• Número y frecuencia de reuniones de revisión contractual.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Número de asuntos pendientes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Número de contratos que no utilizan términos y condiciones estándares o excepciones autorizadas.</td>
</tr>
<tr>
<td>Gestionar desempeño y capacidad</td>
<td>Asegurar la disponibilidad de capacidad adecuada y que se utiliza de forma optima para satisfacer las necesidades de desempeño.</td>
<td>• Número de fallas ocasionadas por capacidad insuficiente o por el desempeño del procesamiento.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tiempo empleado para resolver</td>
</tr>
<tr>
<td>Problemas de capacidad.</td>
<td>Asegurar la continuidad de los servicios</td>
<td>Asegurar que los servicios de TI estén disponibles según lo requerido y asegurar que en caso de falla, el impacto sobre el negocio sea mínimo.</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Porcentaje de incrementos de capacidad no planificados sobre el total de incrementos.</td>
<td>• Número de asuntos de continuidad de servicios pendientes.</td>
<td>• Número de brechas en la continuidad del servicio, empleando criterios de duración e impacto.</td>
</tr>
<tr>
<td>Proveer la seguridad de los activos de información</td>
<td>Proveer la seguridad de los activos de información</td>
<td>Proveer la seguridad de los activos de información</td>
</tr>
<tr>
<td>• Variación del número de llamadas y solicitudes de cambios relacionados a la seguridad.</td>
<td>• Número de sistemas sujetos a sistemas de detección de intrusos.</td>
<td>• Tiempo transcurrido entre la detección, reporte y acción sobre incidentes de seguridad.</td>
</tr>
<tr>
<td>Identificar y asignar costos</td>
<td>Identificar y asignar costos</td>
<td>Identificar y asignar costos</td>
</tr>
<tr>
<td>Asegurar la correcta asignación de costos atribuibles a servicios de TI.</td>
<td>Asegurar la correcta asignación de costos atribuibles a servicios de TI.</td>
<td>Asegurar la correcta asignación de costos atribuibles a servicios de TI.</td>
</tr>
<tr>
<td>Entrenar y concientizar a los usuarios</td>
<td>Entrenar y concientizar a los usuarios</td>
<td>Entrenar y concientizar a los usuarios</td>
</tr>
<tr>
<td>Asegurar que los usuarios están haciendo un uso efectivo de la tecnología y están al</td>
<td>Asegurar que los usuarios están haciendo un uso efectivo de la tecnología y están al</td>
<td>Asegurar que los usuarios están haciendo un uso efectivo de la tecnología y están al</td>
</tr>
<tr>
<td>Tarea</td>
<td>Metodología</td>
<td>Indicador de Medición</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>
| Asistir y asesorar al usuario | Asegurar que cualquier problema experimentado por el usuario sea resuelto de forma apropriada. | • Porcentaje de empleados entrenados en conducta ética.  
|   |   | • Número de violaciones éticas identificadas.  
|   |   | • Porcentaje de empleados entrenados en prácticas de seguridad.  
|   |   | • Número de incidentes de seguridad identificados relacionados con los empleados.  
| Gestionar configuración | Mantener monitoreados todos los componentes de TI y prevenir alteraciones no autorizadas. | • Número de solicitudes de asistencia.  
|   |   | • Tiempo para resolver las solicitudes de asistencia.  
|   |   | • Número de solicitudes de asistencia repetidas.  
| Gestionar problemas e incidentes | Asegurar que los problemas e incidentes sean resueltos, y que se investiguen las causas para evitar la recurrencia. | • Frecuencia de análisis de excepción, atendiendo asuntos de redundancia, obsolescencia y corrección de la configuración.  
|   |   | • Número de versiones o actualizaciones instaladas.  
|   |   | • Porcentaje de cambios reactivos (en lugar preventivos).  
|   |   | • Tiempo entre la primera detección de problemas y registro en el sistema de gestión.  
|   |   | • Tiempo entre el registro de problema y resolución o notificación a nivel superior.  
|   |   | • Porcentaje de problemas reportados con solución conocida.
<table>
<thead>
<tr>
<th>Gestionar del correcto uso de la información</th>
<th>Asegurar la integridad, exactitud y validez de la data durante su ingreso, actualización y almacenamiento.</th>
<th>• Porcentaje de actualizaciones reprocesadas. &lt;br&gt;• Porcentaje de errores prevenidos al momento del ingreso. &lt;br&gt;• Tiempo entre la ocurrencia de errores, detección y corrección.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gestión de seguridad física</td>
<td>Proveer de un entorno físico que proteja a los equipos de TI y al personal.</td>
<td>• Frecuencia de pruebas sobre alarmas de incendio y planes de evacuación. &lt;br&gt;• Frecuencia de inspecciones físicas. &lt;br&gt;• Tiempo entre el registro y resolución de incidentes físicos.</td>
</tr>
<tr>
<td>Gestionar las operaciones</td>
<td>Asegurar que las actividades de soporte TI se realizan regularmente y de forma ordenada.</td>
<td>• Variación del número de problemas, retrasos y desviaciones. &lt;br&gt;• Medición de la congruencia entre la demanda de usuarios y capacidad de los recursos. &lt;br&gt;• Frecuencia de respaldos. &lt;br&gt;• Edad promedio de equipos.</td>
</tr>
</tbody>
</table>

**Dominio: Monitoreo**

Los procesos de la unidad de tecnología de información y comunicación deben ser evaluados periódicamente para verificar la calidad y cumplimiento de los requerimientos de control. Dicha evaluación debe pasar por el monitoreo de los procesos implantados y de los nuevos controles, a fin de verificar su efectividad.
Entre las actividades a realizar para un efectivo monitoreo, se mencionan: evaluación de los procesos, evaluación del control interno, obtención de aseguramiento independiente (certificaciones) y realización de auditorias independientes.

La importancia de mantener certificaciones y auditorias independientes, radica en la obtención de una opinión de un tercero con un punto de vista diferente, con base en su experiencia, los procesos y resultados de lo que se está evaluando, de manera de dar un mayor nivel de confianza a la organización. Entre los indicadores a definir se pueden mencionar los siguientes:

<table>
<thead>
<tr>
<th>Tabla 3. Indicadores de gestión del dominio Monitoreo según Cobit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proceso IT</strong></td>
</tr>
<tr>
<td>Monitorear los procesos</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Evaluar la adecuación del control interno</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
| Obtenir aseguramiento independiente | Incrementar la confianza en los procesos de TI entre la organización, clientes y proveedores. | • Número de procesos de aseguramiento iniciados.  
• Número de interacciones antes de la aceptación de los reportes de aseguramiento. |
|-----------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Proporcionar auditoría independiente | Incrementar los niveles de confianza y obtener beneficios de asesoría basada en las mejores prácticas. | • Número de acciones correctivas y sostenibles tomadas como resultado de nuevos hallazgos de auditoria.  
• Incremento en el número de auditores con certificaciones técnicas y profesionales.  
• Mejora en el tiempo del ciclo del proceso de auditoria, desde la planificación al informe. |

Así mismo, durante el proceso de evaluación se pueden definir múltiples indicadores de gestión adicionales, que permitan a la organización mantener un adecuado control sobre su gestión.
3.3. Aspectos a cubrir para la implantación de la seguridad de una WLAN

Vistos los aspectos teóricos generales que conforman el estándar de seguridad internacional UNE/ISO-IEC 17799 y la metodología Cobit, es el momento de aplicar ambos esquemas al tema de la investigación.

Por consiguiente de los datos recopilados durante la investigación y los aportes de la bibliografía consultada, la implantación de la seguridad de una WLAN debe cubrir las siguientes actividades macro:

1. Evaluar la situación de la organización con respecto a la seguridad
2. Definir el proyecto de implantación de la seguridad en la red inalámbrica
3. Redactar políticas de seguridad inalámbrica
4. Establecer autoridades sobre la seguridad inalámbrica
5. Organizar las unidades de TIC
6. Establecer normas y políticas para la seguridad física
7. Definir los requerimientos de seguridad de las aplicaciones
8. Establecer un método de autenticación
9. Establecer un método de cifrado
10. Definir los requerimientos de registro y auditoria de usuarios
11. Establecer mecanismos de seguridad para oficinas remotos y sucursales
12. Diseñar la topología de red
13. Establecer un presupuesto
14. Establecer requerimientos de hardware y software
15. Adquirir solución de hardware y software
16. Instalar y probar solución de hardware y software
17. Establecer normas y políticas para la gestión y control del hardware y software
18. Establecer normas y políticas de monitoreo, control y seguimiento de eventos
19. Establecer procedimientos de evaluación de rendimiento y calidad de servicio
3.3.1. Cobit como metodología de implantación de seguridad en WLAN

Según la metodología Cobit, todo comienza a partir de los objetivos de la organización. En tal sentido, en la figura 24 se muestran en color amarillo, las preguntas que le permitirán al negocio, identificar los objetivos de la institución, particularmente la que dicta: ¿Qué necesita?, la cual hace referencia a la información que requiere el negocio y que puede ser provista por los recursos de TIC disponibles en la organización.

![Figura 24. Principios de Cobit](image)

En tal sentido, la implantación exitosa de la seguridad de una WLAN debe tener en cuenta un conjunto de elementos organizacionales, económicos, funcionales, operativos y técnicos. Usando la metodología Cobit, pueden definirse un conjunto de objetivos de control que sirvan como pauta de referencia a los administradores de redes, gerentes de TIC y/o encargados de sistemas para la implantación de la seguridad de una WLAN tradicional:
### Tabla 4. Metodología de implantación de la seguridad en WLAN aplicando Cobit

<table>
<thead>
<tr>
<th>Metodología de Implantación de la seguridad en WLAN aplicando Cobit</th>
<th>Nivel de Riesgo</th>
<th>Ref. de Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. Entendimiento del negocio (PO)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Objetivo Control</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtener un conocimiento general de la empresa que utiliza la tecnología WLAN.</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td><strong>Acciones</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entrevistar al encargado de Sistemas para conocer:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Información de la empresa (nombre, sector económico, organización de TIC, etc.)</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td><strong>Objetivo Control</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conocer las TIC que soportan la operación del negocio.</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td><strong>Acciones</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Levantar información con el encargado de sistemas relativa a:</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>- Diagrama de red (plataforma, equipos, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Información de los sistemas operativos usados por la empresa.</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>- Planes de expansión donde el uso de la tecnología WLAN este presente y su consideración en el impacto de la seguridad.</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td><strong>II. Planificación del proyecto de implantación (PO)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Objetivo control</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definir y desarrollar el proyecto de implantación de la seguridad en la red inalámbrica segura</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>Acciones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Entrevistar al encargado de Sistemas para conocer y definir:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Responsables del proyecto</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Objetivos y necesidades a cubrir</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Alcance y limitaciones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Presupuesto disponible</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objetivo control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establecer los protocolos de comunicación y seguridad bajo la cual se van a usar las tecnologías WLAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acciones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas para definir y conocer:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Estándar de comunicación a utilizar 802.11a /b/g de acuerdo a las posibilidades del cliente.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Políticas de seguridad relacionadas con la tecnología WLAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Que está permitido y qué denegado sobre la WLAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Medidas de seguridad para el uso de la tecnología.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Evaluaciones de seguridad realizadas anteriormente a la plataforma y sus resultados.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Qué aspectos incluyen los programas de seguridad aplicados.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Frecuencia definida para la aplicación de los programas de seguridad.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Personal interno o terceras partes involucradas en las evaluaciones previas.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Planes de acción que permitan mitigar los riesgos.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Autoridad sobre las WLAN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>III Organización de las TIC (PO)</th>
<th>Nivel de riesgo</th>
<th>Referencia a Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objetivo de control</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>Identificar las unidades y personas encargadas de implantar la seguridad de la red WLAN y su mantenimiento.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acciones</td>
<td>Nivel de riesgo</td>
<td>Referencia a Documentos</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>IV. Lineamientos, políticas y normas de la seguridad en la Organización (PO)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Objetivo de Control</strong></td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>Establecer los controles preventivos, políticas y procedimientos a aplicar al sitio.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Acciones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas, los directivos de la organización y la unidad de recursos humanos para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desarrollar prácticas y políticas de seguridad relacionadas con WLAN y divulgar su uso a todos los miembros de la organización.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crear documentación de usuario para el uso apropiado de las tecnologías WLAN en la organización.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generar un acuerdo de confidencialidad de información que sea discutido, aprobado y firmado por los miembros de la organización.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>V. Seguridad en Tecnologías inalámbricas (PO)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Objetivo de Control:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establecer los controles de detección a implantar en la</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Acciones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identificar personas y unidades involucradas.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conocer sobre su nivel de entendimiento y discutir sobre qué planes, políticas, etc. aplicables al sitio.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determinar la experiencia del personal en el uso de la tecnología WLAN.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
organización sobre la tecnología WLAN; así como algunos controles preventivos asociados a dicha tecnología y la información transmitida a través de ésta.

Acciones:

Realizar una entrevista con el encargado de Sistemas para acordar:

- Mantener rastros de auditoria de las conexiones establecidas.
- Establecer y ejecutar procedimientos para revisar los rastros de auditoria y detectar actividades no autorizadas.
- Utilizar herramientas para monitorear el tráfico WLAN y detectar ocurrencias inusuales y excepciones potenciales.
- Definir procedimientos para encontrar las excepciones (las excepciones pueden conducir a deshabilitar conexiones de intrusos, configuraciones erradas puntos de acceso).
- Implantar Sistemas de Detección de Intrusos o Firewall en el segmento que contiene la WLAN.
- Establecer el uso de firewall antes de los puntos de acceso para proteger los recursos de posibles atacantes. La actividad debe quedar registrada en las auditorias, monitoreada y revisada.
- Colocar todos los puntos de accesos detrás del firewall.
- Utilizar el filtraje de direcciones MAC como mecanismo de seguridad.
- Implantar mecanismos de filtrados de tramas para que se envíe información innecesaria a otros segmentos de la red tales como el uso de redes virtuales (VLAN).
- Determinar un mecanismo de asignación de direcciones IP (Automático o manual). En caso de usar un DHCP determinar como serán asignadas las direcciones IP, si de manera dinámica o estática a través del administrador (ésta última opción es recomendable en el caso de WLAN y DHCP permite centralizar esta función).
- Configurar las estaciones de trabajo (PC de los clientes) para que estén por defecto, bloqueadas para el acceso a la red WLAN.
- Establecer mecanismos de seguridad como password para cuando son compartidos los archivos o carpetas que sólo se requieran.

<table>
<thead>
<tr>
<th>Objetivo de control</th>
<th>Indique el nivel de</th>
<th>Indique el nombre del(los)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Determinar aspectos relacionados con la seguridad física en la ubicación de los puntos acceso, así como con la configuración de los mismos y comparar estos contra las mejores prácticas.

<table>
<thead>
<tr>
<th>Acciones</th>
<th>riesgo del objetivo control</th>
<th>documento(s) producto del levantamiento realizado</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Decidir la ubicación de las estaciones bases colocándolas preferiblemente lejos de paredes externas y ventanas, cercanos al centro del edificio para evitar radiación externa.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Garantizar la ubicación de los puntos de acceso y antenas en lugares controlados con al menos las mínimas condiciones de seguridad física estipuladas para los equipos de comunicación de redes alámbricas.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objetivo de control</th>
<th>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establecer los mecanismos de cifrado a ser utilizados por la organización.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acciones</th>
<th>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:</td>
<td></td>
</tr>
<tr>
<td>Establecer un mecanismo de cifrado mediante el uso de protocolos preferiblemente WPA ó WPA2 combinado con el protocolo de autenticación EAP o EAP-TLS según sea el caso.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objetivo de control</th>
<th>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establecer mecanismos de autenticación.</td>
<td></td>
</tr>
</tbody>
</table>
Acciones
Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:

- Establecer el proceso de autenticación vía el protocolo RADIUS al momento de que un cliente intenta conectarse a la WLAN.
- Determinar características del servidor de autenticación donde será configurado RADIUS.
- Establecer políticas en relación al uso de servicios de directorio basados en el protocolo LDAP para incrementar la integridad y fortaleza de los mecanismos de autenticación de la organización.
- Determinar el uso de Redes Privadas Virtuales (VPN) como mecanismo de autenticación para sucursales y/o oficinas remotas.

VI. Adquisición e Implantación de la solución inalámbrica (AI)

<table>
<thead>
<tr>
<th>Objetivo control</th>
<th>Nivel de riesgo</th>
<th>Referencia a Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recolectar requerimientos de hardware y software para la solución inalámbrica y la implantación de la seguridad.</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
</tbody>
</table>

Acciones
Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:

- Levantar las necesidades del hardware y el software (puntos de acceso, dispositivos inalámbricos, tarjetas de red inalámbrica, servidor de autenticación, firewall, sistema de detección de intrusos, sistema de monitoreo de la WLAN, sistema de atención de requerimientos de usuarios, sistemas de control de acceso a áreas donde se encuentren los puntos de acceso, etc.).
- De acuerdo a la marca seleccionada por la organización, identificar modelos disponibles según los lineamientos previamente establecidos.

Objetivo control
Diseñar la topología de la solución de red inalámbrica

<table>
<thead>
<tr>
<th>Objetivo control</th>
<th>Nivel de riesgo</th>
<th>Referencia a Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diseñar la topología de la solución de red inalámbrica</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
</tbody>
</table>
## Acciones

Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:
- Identificar cantidad de usuarios de la solución
- Establecer cantidad de puntos de acceso/antenas requeridas y definir su ubicación física.
- Realizar site survey para validar ubicación física de los puntos de acceso.
- Establecer cantidad de puertos requeridos para la interconexión de los puntos de acceso con la red LAN.
- Seleccionar proveedor de equipamiento inalámbrico. (Recomendado hacer un documento de requerimiento de propuesta y enviarlo a los fabricantes de mayor experiencia en el ramo)

Diseñar la red y su seguridad teniendo en consideración aspectos como puntos de acceso e interconexión con la red LAN, servidor de autenticación, servicios y aplicaciones inalámbricas que se ejecutarán a través de la red inalámbrica, herramientas de monitoreo requeridas, sistema de atención de requerimientos, dispositivos inalámbricos terminales y sus características, protocolo de comunicación inalámbrico y compatibilidad con los dispositivos existentes si es el caso, localizaciones remotas y/o sucursales.

### Objetivo de control

Diseñar presupuesto para la implantación de la red y su seguridad.

### Acciones

Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:
- Desarrollar presupuesto para la implantación de la red inalámbrica.
- Desarrollar presupuesto para la implantación de la seguridad en la red inalámbrica.

### Objetivo control

Establecer procedimientos y normas para la instalación de equipos de la red inalámbrica. (Puntos de Acceso, servidores de autenticación, VPN, etc.)
<table>
<thead>
<tr>
<th>Acciones</th>
<th>Nivel de riesgo</th>
<th>Referencia a Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Definir normas de seguridad para la instalación de los elementos de la red inalámbrica.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Establecer configuración básica de la seguridad en los puntos de acceso y dispositivos inalámbricos de acuerdo a los protocolos de comunicación, cifrado y autenticación previamente definidos.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Establecer esquema de registro de la instalación de nuevos equipos en la red inalámbrica.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objetivo control</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>Establecer procedimientos y normas para las pruebas de funcionamiento de los mecanismos de seguridad de la red inalámbrica</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Establecer normas y procedimientos para probar el correcto funcionamiento del mecanismo de cifrado y autenticación implantados en la red inalámbrica.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Seleccionar herramientas para la ejecución de las pruebas de funcionamiento de los mecanismos de seguridad implantados en la red inalámbrica.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VII. Soporte y Servicios (SS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objetivo control</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
<tr>
<td>Establecer lineamientos para la gestión y mantenimiento de usuarios, perfiles y roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acciones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas, el administrador de la red y el personal de recursos humanos para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Definir los procedimientos, normas y políticas para la gestión de usuarios de la red inalámbrica.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Establecer normativas y procedimientos para renovación de contraseñas, cambio de usuario, modificación de roles y perfiles en concordancia con las estrategias de la organización.
- Establecer procedimientos para la creación, modificación y eliminación de usuarios, perfiles y roles coordinados preferiblemente por los responsables de recursos humanos en la organización.

<table>
<thead>
<tr>
<th>Objetivo control</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Definir esquema de atención de requerimientos y solicitudes vinculadas con la red inalámbrica</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
</tbody>
</table>

**Acciones**

Realizar una entrevista con el encargado de Sistemas, el administrador de la red y para:

- Definir el esquema de atención de requerimientos y solicitudes vinculadas a la red inalámbrica. Identificar procesos relacionados según la necesidad.

<table>
<thead>
<tr>
<th>Objetivo control</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Establecer procedimientos y normas para la instalación, actualización y remoción de equipos de la red inalámbrica. (Puntos de Acceso y servidores de autenticación)</td>
<td>Indique nivel de riesgo del objetivo control</td>
<td>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</td>
</tr>
</tbody>
</table>

**Acciones**

Realizar una entrevista con el encargado de Sistemas, el administrador de la red y para:

- Definir normas de seguridad para la actualización y remoción de los elementos de la red inalámbrica.
- Establecer procedimientos y normas para modificar la configuración de la seguridad en los puntos de acceso y dispositivos inalámbricos de acuerdo a los protocolos de comunicación, cifrado y autenticación previamente definidos.
- Establecer esquema de registro de las instalaciones, cambios de configuración, actualizaciones de los elementos de la red inalámbrica.
- Definir responsables dentro de la organización de
Estudio de metodologías de implantación de la seguridad en redes inalámbricas de área local
Universidad Metropolitana, Postgrado de la Facultad de Ingeniería, Caracas - Venezuela

<table>
<thead>
<tr>
<th>Objetivo de control</th>
<th>Nivel de riesgo</th>
<th>Referencia a Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establecer esquema de autorización para remoción de elementos de la red inalámbrica y cambios de la configuración de los parámetros de seguridad en la WLAN.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VIII. Monitoreo, control y seguimiento (ME)

<table>
<thead>
<tr>
<th>Acciones</th>
<th>Indique el nombre del(los) documento(s) producto del levantamiento realizado.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:</td>
<td></td>
</tr>
<tr>
<td>- Categorizar y tipificar los eventos de seguridad y sus niveles de criticidad.</td>
<td></td>
</tr>
<tr>
<td>- Establecer variables de seguridad a monitorear y fijar sus respectivos umbrales máximos y mínimos.</td>
<td></td>
</tr>
<tr>
<td>- Establecer responsabilidades de monitoreo, control y seguimiento dentro de las unidades de TIC</td>
<td></td>
</tr>
<tr>
<td>- Documentar procedimientos de monitoreo, control y seguimiento de eventos de seguridad.</td>
<td></td>
</tr>
<tr>
<td>- Establecer mecanismos de alerta por niveles según la criticidad de los eventos que se susciten.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objetivo de control</th>
<th>Nivel de riesgo</th>
<th>Referencia a Documentos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluar localizaciones de la WLAN a través de alguna herramienta centralizada de monitoreo de los puntos de acceso y los dispositivos inalámbricos en la red.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acciones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realizar una entrevista con el encargado de Sistemas y el administrador de la red para:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Seleccionar una herramienta que de manera centralizada permita visualizar un mapa de la red, controlar, monitorear y gestionar los eventos que se susciten en la WLAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Definir características del(los) servidores de monitoreo.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Evaluar las ubicaciones de los puntos de acceso, tanto las oficialmente sancionadas y aquellos no oficiales colocados que emanan señales desde dentro del sitio.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Determinar si los SSID\textsuperscript{13} son renombrados.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Determinar si los SSID son disimulados a través de la desactivación del broadcasting hacia el SSID de las estaciones base.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Revisar las direcciones MAC para inventariar los dispositivos WLAN con aquellos detectados por los puntos de acceso. Los puntos de acceso no documentados podrían ser conexiones no autorizadas, de terceros o equipos introducidos de forma no apropiada.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Aplicar pruebas perimetrales fuera de las facilidades, de ser posible, verificar si el rango de cobertura de los puntos de acceso es extendido más allá de las áreas de la organización.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Leyenda**

Nivel de Riesgo: Alto ☐ Medio ☐ Bajo ☐

\textsuperscript{13} SSID Identificador de Servicio (Service Set Identifier)
3.3.1.1. Cuadro de mando integral a partir de Cobit

A partir de los objetivos de control establecidos en cada dominio se puede construir un cuadro de mando integral (Balanced Scorecard en Inglés) tal y como se muestra en la figura 25:

![Figura 25. Cuadro de mando integral a partir de los dominios de Cobit.](image)

El cuadro de mando integral se deja propuesto como insumo para el lector, ya que no forma parte del objeto de estudio de la investigación.
### 3.3.2. ISO 17799 metodología de implantación de la seguridad en WLAN

Ahora bien, usando el estándar de seguridad internacional UNE/ISO-IEC 17799, la implantación de la seguridad de una WLAN tradicional puede llevarse a cabo de acuerdo a la siguiente metodología:

**Tabla 1: Sistema de Gestión de la Seguridad de la Información para redes inalámbricas de área local**

<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>3.1</td>
<td>Política de Seguridad de la información</td>
<td>a. ¿Existe una política de seguridad de la información en la organización, aprobada por los directivos de la institución, publicada y comunicada a todos los miembros de la organización? b. ¿Existe un comité gerencial encargado de la política de seguridad de la información en la organización comprometido con el manejo de la seguridad de la información?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>3.1.2</td>
<td>Revisión y Evaluación</td>
<td>a. Si la política de la seguridad tiene un responsable, establezca responsables para mantenerla y revisarla de acuerdo a los procesos definidos. b. Si se realizan cambios en la seguridad (incidentes, nuevas vulnerabilidades, cambios en la infraestructura técnica u organizacionales) verifique que los procesos aseguran la detección de los cambios que afecten los inventarios originales.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 2.1 Seguridad de la información de la Infraestructura

| 2.1.1| 4.1.1 | Comité de gerencia de la seguridad de la información | Verifique que exista un comité de gerencia que garantice una clara orientación y un soporte apreciable para las iniciativas de seguridad dentro de la organización. | |

| 2.1.2| 4.1.2 | Coordinación de la seguridad de la información | Asegúrese que los representantes del comité de gerencia de la seguridad de información, intercambien funciones y responsabilidades con los niveles intermedios de coordinación en la organización, a fin de garantizar la implementación adecuada de los controles de seguridad de la información. | |

<p>| 2.1.3| 4.1.3 | Asignación de responsabilidades de la seguridad de la información | Establezca lineamientos de responsabilidad para la protección de los activos y escriba procesos de seguridad específicos donde deje claramente establecidas las responsabilidades. | |</p>
<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.4</td>
<td>4.1.4</td>
<td>Proceso de Autorización para el procesamiento de la información</td>
<td>Establezca un proceso de autorización para el procesamiento de nuevas informaciones, tales como nuevas funcionalidades de hardware o software.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2.1.5 | 4.1.5                 | Asesor Especialista en seguridad de la información | a. Garantice que el asesor de seguridad de la información sea llamado cuando sea requerido.  
   b. Puede ser una empresa o persona que colabore con la coordinación de los conocimientos y experiencias que garanticen la consistencia y ayuden a tomar las decisiones relacionadas con la seguridad dentro de la organización. |                                               |              |
| 2.1.6 | 4.1.6                 | Cooperación entre organizaciones | Establecer mecanismos de comunicación con organismos de seguridad del estado, entes reguladores, operadores de telecomunicaciones, proveedores de servicios de información que le permitan tomar acciones rápidas en caso de la presencia de incidentes de seguridad. |                                               |              |
| 2.1.7 | 4.1.7                 | Auditorías externas de la seguridad de la información | Se recomienda revisar periódicamente con personal externo, la política de seguridad implementada. |                                               |              |
| 2.2   | 4.2                   | Seguridad del acceso de terceros |                                                                                           |                                               |              |
| 2.2.1 | 4.2.1                 | Identificación de los riesgos ante acceso de terceras partes | Identificar los riesgos ante el acceso de terceros mediante la apropiada identificación e implementación de estrictos controles de seguridad.  
   **Nota:** verificar si la organización cuenta con sucursales y/o sedes donde los usuarios requieran acceso a la red inalámbrica. Establecer procedimientos para autorización de usuarios a la red inalámbrica corporativa y la asignación de roles según los perfiles de usuarios previamente establecidos. Se recomienda definir un mecanismo de autenticación para control de acceso a la WLAN. |                                               |              |
| 2.2.2 | 4.2.2                 | Requerimientos de seguridad en contratos con terceras partes | Establecer modelos de contratos donde se plasme de forma explícita los requerimientos y exigencias para asegurar el cumplimiento de las políticas y estándares de seguridad de la organización.  
   **Nota:** Defina con el tercero, personas contacto responsables de garantizar las medidas establecidas en el contrato y coloque algún de clausula que implique obligaciones de tipo legal o económica que comprometan los intereses del tercero en caso de incumplimiento de las políticas de seguridad de la organización. |                                               |              |
### Seguridad Organizacional

<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td>4.3</td>
<td>Outsourcing</td>
<td>Requerimientos de seguridad en los contratos de Outsourcing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.3.1</td>
<td></td>
<td>Si los requerimientos de seguridad son plasmados en los contratos con terceras partes, y la organización está dejando en manos de otra empresa la administración y control de todos o parte de los sistemas de información, redes y ambientes de escritorio, estos deben contener de que forma se cubren las exigencias legales, como se prueban y mantienen los esquemas de seguridad de la organización, los derechos de auditorías, la seguridad física y como se mantendrá la disponibilidad de los servicios en caso de presencia de desastres.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Nota:** Si desea subarrendar la administración y control de la WLAN, asegúrese que los contratos contengan acuerdos de servicio, tiempos, garantías explícitas, cláusulas de confidencialidad de la información de la organización, niveles de satisfacción en lo que respecta a la disponibilidad de los servicios, entre otros aspectos.

### Clasificación y de los Activos

<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>5.1</td>
<td>Responsabilidad sobre los activos</td>
<td>Inventario de Activos</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.1.1</td>
<td></td>
<td>Se recomienda mantener un inventario con los activos más importantes y la información de sus características.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Nota:** Preferiblemente escriba un procedimiento para gestión de activos donde lleve control de las instalaciones, actualizaciones y remociones de los puntos de acceso inalámbricos y/o antenas y los dispositivos móviles propiedad de la organización. Este proceso puede ser automatizado mediante un software o manual.

### Clasificación de la Información

<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>5.2</td>
<td>Clasificación de la información</td>
<td>Pautas de Clasificación de la Información</td>
<td>Verificar si existe algún esquema de clasificación de los contenidos e informaciones de la organización, mediante el cual, se pueda determinar como se debe manejar la información y como protegerla. De no existir solicite al Comité de Gerencia de la seguridad de la información de la organización.</td>
<td></td>
</tr>
</tbody>
</table>

**Nota:** Según la WLAN que esté implementando, los tipos de contenidos que viajan mediante estas redes, clasifiquen los contenidos y defina mecanismos de cifrado de la información (EAP, EAP-TLS, Certificados SSL) y protocolos de autenticación para garantizar el principio de no repudiación e integridad de las informaciones.
### Identificación y manipulación de la información
De acuerdo al esquema de clasificación de los contenidos e informaciones de la organización, redacte procedimientos para la manipulación e identificación de la información.

| 3.2.2 | 5.2.2 | Identificación y manipulación de la información | De acuerdo al esquema de clasificación de los contenidos e informaciones de la organización, redacte procedimientos para la manipulación e identificación de la información. |

#### Seguridad del Personal de la Organización

<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>5.1</td>
<td>Seguridad en el trabajo</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 4.1.1 | 6.1.1 | Incluir la seguridad dentro de las responsabilidades del trabajo | Asegúrese que dentro de la política de seguridad de la organización se encuentren los roles y responsabilidades del personal con respecto a la seguridad. Se pudieran incluir responsabilidades generales para implementar y mantener la política de seguridad de acuerdo a las responsabilidades específicas de un perfil de personal, procesos o actividades especiales de seguridad. **Recomendación:** Incluya dentro de estas políticas de seguridad la verificación de accesos no autorizados a la WLAN por parte del personal, así como la colocación de puntos de acceso no autorizados por parte del personal con el propósito de incrementar el compromiso del personal con la seguridad de la WLAN de la organización. |

| 4.1.2 | 6.1.2 | Investigación y políticas de personal | Establezca procedimientos para investigar el carácter del personal, establezca verificaciones permanentes sobre el personal fijo de la organización y el uso dado a sus herramientas de trabajo. **Recomendación:** Selecione una herramienta donde se registren las operaciones realizadas por el personal durante su jornada laboral, donde se registre el uso de los recursos de los cuales dispone. Establezca procedimientos para garantizar el uso adecuado de los recursos, por ejemplo herramientas para administración del ancho de banda de la WLAN a fin de evitar caídas y colapsos periódicos. |

<p>| 4.1.3 | 6.1.3 | Acuerdos de confidencialidad | Establezca como norma que todos los miembros de la organización firmen el acuerdo de confidencialidad de la información como parte de los términos y condiciones de contratación inicial de la relación laboral, como mecanismo de prevención de la información de la organización y los activos de la misma. <strong>Recomendación:</strong> Establezca dentro de los procedimientos de la política de seguridad de la organización mecanismos para que miembros internos, terceros y responsables en caso de outsourcing también firmen estos acuerdos de confidencialidad. |</p>
<table>
<thead>
<tr>
<th>Referencia</th>
<th>Area de Autoría, objetivo y pregunta</th>
<th>Resultados</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Seguridad del Personal de la Organización</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.4</td>
<td>6.1.4</td>
<td>Términos y condiciones de contratación laboral</td>
</tr>
<tr>
<td>4.2</td>
<td>6.2</td>
<td>Entrenamiento de Usuarios</td>
</tr>
<tr>
<td>4.3</td>
<td>6.3</td>
<td>Respondiendo a los incidentes de seguridad malas prácticas</td>
</tr>
<tr>
<td>4.3.2</td>
<td>6.3.2</td>
<td>Reportando debilidades de la seguridad</td>
</tr>
<tr>
<td>4.3.3</td>
<td>6.3.3</td>
<td>Reportando inadecuado funcionamiento del Software</td>
</tr>
<tr>
<td>4.3.4</td>
<td>6.3.4</td>
<td>Aprender de los incidentes</td>
</tr>
<tr>
<td>Referencia</td>
<td>Area de Autoría, objetivo y pregunta</td>
<td>Resultados</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Seguridad física y del entorno de la organización</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Clausula del Estándar</td>
<td>Sección</td>
</tr>
<tr>
<td>5.1</td>
<td>7.1</td>
<td>Seguridad del área</td>
</tr>
<tr>
<td>5.1.1</td>
<td>7.1.1</td>
<td>Seguridad física perimetral</td>
</tr>
<tr>
<td>5.1.2</td>
<td>7.1.2</td>
<td>Controles físicos de entrada</td>
</tr>
<tr>
<td>5.1.3</td>
<td>7.1.3</td>
<td>Asegurando oficinas, salas y áreas físicas.</td>
</tr>
<tr>
<td>5.1.4</td>
<td>7.1.4</td>
<td>Trabajando en áreas seguras</td>
</tr>
<tr>
<td>5.1.5</td>
<td>7.1.5</td>
<td>Areas solapadas de distribución y carga de información</td>
</tr>
<tr>
<td>5.2</td>
<td>7.2</td>
<td>Equipamiento de Seguridad</td>
</tr>
<tr>
<td>5.2.1</td>
<td>7.2.1</td>
<td>Proteger equipos en lugares apropiados</td>
</tr>
<tr>
<td>5.2.2</td>
<td>7.2.2</td>
<td>Fuentes de alimentación</td>
</tr>
<tr>
<td>5.2.3</td>
<td>7.2.3</td>
<td>Seguridad del cableado</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adquiera patch coord certificados para conectar los puntos de acceso inalámbricos, antenas y servidores a los switchs de la red alámbrica de la organización. Se recomienda no fabricar estas piezas de la arquitectura en campo.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.2.4</th>
<th>7.2.4</th>
<th>Mantenimiento de equipos</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Seguir las recomendaciones de mantenimiento de equipos en cuanto a software y hardware estipuladas por el fabricante de la pieza. Particularmente para puntos de acceso (actualizaciones de sistema operativo, actualizaciones de consola de administración, actualizaciones de hardware, etc), tarjetas de red inalámbricas, firewall, sistemas IDS entre otros. Garantizar mediante procedimientos que sólo el personal autorizado por las unidades de TIC realicen estas actividades. Mantener registro de los cambios y actualizaciones mediante lo establecido en los procedimientos relacionados. Se recomienda adquirir contratos de soporte y garantías que cubran piezas y partes de los elementos de red de la WLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.2.5</th>
<th>7.2.5</th>
<th>Asegurando equipos fuera de norma</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Establezca procedimientos para garantizar que sólo bajo estricta autorización de los responsables de la implementación de la seguridad en la WLAN, sean colocados en funcionamiento equipos que no cumplan las premisas de la política de seguridad de la organización.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.2.6</th>
<th>7.2.6</th>
<th>Disposiciones de seguridad para equipos reutilizados</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Establezca procedimientos dentro de la política de seguridad para desincorporar equipos de la WLAN y dejarlos fuera del ambiente de producción.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.3</th>
<th>7.3</th>
<th>Controles Generales</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1</td>
<td>7.3.1</td>
<td>Política de bloqueo de escritorios y pantallas</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Desarrolle procedimientos para que los dispositivos cliente que accedan a la WLAN tengan activados mecanismos de bloqueo de pantalla automático luego de transcurrido un periodo sin uso del dispositivo.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.3.2</th>
<th>7.3.2</th>
<th>Propiedades de la remoción de equipos</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Implementar procedimientos para el retiro autorizado de los elementos de la WLAN. Mantenga actualizado los sistemas de monitoreo y ubicación de los elementos de la WLAN y audite periódicamente sus componentes a fin de prevenir retiros no autorizados de elementos críticos de la WLAN que se encuentre operando. Deje registros de los retiros realizados indicando fecha, responsable, causa del retiro del equipo y ente responsable de autorizar el retiro del elemento.</td>
</tr>
</tbody>
</table>
## Síntesis de la Gestión de la Seguridad de la Información para redes inalámbricas de área local

### Administración de la operación y las comunicaciones

<table>
<thead>
<tr>
<th>Referencia</th>
<th>Cláusula del Estándar</th>
<th>Sección</th>
<th>Pregunta de verificación</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>8.1</td>
<td>Responsabilidad y procedimientos operativos</td>
<td>Documentando procedimientos operativos</td>
<td>Establezca procedimientos para documentar las actividades operativas como instalación, configuración de parámetros de seguridad en puntos de acceso, backup de configuraciones de seguridad, gestión de certificados digitales, activación de mecanismos de autenticación y cifrado de información en los dispositivos clientes y servidores de la WLAN.</td>
<td></td>
</tr>
<tr>
<td>6.1.1</td>
<td>8.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.2</td>
<td>8.1.2</td>
<td>Cambios operativos</td>
<td>Establezca procedimientos para realizar cambios sobre los elementos de la WLAN, por ejemplo instalación de parches y actualizaciones de software de los puntos de acceso de la WLAN. Deje registro de los cambios siguiendo los procedimientos establecidos en la política de seguridad de la organización.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.3</td>
<td>8.1.3</td>
<td>Procedimientos de gestión de incidentes</td>
<td>Aplique los procedimientos para la gestión de los incidentes de seguridad para administrar los incidentes de la plataforma WLAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.4</td>
<td>8.1.4</td>
<td>Segregación de deberes</td>
<td>Se recomienda separar las áreas de responsabilidades a fin de reducir las brechas de seguridad por accesos no autorizados.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.5</td>
<td>8.1.5</td>
<td>Separación de ámbitos de desarrollo y ámbitos de operación</td>
<td>Se recomienda separar las WLAN de prueba de las que se encuentran en operación, para evitar incidentes de seguridad por accesos no autorizados mediante equipos o dispositivos que no cumplen con las políticas de seguridad de la organización.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.6</td>
<td>8.1.6</td>
<td>Administración de facilidades por entes externos</td>
<td>En caso de que la administración o procesamiento de algún tipo de información en la WLAN, sea responsabilidad de un ente externo se recomienda establecer mecanismos para garantizarle a la organización la seguridad de la información y el acceso controlado a los recursos disponibles, establezca mecanismos de autenticación como RADIUS para garantizar confidencialidad e integridad de la información por ellos administrada.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.7</td>
<td>8.1.7</td>
<td>Administración de facilidades por entes externos</td>
<td>En caso de que la administración o procesamiento de algún tipo de información en la WLAN, sea responsabilidad de un ente externo se recomienda establecer mecanismos para garantizarle a la organización la seguridad de la información y el acceso controlado a los recursos disponibles, establezca mecanismos de autenticación como RADIUS para garantizar confidencialidad e integridad de la información por ellos administrada.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Aceptación y planificación de sistemas

<table>
<thead>
<tr>
<th>6.2</th>
<th>8.2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>8.2.1</td>
<td><strong>Planificando las capacidades</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoree el tráfico de la WLAN, registre información sobre los accesos a la WLAN solicitados, la cantidad de usuarios que comparten el ancho de banda para proyectar el incremento de las redes ya que hasta el momento, la WLAN tienen limitadas las velocidades hasta 54 Mbps.</td>
</tr>
<tr>
<td>6.2.2</td>
<td>8.2.2</td>
<td><strong>Aceptación del sistema</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establecer procedimientos de prueba previa puesta en funcionamiento de sistemas y aplicaciones inalámbricas, por ejemplo, aplicaciones WAP, sistemas de monitoreo de puntos de acceso y dispositivos móviles entre otros.</td>
</tr>
</tbody>
</table>

## Protección contra virus y códigos maliciosos

<table>
<thead>
<tr>
<th>6.3</th>
<th>8.3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.1</td>
<td>8.3.1</td>
<td><strong>Control de software malicioso</strong></td>
</tr>
<tr>
<td></td>
<td>a.</td>
<td>Establecer mecanismos para garantizar la distribución y uso de software autorizados (licenciados) en la WLAN. Aplique el uso de herramientas para control de inventario de software en los dispositivos cliente de la WLAN a fin de garantizar la continuidad operativa del negocio.</td>
</tr>
<tr>
<td></td>
<td>b.</td>
<td>Revisar periódicamente los boletines de seguridad de los distintos sistemas operativos, programas y aplicaciones que funcionen en la WLAN a fin de aplicarlos y distribuirlos en el momento preciso y de forma segura a través de la WLAN.</td>
</tr>
<tr>
<td></td>
<td>c.</td>
<td>Implemente mecanismos preferiblemente automatizados de distribución de actualizaciones y parches a los dispositivos de la WLAN. (Puntos de acceso, Servidores de autenticación, firewall, IDS, VPN, dispositivos móviles, etc.).</td>
</tr>
<tr>
<td></td>
<td>d.</td>
<td>Proteja la red corporativa con una solución antivirus robusta que cuente con mecanismos de actualización de huellas antivirus y distribución de actualizaciones a través de la WLAN y la LAN.</td>
</tr>
</tbody>
</table>

## Respaldo de la información

<table>
<thead>
<tr>
<th>6.4</th>
<th>8.4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>8.4.1</td>
<td><strong>Respaldar la información del negocio</strong></td>
</tr>
<tr>
<td></td>
<td>Respalde configuraciones de puntos de acceso, servidores de autenticación, base de datos de usuario, entre otras que comprometan el funcionamiento de la WLAN. Desarrolle una política de respaldo para la organización y aplique una cláusula para el respaldo de la información crítica de la WLAN. Defina un método de respaldo (incremental, mensual, diario, semanal, etc). Mantenga registro de las operaciones de respaldo realizadas indicando responsable, fecha, identificación del medio de respaldo, etc.)</td>
<td></td>
</tr>
<tr>
<td>6.4.2</td>
<td>8.4.2</td>
<td><strong>Registro de las operaciones</strong></td>
</tr>
<tr>
<td></td>
<td>No aplica</td>
<td></td>
</tr>
<tr>
<td>6.4.3</td>
<td>8.4.3</td>
<td><strong>Registro de fallas</strong></td>
</tr>
<tr>
<td></td>
<td>Establezca procedimientos para el registro de las fallas de los mecanismos de seguridad de la WLAN. Utilice el sistema de atención de requerimientos y solicitudes para llevar control de los incidentes de fallas en los mecanismos de seguridad establecidos en la WLAN.</td>
<td></td>
</tr>
<tr>
<td>6.5</td>
<td>8.5</td>
<td>Administración de la red</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>--------------------------</td>
</tr>
<tr>
<td>6.5.1</td>
<td>8.5.1</td>
<td>Controles de la red</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defina los mecanismos de control para salvaguardar la confidencialidad e integridad de la data procesada sobre la WLAN. Seleccione los protocolos de autenticación y de cifrado de datos en función del estándar de comunicación 802.11 a/b/g que desee implementar. Se recomienda autenticar usando WPA/WPA2 con AES como algoritmo para cifrar las comunicaciones EAP/EAP-TLS para autenticación del lado del cliente y RADIUS del lado del servidor. Adicionalmente para el acceso remoto a la WLAN aplique sistemas VPN para acceder los contenidos de la red inalámbrica. Separe la administración de la WLAN de la administración de los sistemas inalámbricos presentes en los casos que sea necesario. Asegúrese de controlar los accesos desde sedes y sucursales asignando responsabilidades y procedimientos de administración para la gestión de estos controles.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.6</th>
<th>8.6</th>
<th>Seguridad y manipulación de medios</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.1</td>
<td>8.6.1</td>
<td>Administración de dispositivos removibles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No aplica</td>
</tr>
<tr>
<td>6.6.2</td>
<td>8.6.2</td>
<td>Disposición de medios</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No aplica</td>
</tr>
<tr>
<td>6.6.3</td>
<td>8.6.3</td>
<td>Procedimientos para manipulación de la información</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establezca controles para almacenar en dispositivos de almacenamiento masivo en la red corporativa, información crítica alojada en los dispositivos inalámbricos.</td>
</tr>
<tr>
<td>6.6.4</td>
<td>8.6.4</td>
<td>Seguridad del sistema de documentación</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aplique controles y normas para controlar accesos no autorizados al sistema de documentación de la organización.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6.7</th>
<th>8.7</th>
<th>Intercambio de información y software</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.7.1</td>
<td>8.7.1</td>
<td>Acuerdo de intercambio de software e información</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aplicar esquemas de control de acceso y seguridad para el intercambio de información y software interorganizaciones que prevengan el acceso a sectores de la organización no autorizados. Apoyese en lo estipulado en la política de seguridad de la organización para garantizar que existan los procedimientos para el intercambio de información.</td>
</tr>
<tr>
<td>6.7.2</td>
<td>8.7.2</td>
<td>Seguridad de medios en transito</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No aplica para WLAN</td>
</tr>
<tr>
<td>6.7.3</td>
<td>8.7.3</td>
<td>Seguridad en el comercio electrónico</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aplicar esquemas de control de acceso y seguridad para el intercambio de información y software interorganizaciones que prevengan el acceso a sectores de la organización no autorizados.</td>
</tr>
<tr>
<td>6.7.4</td>
<td>8.7.4</td>
<td>Seguridad en el correo electrónico</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aplicar esquemas de control de acceso y seguridad para el intercambio de información y software interorganizaciones que prevengan el acceso a sectores de la organización no autorizados.</td>
</tr>
<tr>
<td>6.7.5</td>
<td>8.7.5</td>
<td>Seguridad de los sistemas de oficina</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aplicar esquemas de control de acceso y seguridad para el intercambio de información y software interorganizaciones que prevengan el acceso a sectores de la organización no autorizados.</td>
</tr>
<tr>
<td>ID</td>
<td>Cláusula del Estándar</td>
<td>Sección</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------</td>
<td>---------</td>
</tr>
<tr>
<td>7.1</td>
<td>9.1</td>
<td>Política de Control de Acceso</td>
</tr>
<tr>
<td>7.2</td>
<td>9.2</td>
<td>Administración de Accesos de Usuarios</td>
</tr>
<tr>
<td>7.2.1</td>
<td>9.2.1</td>
<td>Registro de Usuarios</td>
</tr>
<tr>
<td>7.2.2</td>
<td>9.2.2</td>
<td>Administración de privilegios</td>
</tr>
<tr>
<td>7.2.3</td>
<td>9.2.3</td>
<td>Administración de Contraseñas de usuarios</td>
</tr>
<tr>
<td>7.2.4</td>
<td>9.2.4</td>
<td>Revisión de derechos de acceso de usuarios</td>
</tr>
<tr>
<td>7.3</td>
<td>9.3</td>
<td>Responsabilidades de los Usuarios</td>
</tr>
<tr>
<td>7.3.1</td>
<td>9.3.1</td>
<td>Uso de contraseñas</td>
</tr>
<tr>
<td>7.3.2</td>
<td>9.3.2</td>
<td>Equipos de usuarios desatendidos</td>
</tr>
<tr>
<td>7.4</td>
<td>9.4</td>
<td>Control de Acceso a la Red</td>
</tr>
<tr>
<td>7.4.1</td>
<td>9.4.1</td>
<td>Política de uso de los servicios de la red</td>
</tr>
<tr>
<td>7.4.2</td>
<td>9.4.2</td>
<td>Rutas preestablecidas</td>
</tr>
<tr>
<td>7.4.3</td>
<td>9.4.3</td>
<td>Autenticación de conexiones de usuarios externos</td>
</tr>
<tr>
<td>7.4.4</td>
<td>9.4.4</td>
<td>Nodo de autenticación</td>
</tr>
<tr>
<td>7.4.5</td>
<td>9.4.5</td>
<td>Diagnostico remoto para protección de puertos</td>
</tr>
<tr>
<td>7.4.6</td>
<td>9.4.6</td>
<td>Segregación en redes</td>
</tr>
<tr>
<td>7.4.7</td>
<td>9.4.7</td>
<td>Protocolos de conexión a la red</td>
</tr>
<tr>
<td>7.4.8</td>
<td>9.4.8</td>
<td>Control de rutas de red</td>
</tr>
<tr>
<td>7.4.9</td>
<td>9.4.9</td>
<td>Seguridad de los servicios de la red</td>
</tr>
<tr>
<td>7.5</td>
<td>9.5</td>
<td>Control de Acceso a los sistemas operativos</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>7.5.1</td>
<td>9.5.1</td>
<td>Identificación automática de dispositivos terminales</td>
</tr>
<tr>
<td>7.5.2</td>
<td>9.5.2</td>
<td>Procedimientos de Log-On de dispositivos terminales</td>
</tr>
<tr>
<td>7.5.3</td>
<td>9.5.3</td>
<td>Identificación y autorización de usuarios</td>
</tr>
<tr>
<td>7.5.4</td>
<td>9.5.4</td>
<td>Sistema de administración de contraseñas</td>
</tr>
<tr>
<td>7.5.5</td>
<td>9.5.5</td>
<td>Uso de utilidades del sistema</td>
</tr>
<tr>
<td>7.5.6</td>
<td>9.5.6</td>
<td>Alarma para resguardar usuarios</td>
</tr>
<tr>
<td>7.5.7</td>
<td>9.5.7</td>
<td>Time-out en dispositivos terminales</td>
</tr>
<tr>
<td>7.5.8</td>
<td>9.5.8</td>
<td>Limitación del tiempo de conexión</td>
</tr>
<tr>
<td>7.6</td>
<td>9.6</td>
<td><strong>Control de Acceso a las aplicaciones</strong></td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>7.6.1</td>
<td>9.6.1</td>
<td><strong>Restricciones de acceso a la información</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Si existen en la organización un conjunto de aplicaciones, si el negocio así lo requiere se pueden establecer políticas de control de acceso por grupo de usuarios de acuerdo a las aplicaciones que estos utilicen.</td>
</tr>
<tr>
<td>7.6.2</td>
<td>9.6.2</td>
<td><strong>Aislamiento de sistemas sensibles</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Algunas aplicaciones por sus características es recomendable que sean aisladas en ambientes de computo dedicados exclusivamente para ellas y que los recursos compartidos sólo se habilite para aplicaciones en las cuales se confíe.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.7</th>
<th>9.7</th>
<th><strong>Monitoreo de uso y acceso a los sistemas</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1</td>
<td>9.7.1</td>
<td><strong>Registro de eventos</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defina un esquema de monitoreo mediante el cual pueda hacerle seguimiento a los eventos suscitados en la WLAN y su entorno de acción. Se recomienda utilizar herramientas de software para llevar de manera proactiva el monitoreo de los dispositivos, su comportamiento y eventos en la red a fin de facilitar las labores de investigación en el futuro por eventos que han sucedido con anticipación.</td>
</tr>
<tr>
<td>7.7.2</td>
<td>9.7.2</td>
<td><strong>Uso de sistemas de monitoreo</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Documente procedimientos que establezcan el uso de las facilidades de monitoreo en los elementos que conforman la WLAN y su entorno crítico de acción. Habilite controles para verificar que los usuarios hagan solamente las actividades debidamente autorizadas por la organización. Así mismo, coloque en sus procedimientos de monitoreo, el chequeo periódico de la información que ha sido monitoreada para tomar medidas preventivas de acción.</td>
</tr>
<tr>
<td>7.7.3</td>
<td>9.7.3</td>
<td><strong>Sincronización de relojes</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active las facilidades de sincronización universal de horarios para los sistemas de computación existentes en la WLAN. Este mecanismo le permitirá mantener la consistencia de los eventos que puedan surgir de una auditoría o futura revisión.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.8</th>
<th>9.8</th>
<th><strong>Computación Móvil y teletrabajo</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1</td>
<td>9.8.1</td>
<td><strong>Computación Móvil</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Se recomienda diseñar una política de trabajo con dispositivos móviles especialmente en ambientes no protegidos. Aplique los mecanismos de seguridad para autenticación y cifrado de datos que se han mencionado anteriormente en la metodología. Haga del conocimiento del comité de gerencia de la seguridad de la información, que perfiles de usuario en la organización trabajaran en la WLAN y que tipo de actividades realizaran. Establezca procedimientos que le permitan verificar periódicamente las configuraciones de estos dispositivos, establezca políticas de distribución de actualizaciones de software y controladores a través de la WLAN.</td>
</tr>
<tr>
<td>7.8.2</td>
<td>9.8.2</td>
<td><strong>Teletrabajo</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aplique las técnicas, procedimientos y mecanismos previamente listados para el control de acceso remoto a las redes de la organización.</td>
</tr>
</tbody>
</table>
### Desarrollo y mantenimiento de sistemas

<table>
<thead>
<tr>
<th>ID</th>
<th>Clausula del Estándar</th>
<th>Sección</th>
<th>Requerimientos de seguridad de sistemas</th>
<th>Hallazgos</th>
<th>Cumplimiento</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>10.1</td>
<td>8.1.1</td>
<td>Requisitos, análisis y especificaciones de la seguridad</td>
<td>Asegúrese de que los nuevos sistemas cumplan con los requisitos de seguridad establecidos en la política de la organización. Los requisitos de seguridad y control identificados podrían reflejar el valor que tienen los activos de información involucrados para el negocio y en consecuencia el impacto de las fallas de seguridad. En tal sentido, es recomendable determinar los riesgos antes de iniciar el desarrollo de un sistema. En WLAN podría aplicar para sistemas WAP</td>
<td></td>
</tr>
<tr>
<td>8.2</td>
<td>10.2</td>
<td>8.2.1</td>
<td>Validación de datos de entrada</td>
<td>Verifique que todos los datos de entrada a la aplicación sean validados para asegurar que son correctos. En WLAN podría aplicar para sistemas WAP u otro tipo de sistemas que se utilicen a través de la WLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.2.2</td>
<td>Control de procesamiento interno</td>
<td>Verifique los ciclos de procesamiento de información para determinar las áreas de riesgo potencial y establecer los mecanismos de seguridad necesarios.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.2.3</td>
<td>Autenticación de mensajes</td>
<td>Habilite en sus sistemas mecanismos de validación por medio de mensajes de autenticación que garanticen el control de las operaciones permitidas a cada usuario según su perfil dentro de la organización. Según el tipo de información que se desee controlar, variarán los mensajes de autenticación.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.2.4</td>
<td>Validación de datos de salida</td>
<td>Verificar que los datos emitidos por las aplicaciones concuerden con la información almacenada y concuerdan con la situación. En la WLAN aplica esta clausula si cuenta con aplicaciones que permitan ingreso de datos y emitan resultados como por ejemplo sistemas de registro de inventario inalámbricos entre otros.</td>
<td></td>
</tr>
<tr>
<td>8.3</td>
<td>10.3</td>
<td>Controles Criptográficos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3.1</td>
<td>10.3.1</td>
<td>Política de uso de controles criptográficos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identifique en conjunto con el comité de gerencia de la seguridad de la información, que información en la organización debe contar con mecanismos de cifrado. Identifique con ellos, el nivel de protección de la información mediante un análisis de riesgo. Establezca dentro de la política de seguridad de la organización un procedimiento que indique la política de controles criptográficos para la protección de información.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3.2</td>
<td>10.3.2</td>
<td>Cifrado</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defina los protocolos de cifrado que utilizará la WLAN. Se recomienda analizar la compatibilidad de los equipos existentes, de ser el caso, con los protocolos más avanzados como por ejemplo WPA2 con CCMP con AES o TKIP a fin de brindarle altos niveles de integridad a la información que se envía mediante la WLAN.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3.3</td>
<td>10.3.3</td>
<td>Firmas digitales</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Las firmas digitales pueden colaborar con usted, para garantizar el principio de no repudiación durante el intercambio de documentos electrónicos. Se puede aplicar este mecanismo para identificar mensajes confidenciales en la WLAN.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3.4</td>
<td>10.3.4</td>
<td>Servicios de no repudiación</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Uno de los principios que debe perseguir la política de seguridad es la no repudiación de los contenidos procesados en la organización. Es decir, que cuando se envíe un documento se garantice que lo envíe quien dice que lo envío y no otra persona no autorizada para ello. En tal sentido, de acuerdo al tipo de contenidos que se compartan en su organización, debe establecer mecanismos de seguridad como firmas digitales o certificados digitales SSL para garantizar el cumplimiento de este principio. En WLAN, puede implementar certificados digitales usando el servidor de autenticación para distribuir estos certificados en la red.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3.5</td>
<td>10.3.5</td>
<td>Administración de llaves</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>En las redes inalámbricas de área local, las comunicaciones mediante protocolos WEP/WPA/WPA2 utilizan mecanismos de intercambio de llaves, sin embargo, la administración de llaves es centralizada solamente en esquemas WPA y WPA2 por lo que se recomienda utilizar estos protocolos para la comunicación en su WLAN.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.4</td>
<td>10.4</td>
<td>Seguridad de archivos de sistema</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.4.1</td>
<td>10.4.1</td>
<td>Control de Software operacional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establezca controles estrictos para la instalación de program as o aplicaciones en sistemas que forman parte de la operación diaria del negocio. De esta manera reducirá los riesgos de alteraciones en la operación por sistemas corruptos. Mantenga control sobre las actualizaciones de sistema operativo de los elementos de la WLAN para minimizar las fallas por problemas relacionados con instalaciones que no cumplan con las normas de seguridad establecidas.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.4.2</td>
<td>10.4.2</td>
<td>Protección de datos de prueba de sistemas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Si tiene en su organización redes inalámbricas de prueba para desarrollo de sistemas, coloque dicha red en un segmento de red separado de las redes tradicionales, así como los servidores donde se alojan los sistemas de prueba que se estén desarrollando. Aplique Virtual LAN para llevar a cabo esta acción.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.4.3</td>
<td>10.4.3</td>
<td>Control de acceso a librerías de program as fuente</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Si tiene en su organización redes inalámbricas de prueba para desarrollo de sistemas, coloque dicha red en un segmento de red separado de las redes tradicionales, así como los servidores donde se alojan los sistemas de prueba que se estén desarrollando. Aplique Virtual LAN para llevar a cabo esta acción. Establezca mecanismos de control de acceso a las librerías de los program as fuente que están desarrollados o en desarrollo. Esta acción le permitirá resguardarse de posibles brechas de seguridad por acciones de piratas informáticos que hayan logrado descifrar los códigos fuentes de los sistemas de su organización.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.5</td>
<td>10.5</td>
<td>Seguridad en procesos de soporte y desarrollo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.5.1</td>
<td>10.5.1</td>
<td>Procedimientos de control de cambio</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establezca procedimientos de control de cambio para los sistemas de su organización.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.5.2</td>
<td>10.5.2</td>
<td>Revisión técnica de cambios en los sistemas operativos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establezca procedimientos y responsables que aseguren el éxito de la aplicación de cambios sobre los sistemas. Así mismo establezca equipos de prueba según las características del proyecto de aplicación inalámbrica que este desarrollando que verifiquen la validez de los cambios realizados y su funcionamiento adecuado luego de ser pasados al ambiente operativo.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Cláusula del Estándar</td>
<td>Sección</td>
<td>Pregunta de verificación</td>
<td>Hallazgos</td>
<td>Cumplimiento</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------</td>
<td>---------</td>
<td>--------------------------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>9.1</td>
<td>11.1</td>
<td>9.1.1</td>
<td>Aspactos de la administración de la continuidad del negocio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1.1</td>
<td>11.1.1</td>
<td>Proceso de administración de la continuidad del negocio</td>
<td>El comité de gerencia de la seguridad de la información en conjunto con los responsables de las TICs, deben definir un plan para garantizar el desarrollo y mantenimiento de la continuidad operativa del negocio, en el que se mencionen cronogramas de pruebas y actualización de las TIC, se formulen y documenten las estrategias de continuidad del negocio que son específicas a cada organización. Se definan responsables por área, se identifiquen áreas de riesgo y vulnerabilidades que puedan incidir en la continuidad de las operaciones. En tal sentido, según se debe definir cuáles áreas de la WLAN son críticas para la continuidad del negocio y establecer lineamientos y estrategias para garantizar su continuo funcionamiento y alta disponibilidad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1.2</td>
<td>11.1.2</td>
<td>Continuidad del negocio y análisis del impacto.</td>
<td>Se recomienda solicitar al asesor de seguridad un análisis de riesgo que permita dilucidar el impacto de las interrupciones en el servicio y las operaciones del negocio. Este análisis debe ser suministrado al comité de gerencia de la seguridad de la información para ser revisado a fin de diseñar estrategias para el plan de continuidad del negocio en base a los resultados del análisis de riesgo y su impacto en las actividades relevantes de la organización.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1.3</td>
<td>11.1.3</td>
<td>Redactando e implementando un plan de continuidad del negocio</td>
<td>Se recomienda redactar el plan de continuidad del negocio y probarlo a fin de conocer las ventanas de tiempo tolerables que puede soportar el negocio en presencia de una interrupción en el servicio. Se recomienda contar con piezas de respaldo en sitio previamente configuradas como puntos de acceso inalámbricos de respaldo, switches de acceso a la red corporativa, tarjetas de red inalámbrica para los dispositivos terminales de respaldo, y de ser necesario un servidor de backup para los servicios de autenticación.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1.4</td>
<td>11.1.4</td>
<td>Marco de planificación de la continuidad del negocio</td>
<td>Recuerde que este plan es un marco que engloba todos los demás planes de continuidad del negocio, por lo que es altamente recomendable realizar pruebas periódicamente de cada uno de ellos a fin de identificar las prioridades en las que serán mantenidos y ejecutados en presencia de algún tipo de interrupción.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9.1.5 11.1.5 Pruebas, mantenimiento y determinación del plan de continuidad del negocio

Se recomienda establecer un procedimiento que regularice las pruebas relativas al plan de continuidad del negocio, donde se establezcan periodos y situaciones simuladas de prueba. Así mismo es fundamental que el comité de gerencia de la seguridad garantice que los establecido en el plan de continuidad del negocio esté siempre alineado con las estrategias del negocio.

<table>
<thead>
<tr>
<th>Referencia</th>
<th>Área de Autoría, objetivo y pregunta</th>
<th>Resultados</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>12.1</td>
<td></td>
</tr>
<tr>
<td>10.1.1</td>
<td>12.1.1</td>
<td></td>
</tr>
<tr>
<td>10.1.2</td>
<td>12.1.2</td>
<td></td>
</tr>
<tr>
<td>10.1.3</td>
<td>12.1.3</td>
<td></td>
</tr>
<tr>
<td>10.1.4</td>
<td>12.1.4</td>
<td></td>
</tr>
</tbody>
</table>

La Ley Especial Contra Delitos Informáticos regula todo lo que concierne a la seguridad y protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías. En tal sentido se deben desarrollar procedimientos alineados con lo estipulado en esta ley de la nación.

Establecer procedimientos para respetar los derechos de propiedad intelectual acordes con la legislación establecida al respecto. Dichos procedimientos se recomiendan estén bien implementados. Respetar los acuerdos establecidos al adquirir licencias para el uso de software.

Establece procedimientos y mecanismos para resguardar los registros de la organización para evitar que sean destruidos o falsificados. Algunas leyes obligan a las organizaciones a mantener registro de información por periodos de tiempo establecidos.

Establezca mecanismos de seguridad para garantizar la confidencialidad de los datos e informaciones personales. Según el protocolo de comunicación seleccionado para la WLAN, garantice la aplicación de políticas y procedimientos que habiliten estas facilidades en los dispositivos móviles, puntos de acceso y servidores de autenticación a fin de asegurar la privacidad de los contenidos.
| 10.1.5 | 12.1.5 | Prevención de malos usos de las facilidades de procesamiento de información | Utilice mecanismos centralizados de control de las operaciones del negocio a fin de evitar usos inadecuados de informaciones claves para la organización en actividades no relacionadas con los intereses del negocio. Identifique y controle los dispositivos móviles que salen y entran a la organización. Audite los contenidos allí almacenados y... |
| 10.1.6 | 12.1.6 | Regulaciones de los controles criptográficos | De ser requerido por el estado, país o sector de la economía donde se desenvuelva la organización establezca los esquemas de cifrado de información indicados por la legislación. No aplica aún en Venezuela. |
| 10.1.7 | 12.1.7 | Recolección de evidencias | Mantenga activos sus esquemas de auditoría, registro y seguimiento por periodos de tiempo adecuados de acuerdo al esquema de registro de información diseñado en la organización a fin de proveer evidencias en situaciones que por ley así lo requieran. |
| 10.2 | 12.2 | Revisión de cumplimiento de las políticas y técnicas de seguridad |  |
| 10.2.1 | 12.2.1 | Cumplimiento de la política de seguridad | Periodicamente debe ser verificado el cumplimiento de la política de seguridad, los estándares y procedimientos establecidos en la organización. Diseñe un procedimiento para con este respecto. |
| 10.2.2 | 12.2.2 | Verificación técnica del cumplimiento de la política de seguridad | Solicitar auditorias de los sistemas de vinculados con la WLAN a fin de verificar el cumplimiento de estándares, normas y procedimientos establecidos en la política de seguridad de la organización. Se debe chequear el funcionamiento de los protocolos de autenticación y cifrado de datos, los accesos no autorizados de personal ajeno a la organización. Verificar los registros de incidentes de seguridad en la WLAN y sus efectos. Chequear los sistemas operativos de los equipos de la WLAN, verificar las versiones y niveles de actualización de parches, revisar si existen puntos de acceso no autorizados y no documentados en base a los inventarios previos. |
### Consideraciones de auditorías de sistema

<table>
<thead>
<tr>
<th>10.3</th>
<th>12.3.1</th>
<th>Controles del sistema de auditorias</th>
<th>Se recomienda planificar minuciosamente los procesos de auditoria de la seguridad de la WLAN a fin de evitar interrupciones y posibles inconvenientes en los procesos del negocio.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>12.3.2</td>
<td>Protección de las herramientas de auditoria</td>
<td>Todas las herramientas de auditoría deben ser protegidas y controladas para evitar el uso inapropiado de las mismas o algún tipo de inconveniente relativo a la aplicación del proceso de revisión de la seguridad en la WLAN.</td>
</tr>
</tbody>
</table>
CONCLUSIONES

1. Las vulnerabilidades de seguridad presentes en las redes inalámbricas de área local en las organizaciones, generalmente responden al desconocimiento acerca de las tecnologías, protocolos y estándares disponibles por parte de los responsables de las unidades de TIC y a la falta de uso de metodologías para la implantación de la seguridad en este tipo de redes.

2. El mayor uso de las redes inalámbricas en las organizaciones y el aprovechamiento de los beneficios que éstas pueden aportar en el incremento de la productividad, eficacia y eficiencia de los procesos críticos del negocio, debe ir acompañado de metodologías orientadas a garantizar altos niveles de seguridad para los activos de información, los cuales, en la actualidad, representan el corazón de los negocios.

3. Las metodologías y los estándares internacionales ofrecen un marco de referencia basado en las mejores prácticas aplicadas a un área o sector específico del conocimiento. En la presente investigación, se utilizó el estándar de seguridad internacional ISO 17799 y la metodología Cobit como marco de referencia para la implantación de la seguridad en redes inalámbricas de área local. Ambos esquemas en la práctica se complementan uno al otro, con lo cual, se obtiene un grupo de herramientas que permiten abarcar en primer lugar, el entorno de seguridad de la red inalámbrica de área local, que es la organización, mediante la aplicación del estándar ISO 17799. En segundo lugar abarca los aspectos relativos a la implantación de la seguridad en la red inalámbrica propiamente dicha, usando la metodología Cobit, que además le brinda al negocio, una herramienta de control integral sobre la implantación de la seguridad de la WLAN desde el punto de vista financiero, del cliente, de los procesos involucrados y de la formación del recurso humano vinculado. En consecuencia, aumenta la probabilidad de éxito para que las organizaciones al
combinar ambas perspectivas, puedan diseñar, desarrollar e implantar una cultura de seguridad global que integre las diferentes aristas que generalmente caracterizan los negocios hoy por hoy.

4. Las organizaciones competitivas hoy en día fundamentan las estrategias del negocio en base a la disponibilidad, eficiencia y efectividad con la que puedan tomar sus decisiones. En este sentido la manera como se implante la seguridad de los medios que permiten acceder a los activos de información, en este caso, las WLAN, representa una clave para el éxito de las operaciones, independientemente del sector en el que se desenvuelva la institución.

5. Desde el punto de vista gerencial, es necesario contar con herramientas metodológicas como las estudiadas en la presente investigación, que facilitan el desarrollo de innovadoras soluciones basadas en las tecnologías inalámbricas y brindan el conocimiento necesario para dominar los aspectos relativos al mundo de las WLAN de una manera resumida, simple, concreta y fácil de extrapolar a otros campos relacionados a las Tecnologías de Información y Comunicación.

6. Las unidades responsables de las Tecnologías de Información y Comunicación, tienen cada vez mayor cantidad de retos y responsabilidades dentro de la línea estratégica de las organizaciones, lo cual implica un mejor y más estructurado orden en las labores de trabajo que le brinden a las mismas, amplias garantías en la continuidad de las operaciones. Este aspecto se encuentra directamente relacionado con la seguridad y la manera en la cual se gerencia dentro de la comunidad que conforma la institución. En este sentido, es crucial concientizar a los directivos de las organizaciones de su corresponsabilidad en el desarrollo de las estrategias de implantación de la seguridad como parte de los medios de lograr la logística necesaria para
impulsar la cultura de la seguridad en cada miembro de la empresa.

7. La implantación de la seguridad debe ser considerada como una de las principales misiones de los directivos de una organización dado los elevados costos que representa la paralización de la cadena de valor por incidentes no previstos de seguridad y su efecto negativo en la productividad y competitividad del negocio.
RECOMENDACIONES

1. Revisar periódicamente las nuevas versiones del estándar ISO 17799, de la metodología Cobit, de los avances de las tecnologías inalámbricas y sus respectivos estándares y protocolos a fin de garantizar la vigencia de la aplicación de ambos esquemas metodológicos.

2. Utilizar las metodologías de implantación resultado de la presentación investigación como una guía de trabajo para experimentar en una organización donde se pueda evaluar su aplicación real.

3. El desarrollo tecnológico de las WLAN aún es limitado en cuanto a las velocidades de transmisión, por lo que su implantación está dirigida a sectores específicos cuya principal necesidad es la movilidad. En tal sentido, es recomendable tener en cuenta este aspecto antes de desarrollar una solución de red corporativa basada en el uso de este tipo de redes, dado los altos costos que implica el desarrollo de un esquema de seguridad global basado en las mejores prácticas aquí estudiadas.

4. Por su flexibilidad y compatibilidad, se recomienda el estudio de implantación de estas metodologías en otras áreas de las Tecnologías de Información y Comunicación.

5. La documentación precisa, así como las técnicas metodológicas aplicadas, pueden ser elementos claves a considerar en cualquier tipo de proyecto de investigación, y especialmente si es de Tecnologías de Información y Comunicación, ya que ofrecen a todo aquel ente interesado en realizar estudios similares, un esquema de trabajo organizado y bien estructurado del proceso realizado. De igual manera el investigador se beneficia al mantener una estructura lógica y ordenada de su trabajo.
Bibliografía

Referencias citadas y notas

Disponible: www.bsi-global.com
[Consulta: 2006, Mayo 15]

Disponible: http://www3.ca.com/Files/WhitePapers/secure_manageable_enterprise_wylans.pdf
[Consulta: 2006, Abril 05]

Disponible: http://www.ca.com/wireless
[Consulta: 2006, Abril 05]

Disponible: http://www.cwnp.com
[Consulta: 2006, Mayo 10]

Disponible: http://www.cwnp.com
[Consulta: 2006, Abril 03]

Disponible: www.pc-news.com
[Consulta: 2006, Febrero 2]

[7] IEEE “802.1x Control de acceso basado en puertos”
Disponible: http://www.ieee802.org/1/pages/802.1x.html
[Consulta: 2006, Mayo 8]

Disponible: www.isaca.org
[Consulta: 2006, Junio 3]

[9] Lehembre, Guillaume, “Seguridad Wi-Fi WEP, WPA y WPA2”
[Consulta: 2006, Mayo 3]

[10] Microsoft Corporation “Introducción a la actualización de seguridad de WPA inalámbrico en Windows XP”
[Consulta: 2005, Diciembre 20]


Glosario de Términos

A

AAA: Tres pasos fundamentales del proceso de autenticación en redes de datos. Autenticación (proceso por el cual el usuario se identifica de forma unívoca y en muchos casos sin la posibilidad de repudio), Autorización (proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma) y Auditoria (mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no).

Access Point: Dispositivo que ejerce básicamente funciones de puente entre una red Ethernet con una red inalámbrica.

AES: Advanced Encryption Standard, también conocido como Rijndael, es un esquema de cifrado de datos por bloque adoptado como un estándar de codificación por el gobierno de los Estados Unidos.

C

CSS: Common Channel Signaling, es la transmisión de señales de información fuera de la señal de banda de información.

CHAP: Protocolo de Autenticación por desafío Mutuo (Challenge Handshake Authentication Protocol). Es un método de autenticación remota o inalámbrica.

D

DES3: Data Encryption Standard, es un algoritmo de cifrado cuyo uso se ha propagado ampliamente por todo el mundo. Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas.

E

EAP: Extensible Authentication Protocol, es una capa de autenticación, muy utilizada en redes inalámbricas y conexiones punto a punto.

EAP-TTLS: EAP-Tunneled Transport Layer Security, es un protocolo ampliamente utilizado entre plataformas, es un mecanismo que ofrece muy buena seguridad mediante el uso de certificados PKI solamente en el servidor de autenticación.

F

FCC: La Comisión Federal de Comunicaciones, es un organismo encargado de la
administración del espectro radioeléctrico en los estados unidos.

**FHSS:** Espectro ampliado por salto de frecuencia, es un método para transmitir señales cambiando rápidamente la portadora entre muchas frecuencias, utilizando una secuencia seudoaleatoria conocida solamente por el transmisor y el receptor.

**Firewall:** Un cortafuegos, es un elemento de hardware o software utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidas según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.

**GHZ:** El hercio es la unidad de frecuencia del Sistema Internacional de Unidades. Proviene del apellido del físico alemán Heinrich Rudolf Hertz, descubridor de la transmisión de las ondas electromagnéticas. Su símbolo es Hz (escrito sin punto como todo símbolo). En inglés se llama hertz.

**HTTP:** Protocolo de transferencia de hipertextos, es usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

**IDS:** Un sistema de detección de intrusos es un programa usado para detectar accesos desautorizados a un computador o a una red.

**IPS:** Un sistema de prevención de intrusos es un dispositivo encargado del control de acceso y la protección contra ataques a los elementos de la red. Es considerado una extensión del IDS, pero en la actualidad se considera una capa más del firewall.

**IPSec:** la abreviatura de Internet Protocol security, es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente fue desarrollado para usarse con el nuevo estándar IPv6, aunque posteriormente se adaptó a IPv4.

**LEAP:** Lightweight Extensible Authentication Protocol, es un método de
autenticación propietario para redes inalámbricas desarrollado por Cisco Systems.

**L2TP**: Layer 2 Tunneling Protocol, utiliza el protocolo PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado.

**M**

**MAC Address**: En redes de computadoras la dirección MAC (Media Access Control address) es un identificador alfanumérico de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los 24 bits restantes).

**MHZ**: Un Megahercio (MHz) equivale a $10^6$ hercios (1 millón), unidad de medida de frecuencia.

**P**

**PPP**: Point-to-Point Protocol, es decir, Protocolo de conexión punto a punto. Es un protocolo que funciona a nivel de la capa de enlace, estandarizado en el documento RFC 1661.

**PLC**: Power Line Communications, también denominada BPL (Broadband over Power Lines) es una tecnología basada en la transmisión de datos utilizando como infraestructura la red eléctrica.

**PPTP**: Point to Point Tunneling Protocol, es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implantar redes privadas virtuales o VPN.

**PAP**: Password Authentication Protocol, es un protocolo de autenticación usado para registrar un usuario en un servidor de acceso remoto o proveedor de servicios de Internet.

**R**

**RC4**: En la criptografía RC4 o ARC4 es el sistema de cifrado de flujo más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas).

**S**

**SSL**: Secure Sockets Layer es un protocolo de cifrado que proporcionan comunicaciones seguras en Internet.
**XOR**: La compuerta lógica Ó-exclusivo es el resultado de aplicar lógica negativa al resultado de la compuerta lógica OR.

**WiMAX**: Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas es un estándar de transmisión inalámbrica de datos (802.16d) diseñado para ser utilizado en el área metropolitana o MAN proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS.