UNIVERSIDAD DE PANAMÁ

FACULTAD DE INFORMÁTICA, ELECTRÓNICA Y COMUNICACIÓN

ESCUELA DE INGENIERÍA EN INFORMÁTICA

ESTUDIO DE FACTIBILIDAD DE CREACIÓN DE UNA RED INALÁMBRICA WIFI PARA EL EDIFICIO A-B DEL CENTRO REGIONAL UNIVERSITARIO DE VERAGUAS

TRABAJO DE GRADUACIÓN PARA OPTAR POR EL TÍTULO DE LICENCIATURA EN INGENIERÍA EN INFORMÁTICA

ELABORADO POR:

ROSA Y., LÓPEZ P.

SANTIAGO, REPÚBLICA DE PANAMÁ.

AGOSTO, 2011

PROFESOR ASESOR:

RAÚL ENRIQUE DUTARI DUTARI, M.SC.

PROFESOR ESPECIAL IV

TIEMPO COMPLETO

AGRADECIMIENTO

Primero a Dios Todopoderoso, que con él nada es imposible, a mi Jesús Nazareno de Atalaya, por estar conmigo siempre.

A mis padres, que han estado para apoyarme siempre e incondicionalmente.

A los profesores de la Facultad de Informática, Electrónica y Comunicación, que de una forma u otra han colaborado a la realización de este estudio y a lo largo de mi carrera, en especial al Profesor Diego Santimateo y la Profesora Giannina Nuñez.

Gracias especiales al Profesor Edwin Cedeño, que en un inicio fue mi asesor, logrando la aprobación del anteproyecto.

Mi enorme agradecimiento a mi asesor el Profesor Raúl Enrique Dutari Dutari, a usted profesor gracias por su apoyo y paciencia. Mil Gracias.

Por último a todos los que de forma directa o indirecta jugaron papeles durante el desarrollo de este trabajo.

DEDICATORIA

A mis amados padres *José A. López L.* y *Rosa E. Pineda.*, quienes han sido mis pilares fundamentales que con su apoyo incondicional son las personas a quienes les debo todos mis logros alcanzados.

A mi amada hija *Darlenys Elena Delgado López*, una razón más para impulsar mis anhelos de alcanzar el éxito.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

RESUMEN DEL PROYECTO

En el Edificio A-B del Centro Regional Universitario de Veraguas, se cuenta con una red cableada, que constituye la red de datos de los Laboratorios de Informática de la FIEC-CRUV. Por otro lado, el modelo de red actualmente ocasiona varios problemas entre ellos están: la dependencia estacionaria de los equipos, la falta de flexibilidad y la movilidad de los equipos que restringe en gran medida el mejor rendimiento y aprovechamiento del sistema de red.

Adicionalmente, desde el año 2010, se instaló un nodo de Internet Para Todos, del Gobierno Nacional, que, sin embargo, presenta inconvenientes en cuanto a la descarga de archivos de gran tamaño y su servicio falla con demasiada frecuencia.

La utilización de tecnologías inalámbricas permite solventar los inconvenientes mencionados con anterioridad, y para lograr el objetivo de ofrecer un servicio de calidad se deben contemplar estos aspectos: confiabilidad, autenticación, integridad, disponibilidad.

El desarrollo de este estudio está estructurado con base en la elaboración de los diseños de la red, tanto físico como lógico; la ubicación de los puntos de acceso (**PA**) y de estación (portátiles), siguiendo la organización de la investigación transeccional descriptiva utilizada en el desarrollo de este escrito.

Por otro lado, se analizan los atributos que se deben tomar en cuenta para brindar seguridad al diseño planteado. Entre los que destacan: la confidencialidad y control de acceso, que por medio de técnicas de seguridad se pueden controlar. Además, se establecen lineamientos que norman aspectos tales como: el propósito de la red, su privacidad, las responsabilidades, sus condiciones de uso, disponibilidad, conexión, procedimientos de seguridad, ética y moral, autorización, regulaciones y estándares.

Finalmente, se plantea un análisis financiero, para determinar la factibilidad del proyecto, mediante el procedimiento de estimación financiera TIRE, VANE, con el objeto de justificar su implementación.

INTRODUCCIÓN

La falta de un sistema de red inalámbrica, que permita mejorar el servicio existente, en el área de edificio A-B del CRUV, se refleja en un conjunto de limitaciones que se observan en los sistemas de comunicación de datos con que cuenta la FIEC (Facultad de Informática, Electrónica y de Comunicación). Estas limitantes ven reflejados en términos de la falta de movilidad y de flexibilidad al momento de conectarse a la red cableada existente; así como también en el libre estacionamiento de equipos, según sea la necesidad de los usuarios de la red que poseen sus propios computadores.

En consecuencia, la necesidad de incorporar las tecnologías inalámbricas a la implementación de los procesos de enseñanza - aprendizaje que ofrece la Universidad de Panamá, en el CRUV (Centro Regional Universitario de Veraguas), en el área del edificio A-B, es el problema que se trata de resolver dentro de este proyecto.

Por lo tanto, en este estudio de factibilidad se busca establecer las especificaciones y el diseño, para la creación de una red inalámbrica en el área del edificio A-B del CRUV. Este sistema de comunicaciones debe, brindar acceso desde un equipo móvil al sistema de comunicación de datos cableado pre-existentes.

En el primer capítulo, se explican las generalidades del problema bajo estudio, detallando los antecedentes, estado actual de la red existente, definición

del problema, justificación del estudio, objetivos generales y específicos, además del alcance y las limitaciones de este estudio.

En el segundo capítulo, se describen las tecnologías **WIFI**, sus antecedentes, los estándares IEEE 802.11X, y sus características técnicas, así como también los aspectos de seguridad de las redes inalámbricas, así como los puntos de diseño de la red **WIFI**.

En el tercer capítulo, se detallan aspectos metodológicos de diseño de investigación, tales como el diseño y el tipo de investigación.

En el cuarto capítulo, se especifica el diseño de la red inalámbrica, las pruebas de cobertura, los diseños físico y lógico, así como también las políticas de seguridad que se aplicarán, la selección de componentes, el presupuesto, y los análisis financieros correspondientes que muestren los costos vs. beneficios del proyecto.

Este proyecto se plantea como una alternativa que mejorará el servicio de acceso a los sistemas de comunicación de datos de las redes LAN de la FIEC, para el Edificio A-B, del Centro Regional Universitario de Veraguas.

CAPÍTULO 1: GENERALIDADES DEL PROBLEMA.

Con el auge de crecimiento de la población universitaria en el Centro Regional Universitario de Veraguas (CRUV), se marcó en sus principios una serie de necesidades académicas, las cuales obligaron a la creación de un movimiento estudiantil y comunitario, el cual tenía el objetivo, la exigencia de procesos de la incorporación de tecnologías de la información en el desarrollo de enseñanza-aprendizaje. Por ello, a continuación se muestra un breve resumen del desarrollo de este planteamiento.

1.1 Antecedentes.

El CRUV, ubicado en la ciudad de Santiago, recibe su actual denominación a partir de la reapertura de la Universidad de Panamá en 1969. Anteriormente el Centro era denominado EXTENSIÓN UNIVERSITARIA DE VERAGUAS, nombre que le dio, la Asamblea Nacional de Panamá, cuando las Extensiones fueron creadas mediante LEY No. 4 del 13 de Enero de 1958 **[BAAR79]**.

La Extensión Universitaria de Veraguas, al reabrir sus puertas después del Golpe de Estado del 11 de octubre de 1968, recibió la nueva denominación de acuerdo con el decreto de Gabinete No. 144, del 3 de junio de 1969, el cual sirvió de base para la reapertura de la Universidad de Panamá y su funcionamiento.

La infraestructura del Centro, es una réplica de los planos y maquetas del trabajo de graduación del Arquitecto veragüense, Carlos A. Hooper, quien donó copia de los planos y de las maquetas.

La Memoria del 7 de febrero de 1972, presenta los siguientes detalles acerca del proyecto de los edificios del Centro:

Las instalaciones tendrían una capacidad de 2,400 estudiantes, atendidos por aproximadamente 50 profesores y 25 unidades administrativas. El programa general del diseño (primera fase): Docencia: 2,500 metros cuadrados, aproximadamente, incluyendo 20 aulas de clases, 6 laboratorios y un auditorio. Servicios comunes: 1,000 metros cuadrados, incluyendo administración, oficinas, almacén y otras **[MEMO72]**.

En esta primera fase, el Centro, presentó una estructura física y equipamiento con las siguientes características:

Edificio principal: Constituido por dos plantas: con una superficie de 450 metros cuadrados.

Edificio Auditórium: De una sola planta, con una superficie de 450 metros cuadrados.

Área de estacionamiento y recreación **[MEMO72]**.

Con relación al espacio de las aulas, y el incremento de la población universitaria se hacía necesario dictar clases en los laboratorios y en el auditórium. Esta situación motivo a la familia universitaria gestionar, la construcción de la segunda fase.

Una partida de B/. 1, 380,000.00 se desgloso para la construcción de las siguientes unidades: 40 aulas, 2 laboratorios, 2 talleres **[MEMO72].**

Con esta partida, se dio la finalización de la construcción de la obra en su segunda fase, dando así por terminada las 2 etapas y así el nacimiento de las infraestructuras del Centro Regional Universitario de Veraguas.

1.1.1 ESTADO ACTUAL DE LA RED DEL EDIFICIO A-B.

En el edificio A-B de Centro Regional Universitario de Veraguas, se cuenta con aulas que poseen un sistema de red, estas secciones, se les denomina Laboratorios de Informática (Aulas: A3, A4, A5), respectivamente; esta surgió de la necesidad de dotar de sistema de red para brindar de acceso a la red de Internet **ADSL** 512kb/128kb, mediante la autogestión de la FIEC **[DUTA09]**.

Esta red se estructura de la siguiente forma: de la red ADSL, se conecta a un **Router** 10Mbits (1RJ-45,1 Consola, 1 RJ-11), además se conecta a un **Switch** principal de 100Mbits (8 RJ-45) **[DUTA09]**.

Del **Switch** principal (8 RJ-45), se interconecta a los Laboratorios de Informática (A3, A4, A5), a la Coordinación de la FIEC (Facultad de Informática, Electrónica y Comunicación), y Mantenimiento, en el cual operan unas 60 estaciones de trabajo. Esta estructura, permite la interconexión entre las estaciones de trabajo en cada Laboratorio, con acceso restringido entre cada estación de trabajo **[DUTA09]**.

En un principio, sólo se contaba con un número restringido de equipos de trabajo, ya que fue en el año 2000, entre los meses de Agosto y Diciembre, que se dio la extensión de red cableada del laboratorio A5, aula A3 y posteriormente se habilito el A4.

Actualmente, la red está con tendencia a la interconexión, a la red universitaria por medio de fibra óptica, la cual está debidamente instalada en espera a la conexión de ambas redes, tanto para la que existe en el Edificio A-B y C.

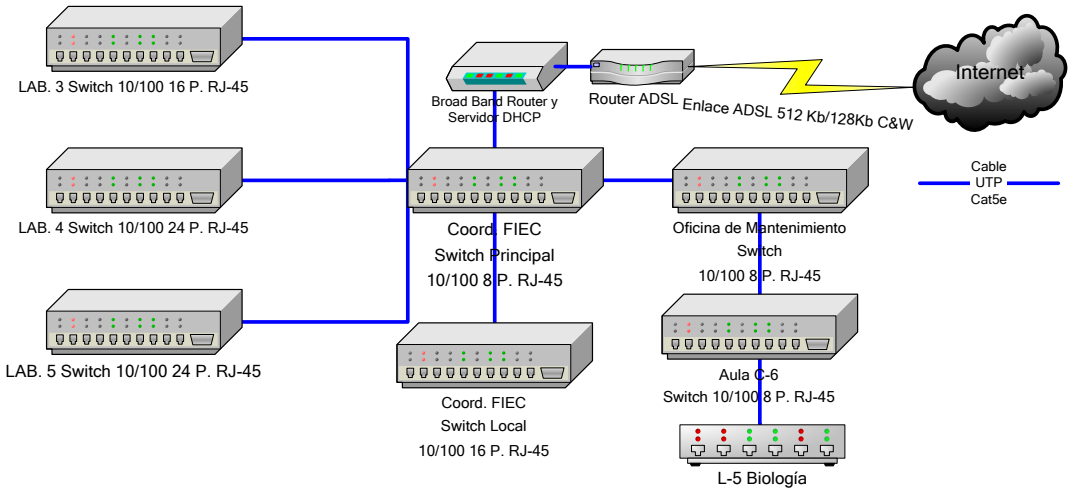

Ilustración 1.1: Diagrama Lógico De La Red De Datos, Del Edificio A-B Del Centro
Fuente: [DUTA09]

La red de comunicaciones de los laboratorios de informática, es independiente a la red administrativa universitaria del Centro, ya que, es suministrada directamente de la Compañía de Cable & Wirelless, y no se encuentran por el momento interconectadas.

La Facultad de Informática, Electrónica y de Comunicación, posee una red cableada estándar, no certificada, la cual no tiene fines de lucro siendo netamente educativa, que se mantiene con régimen de seguridad estructural y de igual manera da cabida a múltiples usuarios.

Adicionalmente, desde inicios del año 2010, se cuenta con un punto de acceso del proyecto **Internet Para Todos**, una **WAN** que fue creada por el Gobierno Nacional y que cuenta con cobertura nacional. Esta red posee una velocidad de 1Mb simétrico, sin embargo, no permite descargar archivos de gran

tamaño; adicionalmente, únicamente permite el uso cuentas de correo Web basadas en Gmail **[DUTA09]**.

En el área de estudio de la propuesta de creación de una red inalámbrica en el edificio A-B del CRUV, es necesario realizar una evaluación a la estructura de la red cableada que existe actualmente, como también a la infraestructura del edificio, se tomará referencia las características de organización física y lógica de la red, para así diseñar el modelo de la red **WIFI** , como complemento a la red cableada existente en las aulas A3-A4-A5, y así proveer de acceso a la red de forma inalámbrica a todo el edificio y a sus alrededores.

1.2 Definición Del Problema.

La falta de un servicio de red inalámbrica en el área del edificio A-B del CRUV, limita la capacidad de acceso al sistema de comunicación de datos de la FIEC, ya que implica limitantes de movilidad y dependencias a las redes cableadas que se encuentran operando actualmente.

Por otro lado, el crecimiento de las redes de datos es incontenible y su importancia para el Centro aún más, ya que en ellas, circula información con mayor rapidez y eficiencia, sustituyendo los viejos modelos de procesos de comunicación.

Hoy en día, en el área del edificio A-B del CRUV, la red que permite el acceso al canal de comunicación de datos, es mediante redes cableadas. A esto

se le añade la escasa documentación física que se tiene de ella, imposibilitando así su crecimiento controlado; cada cable nuevo colocado contribuye a aumentar el caos, tanto en diseño como en administración del sistema. Por lo tanto es imperativa la redefinición de la misma en cuanto a topología física y lógica.

Por otra parte, dicha red presenta fallas a nivel físico, por la misma estructura física de su localización existente: en las aulas (A3, A4, A5). Además, se suma un problema de calidad de servicio (**QoS**), que se evidencia en la falta de rendimiento en el acceso a la red de comunicación. Finalmente, no existen controles de seguridad adecuados para utilizar la conexión de banda ancha.

Actualmente, es de vital importancia tener como horizonte el mejoramiento y actualización constante de la tecnología de redes de datos, hoy en día la tecnología emergente para este tipo de transporte rápido de información es la tecnología inalámbrica, las cuales son apoyadas por estudios a nivel mundial, desarrollados por organizaciones internacionales que rigen el desarrollo de las redes **WIFI**, que sin cables, ni ataduras físicas, más que las necesarias por los propios equipos de comunicación, nos permite hacer lo mismo que con las redes cableadas, y ya es tiempo que éstas se consideren como una solución, no tan solo para sitios donde es difícil implementar redes cableadas, sino como un diseño definitivo de propósito general.

Las limitantes de la red cableada obligan a plantear una solución: por la naturaleza de la comunicación inalámbrica, la red **WIFI** ha ganado la reputación

de ser una tecnología madura y robusta que permita resolver los inconvenientes planteados, en el uso de cable como medio físico de enlace de la comunicación.

1.3 Justificación.

Con este estudio, se pretende ofrecer un sistema de red inalámbrica, con el propósito de lograr el mejor aprovechamiento del sistema de comunicación de datos, que se cuenta actualmente en esta área; tomando como referencia, las desventajas entre la red cableada versus, la red **WIFI**, para dotar a las demás áreas del edificio A-B, de acceso al sistema de red, bajo el estándar 802.11X, propuesto por **IEEE**, basados en tecnologías **WIFI**, para el edificio A-B del CRUV,

Existen debilidades en el uso de los equipos en las aulas A3, A4, A5; ya que no existe un control en el uso de los recursos y el principal factor, la dependencia que se encuentran las estaciones de trabajo, a la conexión al sistema de comunicación de datos dentro de las aulas.

Esto conlleva la necesidad de incorporar las nuevas tecnologías **WIFI**, que han demostrado ser una alternativa viable para resolver las necesidades de comunicación, a nivel educativo, o de otros fines, en la infraestructura bajo estudio.

El creciente bagaje tecnológico, que ofrece nuevas funcionalidades que integran datos, así como la incorporación de nuevos servicios telemáticos, lleva

a la necesidad de ampliar las facilidades de comunicación de los sistemas con que actualmente se cuenta.

En consecuencia, las redes inalámbricas, se crean como respuesta a la investigación y desarrollo de la industria inalámbrica y móvil. Hoy muchas empresas y organizaciones de entornos muy variados, se están avocando a estas soluciones para comunicación interna como externa, para permitir la interconexión de dispositivos y por supuesto del enlace con el sistema de comunicación de redes.

La falta de tecnología de un servicio de red inalámbrica en el área de edificio A-B del CRUV, limita la capacidad de resolver obstáculos y limitantes en el acceso al sistema de comunicación de datos, en el edificio objeto del estudio, esto conlleva a ciertas fallas tanto en movilidad como de flexibilidad, del libre estacionamiento de equipos según sea la necesidad del usuario de la red.

Dentro de las especificaciones en facilidades de la comunicación y del enorme horizonte de comunicación inalámbrica, se hace posible resolver los inconvenientes del uso del cable como medio físico de enlace, en la comunicación dentro del área del edificio A-B del CRUV.

Las limitantes que presenta el sistema de red, que actualmente existe en las aulas A3, A4, A5, lleva a la dependencia total de los equipos, para permitir el uso de las computadoras, con la necesidad de enchufes y cables que limitan movilidad del equipo; tanto para disponer de acceso a la red con un móvil, como

igual se restringe en gran medida el mejor rendimiento y aprovechamiento del recurso del sistema de red que existe en las aulas antes mencionadas.

Por otro lado, la red inalámbrica **Internet Para Todos**, también posee debilidades, que le impiden satisfacer las demandas de servicio y necesidades de los usuarios, que le red propuesta procura complementar, en cuanto el acceso y descarga de archivos **[FEFR11]**.

Uno de los factores que más limita a Internet Para Todos, es que sólo permite la utilización de un servidor de correo Web único – Gmail -, lo que limita la funcionalidad del servicio para usuarios de otros servicios de correo Web.

A esta problemática, se suman las fallas a nivel de hardware, que ocasionalmente limitan el contar con el servicio las 24 horas del día. Es relevante, señalar, que dicha observación, es independiente de la cobertura que ofrece del servicio **[FEFR11]**.

Por otro lado, estudios que se han realizado en diferentes organizaciones como: **WECA**, **IEEE**, **ETSI** encargadas del desarrollo de tecnologías **WIFI** han demostrado que:

> *"Existen a nivel mundial una auge incremental en tendencias tecnológicas de comunicación inalámbricas, ofreciendo un apoyo técnico en el aprendizaje y de los recursos necesarios, que llevan a gestionar proyectos de incursión en aumento de la productividad tanto de profesores como de estudiantes…"* **[BASU04].**

La principal ventaja de este tipo de redes (**WIFI**), es que: no necesita licencia para la utilización de la banda de 2.4GHz, en donde opera esta tecnología, la libertad de movilidad que permite a sus usuarios.

Por otro lado, se puede hacer uso de la red, en cualquier lugar ya sea abierto o cerrado, buscando un lugar fijo y agradable en donde se puede trabajar.

De igual modo este estudio, se permitirá mostrar la zona de servicio de la misma, para conocer el alcance y limitantes de la creación de la red inalámbrica, en el área del edificio A-B del CRUV, que ofrezca el acceso al mayor número de posibles usuarios, la ubicación de cada punto de acceso, para que así el área bajo estudio este cubierta las 24 horas del día por la cobertura del sistema de red.

El estudio de factibilidad, debe comprender entre otros aspectos: el análisis físico y lógico de la red, sus perspectivas económicas y financieras, como también la seguridad en el acceso al sistema de red **WIFI**.

Este proyecto podrá servir de guía y referencia para posibles implementaciones de redes inalámbricas a nivel general del CRUV y otros sitios, ya que, a nivel local, no existen recursos publicados en cuanto al diseño de redes **WIFI**.

Actualmente, a nivel mundial diversas organizaciones educativas han adoptado los sistemas de redes inalámbricas, para cubrir sus necesidades de conexión al sistema de red; un ejemplo es: **Red Inalámbrica: nuevo servicio de Calidad**, de la Universidad de Colima; que propone la incorporación de una red inalámbrica al desarrollo diario de la enseñanza-aprendizaje en su sistema educativo **[BASU04]**.

El estudio antes mencionado, así como otros más, servirán de guía, para la elaboración de este proyecto de investigación, que se orienta a la innovación que surge en reacción de búsquedas de elementos vanguardistas de la actualidad en el ámbito educativo.

1.4 Objetivos.

Este estudio tiene como principios fundamentales, los siguientes objetivos generales y específicos:

1.4.1 OBJETIVO GENERAL.

Determinar la factibilidad de crear una red inalámbrica **WIFI** para el área del Edificio A-B del Centro Regional Universitario de Veraguas.

1.4.2 OBJETIVOS ESPECÍFICOS.

Analizar la situación actual de la red la estructura física y lógica de la red cableada del área del edificio A-B del CRUV.

Evaluar las infraestructuras físicas del edificio A-B del CRUV.

Examinar los estándares existentes de comunicación de datos no guiada, que ofrecen una alternativa factible para la infraestructura del edificio A-B del CRUV.

Diseñar la estructura de la red **WIFI** para el área del edificio A-B del CRUV.

Definir políticas de seguridad, en cuanto al acceso de usuarios, uso de recursos y balance de carga en la red **WIFI**, en el edificio A-B del CRUV.

Realizar pruebas para la evaluación del diseño de la red inalámbrica en el edificio A-B del CRUV.

Redactar un informe técnico que incluya el diseño y los resultados de las pruebas de evaluación de la red **WIFI**.

1.5 Alcance Y Limitaciones.

Dentro de la propuesta, se tiene como objetivo determinar la factibilidad o no de la creación de una red inalámbrica en el área del edificio A-B del Centro Regional Universitario de Veraguas.

Para la realización de este estudio, inicialmente se analizará la infraestructura física y lógica existente del edificio A-B del CRUV. Posteriormente, se propondrá el diseño de los componentes físicos y lógicos del diagrama de red **WIFI**, incluyendo los elementos que componen la red como propuesta a una futura implementación.

Se comprobará el rendimiento y la confiabilidad de la red inalámbrica en cuanto el uso del recurso compartido y balance de la carga, por medio de políticas de seguridad, además se realizarán pruebas de campo, al diseño de red **WIFI**, además se confeccionará un informe técnico del estudio de factibilidad que incluirá, además de los planos de red inalámbricos los equipos, los costos y además se definirá políticas de seguridad en cuanto al acceso a la red de comunicación de datos del usuario al sistema.

CAPÍTULO 2: TECNOLOGÍAS WIFI.

Las tecnologías de la información, en un principio suplían las necesidades que en ese entonces existían, sin tomar en consideración la proliferación de las redes de datos que a nivel mundial se iban creando, desde ese entonces hasta la actualidad, se han desarrollado diferentes tipos de tecnologías en la comunicación de datos, ya sean en las redes guiadas y no guiadas, ejemplo: en el campo de las redes no guiadas, se habla de las redes **WIFI**. A continuación se detallan sus inicios y el papel que juegan actualmente.

2.1 Antecedentes.

El incremento de tecnologías inalámbricas, condujo a que compañías como Symbol Technologies y Nokia, crearon en 1999 una asociación denominada **WECA**. Esta asociación pasó a denominarse WIFI Alliance en 2003. Su objetivo principal fue: “crear una marca que permitiera fomentar fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos que utilizaran está tecnología” **[CISC05]**.

En abril de 2000, **WECA**, certifica la interoperatibilidad, de equipos según la norma **IEEE 802.11**. Como consecuencia, a partir de ese año, esta organización garantiza que todos los equipos que tengan la marca **WIFI**, pueden trabajar en conjunto sin problemas, independientemente del fabricante de cada marca.

La norma **IEEE 802.11**, fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 mejor conocida como norma Ethernet; esto quiere decir, que en lo único que se diferencia una red **WIFI**, de una red Ethernet es en cómo se transmiten los paquetes de datos.

Por lo tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3.

Actualmente, el término **WIFI**, se refiere al: **Estándar de Fiabilidad Inalámbrica [POWO08]**, que señala la compatibilidad entre los dispositivos

inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante como se mencionó anteriormente.

Debido a la facilidad de implementación, que ofrece la tecnología inalámbrica, en aspectos de comunicación, en diferentes ambientes ya sea empresarial, educativa u organizacional, esta tecnología, ha sido considerada como una herramienta que permite una rápida implementación y libertad de movimientos, en el área de acceso a la información por medio de un sistema de red.

Las redes, por medio de cualquier tecnología de comunicación en general, tienen como objetivo compartir recursos, y su meta principal es hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que lo solicite, cuando lo permitan roles y los permisos correspondientes en cuanto al acceso a la información, sin importar la localización física del recurso y del solicitante.

En consecuencia, el factor distancia entre el usuario que solicita un servicio que ofrece la red, no debe evitar que éste los pueda utilizar como si fueran originados localmente.

Por lo tanto, se puede definir, una red inalámbrica como: el sistema con la capacidad de conectar equipos terminales a la red de datos, sin necesidad de utilizar, cables de comunicación para ello; la comunicación inalámbrica a su vez,

la transmisión de datos sin necesidad de utilizar ningún tipo de cableado **[TSVI04].**

Las redes **WIFI**, en el campo de educación han sido empleadas en proyectos de implementación de tecnologías inalámbricas en campus universitarios, alrededor del mundo **[DETE04]**, como el proyecto de: Red Inalámbrica para todos, del Instituto Tecnológico de Costa Rica, con una plataforma inalámbrica para todas las sedes, brindando cobertura total en cada una de ellas.

Otro ejemplo, es la propuesta para la implementación y montaje de la infraestructura para proveer el servicio de acceso de Internet de banda ancha de forma inalámbrica, a través de WISP COM, una compañía dedicada a la prestación de servicios y soluciones integrales de tecnologías en las áreas de sistemas y telecomunicaciones. Las universidades de Andalucía y de Sevilla, han implementado la propuesta, ofrecida por esta empresa.

Se puede mencionar también, el proyecto de la biblioteca de la Universidad de Andalucía, ubicada en España. Fue el primer edificio del campus totalmente inalámbrico. El rotundo éxito de la iniciativa propicio la revisión de la red inalámbrica para eliminar los puntos del edificio en los que no existía cobertura que actualmente, cuenta con una cobertura inalámbrica del 100% de sus instalaciones, al igual que la Universidad Pablo de Sevilla y el Campus de El Carmen**.**

Además, se presenta el caso de la red inalámbrica de la Universidad de Almería, denominada UAL-i, que es una red de datos **WIFI**, proporcionando acceso a Internet y a la red de la Universidad, principalmente al servicio de biblioteca, a cualquier miembro de la UAL, que se encuentre en el Campus. Finalmente, la red inalámbrica de la Universidad Autónoma de Guadalajara (UAG), en México, a través de su Departamento de Telecomunicaciones de Tecnología de Información. Esta red permite la conexión a la red de comunicación de la UAG, sin la necesidad de conectarse físicamente a un nodo a través de cables **[BASU04]**.

Las publicaciones de proyectos de implementación de redes inalámbricas en los campus universitarios antes mencionados, hacen referencias a la situación orientada a la innovación de tecnologías de comunicaciones y se decide ofrecer a los docentes y estudiantes una plataforma que ofrece una serie de ventajas, tales como:

Movilidad.

Posibilidad de acceso a la información en todo momento.

Oportunidad de una nueva forma de enfrentar el proceso de enseñanza - aprendizaje apoyándose en esta tecnología.

Creación de una red fácil de administrar y con amplia posibilidad de crecimiento y 100% del tiempo brindando conectividad.

2.2 Estándares WIFI IEEE.

IEEE 802.11, es un comité y grupo de estudio de estándares perteneciente a **IEEE** (Instituto de Ingenieros, Eléctricos y Electrónicos), que actúa sobre redes de computadores, concretamente y según su propia definición sobre redes de área local y redes de área metropolitana.

El nombre **IEEE 802.11** se utiliza para referirse a los estándares que son muy conocidos: Ethernet, o **WIFI**, incluso está intentando estandarizar Bluetooth en el 802.15 **[POWO08].**

Aunque se pensaba que el término viene de Wireless Fidelity como equivalente a Hi-Fi, High Fidelity, que se usa en la grabación de sonido, realmente la **WECA** contrató a una empresa de publicidad para que le diera un nombre a su estándar, de tal manera que fuera fácil de identificar y recordar. Phil Belanger, miembro fundador de **WIFI** Alliance que apoyó el nombre **WIFI**, y escribió:

> *"WIFI y el "Style logo" del Ying Yang fueron inventados por la agencia Interbrand. Nosotros (WIFI Alliance) contratamos Interbrand para que nos hiciera un logotipo y un nombre que fuera corto, tuviera mercado y fuera fácil de recordar. Necesitábamos algo que fuera algo más llamativo que "IEEE 802.11b de Secuencia Directa". Interbrand creó nombres como "Prozac", "Compaq", "OneWorld", "Imation", por mencionar algunas. Incluso inventaron un nombre para la compañía: VIVATO"* **[WIKI09A]**.

El primer estándar de WIFI, lo genero el organismo **IEEE**, en el año de 1997, se le denomina **IEEE 802.11**, desde entonces muchos organismos

internacionales han desarrollado una amplia actividad de estandarización de normativa Wireless.

Las redes **WIFI**, cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas, pero necesitan una normativa adicional que defina el uso de los recursos radioeléctricos, estas normativas específicas definen de forma detallada los protocolos de la capa física y de la capa de Control de Acceso al Medio, que regulan la conexión vía radio **[TSVI04].**

La denominación **WIFI**, aplica al protocolo inalámbrico IEEE 802.11b, y superiores; significa que vía radio, mantiene la fidelidad las características de un enlace Ethernet cableado, dado que estos protocolos ya están implementados en múltiples productos comerciales.

2.2.1 TOPOLOGÍA DE LAS REDES INALÁMBRICAS Y SUS CARACTERÍSTICAS TÉCNICAS.

Dentro de este tipo de red, existen 2 clases de topología, a saber: la Red Ad-Hoc y la Red en Modo Infraestructura.

Una red Ad-Hoc, consiste en un grupo de computadoras que se comunican cada una directamente con las otras a través de las señales de radios sin usar un punto de acceso.

Las computadoras de la red inalámbrica que requieren comunicarse entre ellas necesitan usar el mismo canal de radio y configurar un identificador específico de **WIFI**, denominado **ESSID** (Identificador de Conjuntos de Servicios Extendidos), en modo Ad-Hoc.

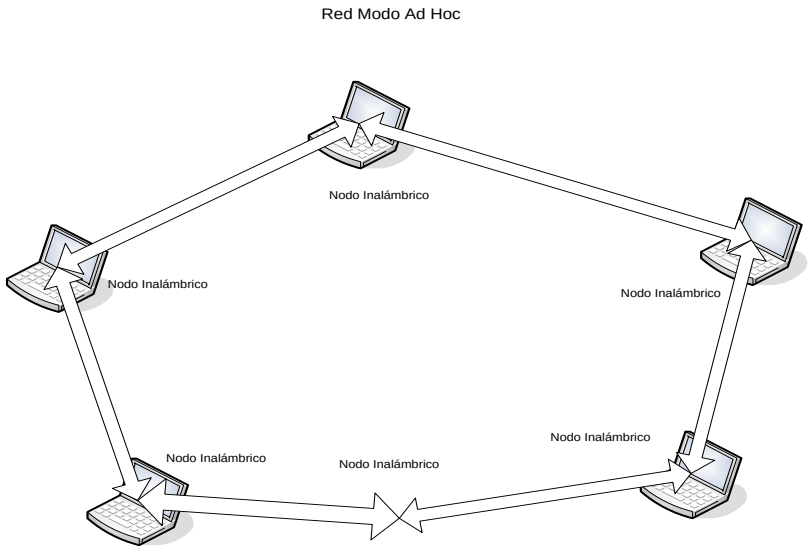

Ilustración 2.1: Red Modo Ad Hoc.
Fuente: [CISYT06]

Se conoce como configuración en Modo Infraestructura, a la forma típica de trabajar cuando se utilizan puntos de acceso. Si deseamos conectar una tarjeta **WIFI**, se debe configurar para accesar a la red en este tipo de conexión y a la vez es el tipo de conexión entre la red **WIFI** y la cableada.

Es más eficaz que la red Ad-Hoc, en la que los paquetes se lanzan al aire, con la esperanza de que lleguen a su destino, mientas que el modo Infraestructura gestiona y se encarga de llevar cada paquete a su sitio mejorando la velocidad.

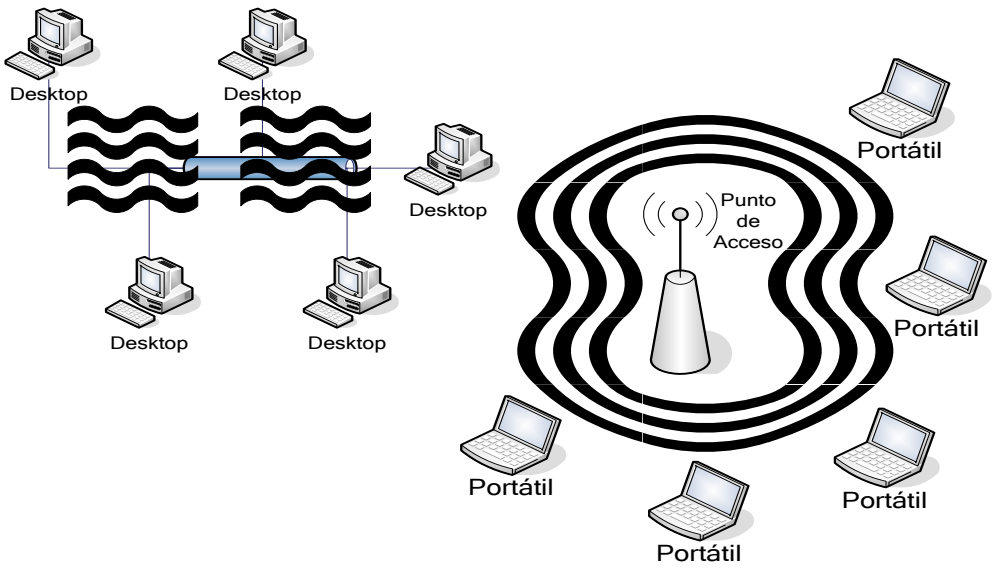

Ilustración 2.2: Red Modo Infraestructura.
Fuente: [CISYT06]

La mayoría de los productos que soportan los protocolos de **IEEE 802.11**, que existen en la actualidad, son de la especificación “b” y de la “g”. El siguiente paso, se dará con la norma **802.11n**, que sube el límite teórico hasta los 600Mbits. Actualmente ya existen varios productos que cumplen un primer borrador del estándar “N” con un máximo de 300Mbits, sin embargo, de manera estable, sólo ofrecen de entre 80Mbits hasta 100Mbits.

La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n), son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En el año 2005, la mayoría de los productos que se comercializaban, respetaban el estándar 802.11g con compatibilidad hacia el 802.11b **[CISYT06]**.

Los estándares 802.11b y 802.11g utilizan bandas de 2,4Ghz, que no necesitan de permisos para su uso. El estándar 802.11, utiliza la banda de 5GHz. El estándar 802.11n, hará uso de ambas bandas 2,4GHz y 5GHz.

Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4Ghz.

2.3 IEEE 802.11, Sus Inicios.

En 1997, la IEEE fijó un estándar para las redes inalámbricas, para normar el desarrollo de este tipo de redes, instauró la norma 802.11, en ese tiempo con un ancho de banda de 1 y 2Mbps.

La norma, en esos momentos, la desarrolló Cisco, Lucent Technologies, 3com y Apple. Por otro lado, Lucent, fue, el principal desarrollador de esta tecnología y represento la empresa que logró que 802.11, sea una norma muy usada en la actualidad, pues los primeros equipos que realmente tenían futuro para su comercialización eran Lucent, aunque en el año 2000, estos equipos eran muy costosos, para ser vendimos masivamente **[CISYT06]**.

Dentro de las características técnicas que existen actualmente en el estándar 802.11, se tienen las siguientes **[WIKI09B]**.

2.3.1 802.11 LEGACY.

La primera versión original del estándar **IEEE 802.11** publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2Mbits utilizando como medio de transmisión a las señales infrarrojas (**IR**), en la banda **ISM** (Industrial, Científico y Médico) a 2,4GHz. **IR** sigue siendo parte del estándar, pero no hay implementaciones disponibles.

La velocidad de transmisión teórica que utiliza esta codificación, logró mejorar la calidad de la transmisión bajo condiciones ambientales variadas, pero implicó dificultades de interoperabilidad entre equipos de diferentes marcas.

Estas debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores **[ROLE03]**.

2.3.2 802.11 B.

La revisión 802.11b del estándar **IEEE**, fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11Mbits y utiliza el mismo método de acceso **CSMA/CA** (Acceso Múltiple por Detección de Portadora con Evasión de Colisiones), definido en la norma original. El estándar 802.11b, funciona en la banda de 2,4GHz. Debido al espacio ocupado por la codificación del protocolo **CSMA/CA**, en la práctica, la velocidad máxima de transmisión con este modelo

de comunicación de datos, es de aproximadamente 5,9Mbit/s sobre **TCP** y 7,1Mbits sobre **UDP**.

Esta tecnología, utiliza una técnica de ensanchado de espectro basada en **DSSS**, pero en realidad, la extensión 802.11b, introduce **CCK** para llegar a velocidades de 5,5 y 11,1Mbits.

Los dispositivos 802.11b, deben mantener la compatibilidad con el anterior equipamiento **DSSS** (Espectro Ensanchado por Secuencia Directa), especificado a la norma original **IEEE 802.11**, con velocidades de bit de 1 y 2Mbits **[ROLE03]**.

2.3.3 802.11A.

En 1997, la **IEEE** crea el Estándar 802.11 con velocidad de transmisión de 2Mbits, además se aprobaron ambos estándares: el 802.11a y el 802.11b en el año de 1999. En el año 2001, aparecieron en el mercado los productos del estándar 802.11a.

La revisión 802.11a del estándar original, fue ratificada en 1999. El estándar 802.11a , utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5Ghz y utiliza 52 subportadoras, **OFDM**, con una velocidad máxima de 54Mbits, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20Mbits.

La velocidad de datos, se reduce a 48, 36, 24, 18, 12, 9 ó 6Mbits en caso necesario. 802.11a, tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto.

No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2,4Ghz tiene gran uso, el utilizar la banda de 5GHz, representa una ventaja del estándar 802.11a, dado que se presentan menos problemas en la comunicación, debido a interferencia de la señal con otros equipos.

Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a, a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso. Esto significa también que los equipos que trabajan con este estándar no poseen mayor cobertura que los del estándar 802.11b, dado que sus ondas son más fácilmente absorbidas por el medio donde se transmiten **[ROLE03]**.

2.3.4 802.11H.

La especificación 802.11h, es una modificación sobre el estándar 802.11, para **WIFI** desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE 802.11 y que se hizo pública en octubre de 2003. 802.11h

intenta resolver algunos de los problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélites.

El desarrollo del 802.11h, sigue las recomendaciones hechas por la **ITU** (Unión Internacional de Telecomunicaciones), que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones, estimó convenientes para minimizar el impacto de abrir la banda de 5GHz, utilizada generalmente por sistemas militares.

802.11h, proporciona a las redes 802.11, la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión: 802.11g.

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución del estándar 802.11b. Este, utiliza la banda de 2,4Ghz pero opera a una velocidad teórica máxima de 54Mbits que, en promedio, es de 22Mbits de velocidad real de transferencia, similar a la del estándar 802.11a y es compatible con el estándar b, ya que utiliza sus mismas frecuencias.

Los equipos que trabajan bajo el estándar 802.11g, llegaron al mercado rápidamente, incluso antes de su ratificación que fue dada aproximada el 20 de junio del 2003.

En la actualidad, se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite establecer un enlace de

comunicación a distancias de hasta 50km, con antenas parabólicas apropiadas **[ROLE03]**.

2.3.5 802.11N.

En enero de 2004, el **IEEE** anunció la formación de un nuevo grupo de trabajo 802.11, para desarrollar otra revisión de este mismo estándar 802.11. Esta nueva norma se debería ajustar, entre otras, a las especificaciones que se enuncian a continuación:

La velocidad real de transmisión, podría llegar a los 600Mbits y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b.

También se espera, que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

A diferencia de las otras versiones de **WIFI**, 802.11n puede trabajar en dos bandas de frecuencias: 2,4GHz, la que emplean 802.11b y 802.11g y 5GHz.

Por lo tanto 802.11n, es compatible con dispositivos basados en todas las ediciones anteriores de **WIFI**.

Existen también otras propuestas, que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008 **[ROLE03]**.

2.3.6 802.11E.

El nuevo estándar 802.11e, tiene como objetivo introducir nuevos mecanismos a nivel de capa **MAC**, para soportar los servicios que requieren garantías de Calidad de Servicio.

Para cumplir con su objetivo, IEEE 802.11e introduce un nuevo elemento llamado Función de coordinación híbrida, con dos tipos de acceso: **EDCA** (Sistema distribuido de control) y **HCCA** (Acceso Hibrido al Canal Controlado) , de este modo se logra incorporar mecanismos de autentificación, para así dotar a la tecnología de mejoras de proveer calidad requerida por los servicios de telefonía IP y video **[UACH03].**

De este modo, la tecnología **IEEE 802.11**, ofrece soporte para tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de **MIMO** (Múltiples entradas Múltiples Salidas), proporcionado por el 802.11e **[ROLE03].**

2.3.7 802.11I.

Tiene como propósito, subsanar la vulnerabilidad actual, en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.11x, **TKIP** (Protocolos de Identidad de Llaves Temporales) y **AES** (Estándar de Encriptación Avanzada). 802.11i, también presentó los protocolos de encriptación

802.11i, utiliza tanto el protocolo de autenticación extendible, como el de extremo a extremo para el transporte. Entre los métodos de autenticación inalámbrica **NIC** y el 802.11i utiliza 802.X para encapsular los mensajes durante inalámbrica Ethernet **[ROLE03]**.

2.3.8 802.11W.

TGw, está trabajando en mejorar la capa del control de acceso del medio de **IEEE 802.11**, para aumentar la seguridad de los protocolos de autenticación y codificación **[IEEE09]**. Actualmente, las LANs inalámbricas envían la información del sistema en tramas desprotegidos, que las hace vulnerables a intersección de terceros mal intencionados.

El objetivo de 802.11w, es aumentar la seguridad al proporcionar confidencialidad de los datos de los marcos de gestión, como también a los mecanismos que permiten a los datos de integridad, la autenticidad de los datos

de origen, protección y reproducción **[GATM02]**. Estas extensiones tendrán interacciones con los estándares futuros IEEE 802.11r y IEEE 802.11u.

Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos, que crean peticiones desasociadas que parecen ser enviadas por el equipo válido **[ROLE03]**.

2.4 Seguridad WIFI.

En las redes inalámbricas, los paquetes de información viajan en forma de ondas de radio. Dichas ondas pueden viajar más allá de las paredes y filtrarse en casas, oficinas adyacentes o ser accesibles en cualquier entorno abierto, dentro de un radio de alcance determinado.

Entre los atributos que una red **WIFI**, debe contemplar se encuentran: confiabilidad, autenticación, integridad, disponibilidad **[ROLE03]**.

Los fundamentos de **WIFI**, que hacen de esta tecnología de punta, también hacen que sea un desafío en términos de seguridad. El tipo de red de área local, se basa en los fundamentos de cable, especialmente en términos de confidencialidad y control de acceso.

En el mundo interconectado, los cables de comunicación ofrecen protección, ya que se tienen que conectar a una toma física para comunicarse.

En el mundo inalámbrico las señales están en el aire, expuestas a todo. Además, las señales inalámbricas cruzar los límites físicos de una organización.

En las redes inalámbricas, es importante que se presenten los atributos de confiabilidad, basadas en sistemas de cifrado y de control de acceso, utilizando mecanismos de autenticación **[CISC05].**

El protocolo 802.11, implementa encriptación **WEP**, pero no se puede mantener **WEP** como única estrategia de seguridad ya que no es del todo segura. Existen aplicaciones para Linux y Windows, como AiroPeek, AirSnort, AirMagnet o WEPCrack, que, escaneando el suficiente número de paquetes de información de una red **WIFI**, son capaces de obtener las claves utilizadas y permitir el acceso de intrusos a la red.

Uno de los atributos, que ostentan los sistemas seguros, es: “asegurar correctamente un punto de acceso” **[XOMB07]**, es decir, cortar el paso desde el exterior a nuestra red a personas que no tienen el permiso de entrar.

En consecuencia, es necesario tomar en cuenta una serie de estrategias que, en su conjunto pueden mantener la red oculta con una serie de medidas de seguridad, para ello, es necesario tener en cuenta los siguientes aspectos:

Confiabilidad: se refiere a la capacidad para enviar y recibir datos, sin que ellos se divulguen a entidades no autorizadas, durante su transmisión. Dentro de los mecanismos que existen se encuentran: Encriptación simétrica y asimétrica.

Integridad: es la capacidad para enviar y recibir datos, tales que las entidades no autorizadas, no puedan alterarlos sin que el transmisor-receptor, detecte el cambio.

Disponibilidad: se define, como la capacidad para recibir y enviar datos. Dentro de los mecanismos de la disponibilidad están los sistemas de defensa que detectan varias formas de ataques del DOS y se protegen contra ellos.

Autentificación: establece, la identidad del remitente o del receptor de la información. Está basada en niveles y protocolos múltiples tales como 802.1x, RADIO, PAP/CHAP, MS-CHAP, entre otros.

Autorización: la autorización se relaciona directamente con la autentificación, en la mayoría de los requisitos del acceso del recurso de red. La autorización establece lo que se permite hacer después de que usted se ha identificado.

Control de acceso: se define, como la capacidad para controlar el acceso de entidades a los recursos basados, de acuerdo a propiedades diversas, tales como: atributos, autentificación, o políticas, entre otros casos. El fundamento de este mecanismo es el punto de acceso, basado en la autentificación o el conocimiento de la llave **WEP** (Privacidad Equivalente a Cableado).

Encriptación: es la capacidad para transformar datos, en octetos sin sentido, por ejemplo el: texto cifrado, basados en un cierto algoritmo. El descifrar, es el acto de dar vuelta los octetos sin sentido a los datos significativos.

Gestión de claves: Una llave, es un código digital que se puede utilizar para cifrar o para descifrar. Algunas llaves se mantienen privadas, y otras se comparten y se deben distribuir de una manera segura. La gestión de claves se refiere al proceso de distribuir las llaves para los procesos mencionados **[CISC05]**.

2.5 Consideraciones Relevantes De Seguridad En WIFI.

Algunas consideraciones que se deben tomar al brindar seguridad a una red WIFI, entre otras, son:

2.5.1 CERRAR EL ACCESO NO AUTORIZADO AL PUNTO DE ACCESO.

Este método, consiste en colocar la antena de manera que limite su alcance, exclusivamente, al área que se desea ofrecer cobertura inalámbrica específicamente. Nunca hay que colocar dicho dispositivo cerca de una ventana ya que el cristal no bloquea la señal **[GATM02].**

Un esquema ideal, sería colocar la antena en el centro del área, dejando que sólo, una leve señal escape a través de los muros o ventanas de la oficina o lugar de trabajo.

Además, se puede configurar el punto de acceso inalámbrico o enrutador de manera que no transmita su **ESSID**. La mayoría de los puntos de acceso están prefijados para enviar un anuncio corto cada varios segundos a cualquier computadora que esté dentro de su alcance. Dentro de las especificaciones del **ESSID**, es el nombre previamente asignado a la red inalámbrica.

2.5.2 CIFRADO WEP.

WEP, es una encriptación estándar, utilizada para cifrar el tráfico a través de una red inalámbrica. Muchos vendedores de puntos de acceso inalámbricos, incorporan este protocolo de encriptación deshabilitado por defecto para permitir una instalación más sencilla.

Con esto, lo único que se consigue en realidad es empobrecer la seguridad de nuestra **WIFI**, ya que los datos que circulen por la Wirelees pueden ser leídos directamente con un Sniffer **WIFI**.

WEP, usa el algoritmo de cifrado **RC4**, para la confidencialidad mientras que el CRC-32, proporciona la integridad. El **RC4**, funciona expandiendo una semilla para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números se unifica con el mensaje mediante una operación puerta lógica para obtener un mensaje cifrado.

El estándar **WEP**, de 64bits usa una llave de 40bits, es enlazado con un vector de iniciación de 24bits para formar la clave de tráfico **RC4** (Código de

Ron). Al tiempo que el estándar **WEP** original, estaba siendo diseñado, llegaron de parte del gobierno de los Estados Unidos, una serie de restricciones en torno a la tecnología criptográfica, limitando el tamaño de clave.

Un sistema **WEP** de 256bits, está disponible para algunos desarrolladores, y como en el sistema anterior, 24bits de la clave pertenecen al cuarto bloque, dejando 232bits para la protección.

El principio del funcionamiento de **WEP**, está en la operación lógica **XOR** (O exclusiva). La operación **XOR**, es un tipo de disyunción lógica entre dos operandos, que resulta en un valor verdadero, o uno si y solo si uno de esos dos operando equivale a uno.

Esta operación presenta la propiedad, que si aplicamos dos veces **XOR** a un valor, se vuelve a obtener el valor original. Por ejemplo, teniendo un valor “A” y calculando “A” **XOR** B = C, tendremos entonces que A **XOR** B **XOR** B será igual a “A” **[CISC05].**

Si dos nodos de una red inalámbrica, conocen un valor “B” secreto y se quiere transmitir una secuencia de bits “A”, aplicar la operación A **XOR** B obteniendo un flujo de datos “C” encriptado, el cual solo puede ser decodificado por aquellos que conocen el valor de “B”.

En este sentido, es posible ver a “B” como una contraseña secreta que deben conocer y compartir todos los nodos que quieran intercambiar mensajes de manera segura entre sí **[ROLE03]**.

2.5.3 CIFRADO WPA.

Luego del deceso del **WEP**, en 2003 se propone el **WPA** (Acceso Protegido WIFI) y luego queda certificado por parte del estándar 802.11, con el nombre de **WPA**, existen dos cambios entre **WPA** y **WPA2** (WPA de segunda generación):

- El reemplazo del algoritmo Michael por un código de autenticación, **CCMP** que es considerado seguro.

- El reemplazo del algoritmo **RC4 [GATM02].**

Prácticamente, todos los dispositivos **WIFI** soportan como mínimo **WPA**, mucho más potente y seguro que **WEP**. Es altamente recomendable activarlo y configurarlo en los equipos.

WPA, es una versión, del protocolo 802.11i que depende de protocolos de autenticación y de un algoritmo de cifrado cerrado: **TKIP**, que genera claves aleatorias y, para lograr mayor seguridad, puede alterar varias veces por segundo una clave de cifrado.

El funcionamiento de **WPA**, se basa en la implementación de un servidor de autenticación que identifica a los usuarios en una red y establece sus privilegios de acceso. No obstante, las redes pequeñas pueden usar una versión más simple de **WPA**, llamada WPA-PSK, al implementar la misma clave de cifrado en todos los dispositivos, con lo cual ya no se necesita el servidor **RADIUS**.

El **WPA**, en su primera versión, sólo admite redes en modo infraestructura, es decir que no se puede utilizar para asegurar redes punto a punto en modo "ad-hoc" **[CISC05].**

2.5.4 CAMBIAR EL SSID Y DESHABILITAR EL BROADCAST.

El Service Set Identifier (**SSID**), es la cadena de identificación usada por los clientes de un punto de acceso, para ser capaces de iniciar una conexión.

Este identificador, viene predefinido por el fabricante y cada uno viene con una cadena por defecto, por ejemplo los 3Com vienen con "101" y en DLINK "Default".

La detección de la difusión de la **SSID**, no impedirá que una persona interesada encuentre la **SSID** de la red. Configurando la red como cerrada, solo añadirá una barrera adicional a un intruso corriente. Detener la difusión de **SSID**

debe considerarse como una precaución adicional, más que una medida de seguridad **[GATM02].**

Por cada punto de acceso, que se instale se debe seleccionar un **SSID** complicado y si es posible suprimir el envío por Broadcast de este id a través de nuestra antena.

Desactivar el broadcasting **SSID**, es uno de los métodos más básicos de proteger una red inalámbrica, ya que para el usuario medio no aparecerá como una red en uso.

2.5.5 DESHABILITAR EL SERVICIO DHCP.

Mediante este paso un intruso puede descifrar nuestra dirección IP, máscara de subred, y otros parámetros TCP/IP relevantes y con los cuales podría obtener acceso a la red **WIFI**.

El servidor **DHCP** (Protocolo Configuración Dinámica de Servidor), integrado en el enrutador distribuye las direcciones IP siempre a cada PC. Por lo tanto, otro método para detener a los intrusos es limitar el número de direcciones IP al número de ordenadores que se tiene.

Cuando se decide mantener activado el **DHCP**, restringiendo el rango de direcciones que asigna, no es necesario modificar los valores "Start IP Address", en donde se debe introducir la primera dirección que debe asignar el servidor, y

"End IP Address", en donde se debe indicar dónde termina el conjunto de direcciones que puede asignar el **Router**.

Para terminar, se puede especificar el tiempo de duración de la asignación en Leased Time, el tiempo durante el cual una dirección pertenecerá a un cliente, pasado el cuál podría ser asignada a otra.

Para desactivar el servidor **DHCP** y configurar todas las direcciones de los dispositivos manualmente, se selecciona la casilla "Disable DHCP Server", de este modo se evita que el **Router**, conceda a un equipo externo los datos de conexión de la red **WIFI**, pasando a formar parte de ella.

En consecuencia, esto implica que se debe introducir la dirección IP, la puerta de enlace y los **DNS** manualmente **[CISC05].**

2.5.6 DESHABILITAR O MODIFICAR LA CONFIGURACIÓN SNMP.

El Protocolo Simple de Administración de Red **(SNMP)**, facilita el intercambio de información de administración entre dispositivos de red.

Es parte de la familia de protocolos **TCP/IP**. **SNMP**, permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de **SNMP**, más utilizadas son dos: **SNMP** versión 1 (SNMPv1) y **SNMP** versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como por ejemplo, operaciones adicionales.

SNMP, en su última versión posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Un dispositivo administrado, es un nodo de red que contiene un agente **SNMP** y reside en una red administrada. Estos recogen y almacenan información de administración, que es puesta a disposición de los **SNMP**.

Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente, es un módulo de software de administración de red que reside en un dispositivo administrado. Este, posee un conocimiento local de información de administración: memoria libre, número de paquetes **IP** recibidos, rutas, etcétera; la cual es traducida a un formato compatible con **SNMP** y organizada en jerarquías.

Por lo tanto, si el punto de acceso soporta **SNMP**, se debe deshabilitar o cambiar tanto la cadena privada como la pública, permitiendo la administración

total de la red inalámbrica para brindar así la libertad de posibles modificaciones o configuración a libre criterio **[CISC05].**

2.5.7 LISTAS DE CONTROL DE ACCESO.

Para un control más efectivo de la red **WIFI**, es interesante el uso de **ACL** (Lista de Control de Acesso). Cuando incorporan este servicio normalmente utilizan el protocolo **TFTP**, para periódicamente descargar actualizaciones de dichas listas para facilitar las tareas administrativas y no tener que configurar las listas de acceso en cada punto de acceso.

Se incluyen unos 25 tipos de permisos diferentes para permitir o denegar operaciones, como por ejemplo: protecciones, desprotecciones, fusiones, aplicación de etiquetas, creación de repositorios o espacios de trabajo, etc.

En consecuencia, al determinar las prioridades de cada solicitud al sistema de red **WIFI**, se podrá permitir el acceso restringido a los servicios red**[GATM02].**

2.5.8 LA ANTENA DEL REPETIDOR DEBE DE ESTAR A LA ALTURA DEL TECHO.

Cuando la antena, es colocada en un lugar apropiado, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

La diferencia, entre el techo y la mesa para algunas de las antenas, puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción.

En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si. **[GATM02]**.

2.5.9 CAMBIAR FRECUENTEMENTE LAS CONTRASEÑAS.

Un producto de fábrica viene con un perfil y una contraseña estándar, a fin de facilitar el acceso a su configuración inicial.

Estos datos son conocidos y están publicados en multitud de páginas webs y foros, por consiguiente, es fácil encontrar en Internet listados en los que figuran los nombres de usuarios y contraseñas empleadas por los fabricantes en cada modelo de **Router**.

Para obtener una contraseña razonablemente segura se puede:

Intercalar mayúsculas, minúsculas y números.

No introducir una secuencia de teclas correlativas como puede ser "abcdef", "45678".

También el **Router** se necesita una contraseña para acceder a sus herramientas de configuración. Cuando se accede al panel de administración del **Router** (que es probable 192.168.1.1) él debe solicitar un nombre de usuario y contraseña. Usualmente, el nombre de usuario aparece en blanco, o es “admin”, y típicamente no se puede modificar.

La contraseña por defecto suele ser 'admin' o 'password', dependiendo del fabricante **[XOMB07].** Es fundamental cambiar las contraseñas por algo único, preferiblemente una combinación de letras y números, con al menos seis caracteres. Este paso, por si solo, no es suficiente para brindar un nivel de protección efectivo.

2.5.10 NO UTILIZACIÓN DE LA MÁXIMA POTENCIA DEL AP.

Se debe utilizar únicamente la potencia necesaria: con potencias altas se tiene más, posibilidades de que la señal salga a la calle más lejos y por tanto, ampliar el radio desde el que un posible atacante podría utilizar sin autorización, a la conexión **[XOMB07].**

2.5.11 UTILIZAR UN FIREWALL.

Considerando que un atacante consiga entrar a una red inalámbrica, se puede configurar un firewall en un ordenador, así como utilizar las cuentas de usuario y los permisos en las carpetas **[XOMB07].**

Las redes inalámbricas que utilizan un firewall, también poseen un sistema de seguridad confiable, a la hora de controlar estadísticas de usuarios que intentaron conectarse y no lo consiguieron, así como el tráfico que atravesó la misma.

Un cortafuego activo, como también se le conoce a los firewalls ya sea hardware o software, desde la puerta de enlace o los ordenadores individuales que controla los datos que entran y salen de un ordenador. Adicionalmente, examinan los datos y bloquean bits determinados, a veces lanzando una advertencia, si los datos coinciden con ciertos criterios.

Dentro de una red, utilizar un cortafuego para que los servicios de entrada y salida necesarios estén abiertos sólo para los ordenadores locales es una buena forma de desalentar a los intrusos de intentar provocar estragos **[GATM02].**

En un cortafuego activo, se puede elegir permitir el paso a sólo ciertos protocolos, así como sólo conexiones que utilizan números de puerto concretos o sólo usuarios específicos.

2.6 Aspectos Relevantes Del Diseño De Redes WIFI.

Las nuevas redes sin cables, hacen posible que se pueda conectar a una red local, cualquier dispositivo sin necesidad de limitantes de conexión a cables, lo que permite, pasear libremente por la oficina con un computador portátil conectado a la red.

También, es posible instalar la red **WIFI** en locales públicos y dar el servicio de acceso a Internet sin cables o impedir el acceso de intrusos. Y todo ello de una forma significativamente segura, cumpliendo con la normativa más estricta y asegurando la confidencialidad.

Por ello, para lograr estas metas, es necesario considerar 4 elementos claves, a saber: alta disponibilidad, escabilidad, manejabilidad, interoperabilidad **[CISC05]**.

Dentro, de los requisitos que se debe tener en cuenta para obtener impedir el acceso a agentes no autorizados, logrando elementos claves en cuento: estabilidad, manejabilidad, interoperabilidad y alta disponibilidad, dentro de estos están los siguientes **[CISC05]**:

2.6.1 APLICACIONES Y RECOPILACIÓN DE DATOS.

Se debe tomar en cuenta las aplicaciones que los usuarios de la red **WIFI**, utilicen, es decir, un usuario puede solicitar acceder su correo y otro puede utilizar una aplicación compleja como, el acceso a un servidor, como también algunos usuarios pueden requerir mayor ancho de banda, esto requiere una conexión confiable a la red, porque una interrupción en el sistema de acceso puede ocasionar que la información del usuario sea vulnerable ya sea a alteraciones o robo, entre otros casos **[CISC05].**

2.6.2 CARGA Y COBERTURA.

Es importante determinar el rendimiento, que necesitarán los usuarios de la red inalámbrica. Existirán zonas de cobertura y cada una a velocidad de transmisión de datos específica, es necesario determinar donde estará el pool de la cobertura para cada velocidad.

Por lo tanto, se debe averiguar el rendimiento que necesitarán los usuarios para determinar la ubicación de los puntos de acceso. Hay que destacar que, en muchos casos, es más importante la cobertura de los puntos de acceso que el ancho de banda, por lo que hay que recurrir a la negociación de automática de la velocidad de ancho de banda **[CISC05].**

2.6.3 ANCHO DE BANDA Y RENDIMIENTO.

La unidad central tiene que servir, a la unidad remota más lenta que exista en la red inalámbrica, por lo tanto, hay que considerar:

Si todos los dispositivos operan a la misma velocidad de transmisión de datos, todos invierten el mismo tiempo en enviar paquetes del mismo tamaño.

Si algunos dispositivos están operando a velocidades más altas, el paquete se transfiere más rápidamente. Esto permite que la quede disponible antes para el siguiente dispositivo que esté operando a enviar algunos datos.

Si se hace un intento de reducir el rendimiento de **RF** a un sitio dado bajando la velocidad del puente, esto también afecta a los puentes de alta velocidad **[CISC05]**.

La ilustración que se presenta a continuación, expone los puntos de vista, planteados previamente.

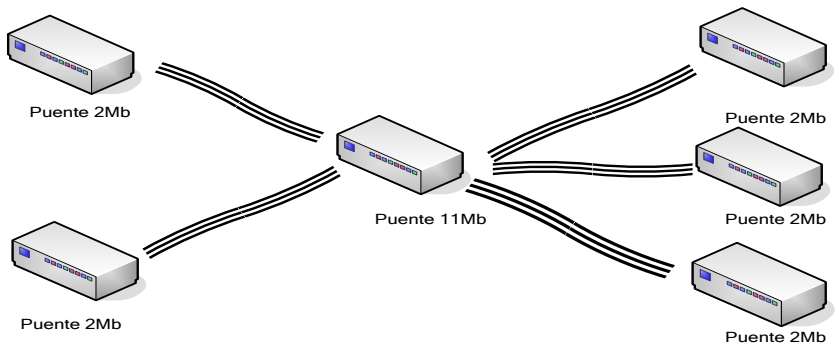

Ilustración 2.3: Distribución Del Ancho de Banda Entre Puentes.
Fuente: [CISC05]

2.6.4 UBICACIÓN DE LOS PUNTOS DE ACCESO.

Es el punto de interconexión de una red inalámbrica con una red de cable, se pueden disponer diferentes **PA**, en una misma red, configurándolos individualmente como subredes, para permitir el desplazamiento físico de uno a otro sin perder la conexión.

La infraestructura de un **PA**, es simple: guardar y repetir, es decir, son dispositivos que validan y retransmiten los mensajes recibidos. Estos elementos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones.

Entre otras, sus características principales son:

La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

Un **PA** compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes **PA** para la retransmisión.

Al respecto sobre la calidad de señal que se dispone en una zona de cobertura **WIFI**, esta viene determinada por la relación entre la potencia de la

señal recibida y el nivel de ruido existente, incluyendo posibles señales interferentes.

Por otro lado, dicha área de cobertura varía considerablemente según el entorno en que se encuentre ubicado dicho **PA**, por lo que no es posible extrapolar resultados obtenidos en un entorno abierto, hacia un entorno cerrado o semicerrado de oficinas.

De este modo, en un entorno de oficinas con paredes y muros de hormigón armado, el área de cobertura se reduce considerablemente, en comparación con un entorno de oficinas donde las separaciones entre despachos estén realizadas a base de ladrillos, madera o vidrio.

Sin embargo, dicha desventaja puede convertirse en un aliado cuando se desea limitar el área de cobertura a un determinado recinto por ejemplo por motivos de seguridad o bien para preservar el ancho de banda disponible.

Hay que tener en cuenta que dicho punto de acceso inalámbrico debe conectarse a un punto de red inalámbrica así como a una toma de red eléctrica lo que limita a veces la ubicación de dicho punto.

En este sentido, la proyección de la señal eléctrica a través de los pares libres del cableado **UTP**, han supuesto un significativo avance.

El entorno adecuado para los usuarios móviles debe contar con las siguientes consideraciones:

Todos los **PA**, de la misma subred: utilice el etiquetado **VLAN** para extender los **Switches**.

Por otro lado, en Modo repetidor: el **PA**, extiende la distancia de otro **PA**; o el **PA**, cableado es el punto de conexión asociado **[CISC05].**

2.6.5 CONSUMO DE ENERGÍA

Como la energía es limitada, el consumo de energía al utilizar tarjetas **PCMCIA**, **Mini-PCI** o **Card-Bus**, siempre es un problema durante la itineracia. Dentro de los modos de energía existen:

Constant Awake Mode(CAM): es el modo predeterminado para cuando la energía no es un problema. Proporciona una alta disponibilidad, como cuando hay energía AC para el dispositivo. Este modo ofrece mejor calidad y por tanto la perspectiva del cliente

Max Power Save Mode (Max PSP): en este modo el **PA** almacena los mensajes entrantes destinados al adaptador cliente, que se reactiva periódicamente y sondea el **PA** para ver si tienes mensajes esperándote**.**

Fast Power Save Mode (Fast PSP): este modo conmuta entre el modo Max PSP, y el modo CAM, en función del tráfico de la red. Este modo conmuta a

CAM cuando se va a recuperar una gran cantidad de paquetes y cambia de nuevo a PSP una vez recuperados los paquetes **[CISC05]**.

2.6.6 ASIGNACIÓN DE CANALES DE RADIO.

El número de canales disponibles de ser usados para dar servicio **WIFI** según el estándar 802.11b varia entre países. Por ejemplo: en España, a la fecha, se pueden utilizar hasta 13 canales los mismos que en toda la comunidad europea.

Sin embargo, el número de canales disponibles en Estados Unidos son 11. Es por ello que sólo permiten trabajar con 11 **FCC** y no con 13 de **ETSI**.

El estándar 802.11b, sólo se dispone de hasta 3 canales para trabajar simultáneamente, sin solapamiento, es posible llegar a utilizar hasta 4 con un análisis de cobertura de forma que la interferencia entre ellos sea pequeña.

Los estándares 802.11b y 802.11g, utilizan la banda de 2.4 – 2.5Ghz. En esta banda, se definieron 11 canales utilizables por equipos **WIFI**, los que pueden configurarse de acuerdo a necesidades particulares. Sin embargo, los 11 canales no son completamente independientes (canales contiguos se superponen y se producen interferencias) y en la práctica sólo se pueden utilizar 3 canales en forma simultánea (1, 6 y 11).

Esto es correcto para los Estados Unidos y muchos países de América Latina, pues en Europa, el **ETSI** ha definido 13 canales, como se mencionó anteriormente. En este caso, por ejemplo en España, se pueden utilizar 4 canales no-adyacentes (1, 5, 9 y 13). Esta asignación de canales usualmente se hace sólo en el Punto de Acceso, pues los “clientes” automáticamente detectan el canal, salvo en los casos en que se forma una red ad hoc o punto a punto cuando no existe Punto de acceso.

Cuando se trabaja con 3 canales radio, los 3 canales sin solapamiento utilizados son el 1-6-11, 3Mhz libres entre canales, mientras que en Europa es posible utilizar hasta 4 siendo estos el 1-5-9-13. El hecho de poder trabajar con 4 canales en lugar de 3 nos facilita la planificación de canales radio en instalaciones con varios puntos de acceso inalámbricos.

2.6.7 COBERTURA DE RADIO.

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio.

Entre dos antenas iguales, el rango de una antena alta es 2x-4x, más que las bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si.

Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre los 0° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su alcance se podrá incrementar de 1 a 4 en su cobertura cuadral.

El patrón horizontal se puede incrementar de 1 hasta 24 dependiendo del medio en que se propague la onda. En una estación, con antena no dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10dB en la recepción de transmisión de una estación sobre otra estación.

Estos 10dB son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estación-a-estación.

CAPÍTULO 3: MARCO METODOLÓGICO.

En este capítulo se establece la Metodología de la Investigación del estudio de factibilidad, dentro de sus aspectos, se tratan: el diseño de investigación y el tipo de investigación en el cual se fundamenta este proyecto.

3.1 Diseño De Investigación.

Tomando en cuenta, los enfoques, en que se basa el desarrollo del estudio de factibilidad, el tipo de investigación está dentro de la categoría del

modelo de tipo no experimental, y a su vez, en el diseño Transeccional descriptiva ya que se recolectan los datos en un sólo momento **[SAMP05]**. En este estudio en particular, se realizan las pruebas de campo del diseño de la red **WIFI**, teniendo en cuenta el modelo lógico de la red, para luego probar este esquema mediante ensayos sobre él.

Los estudios transeccionales tienen como fin el indagar la incidencia y los valores en que se manifiesta una o más variables **[SAMP05]**, en este estudio la factibilidad se pretende determinar, la factibilidad o no de creación de una red inalámbrica en el Edificio A-B del Centro, con el fin de diseñar un estudio técnico del proyecto.

Este tipo de diseño, permite determinar una visión no experimental-descriptiva, y se encuentran caracterizados, por este tipo y el diseño de investigación. Este tipo de investigación se plantea de dos formas: Transeccional y Longitudinal.

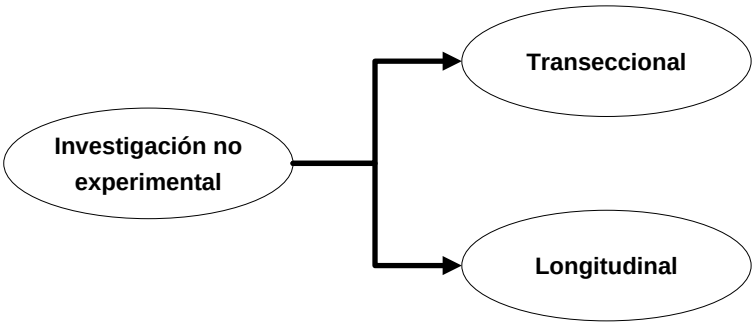

Ilustración 3.1: Diseño De La Investigación.
Fuente: [SAMP05].

3.2 Tipo De Investigación

El tipo de investigación está basado en la Metodología de Exploración Científica de Tipo Transeccional Descriptiva, puesto que:

> *"Se utilizan en investigaciones con objetivos de tipo exploratorio o descriptivo para el análisis de la interacción de las variables en un tiempo específico, como se ajusta al tipo de desarrollo de la investigación..."* **[SAMP05]**.

El autor indica que este tipo de investigación, utiliza los métodos cualitativos para presentar los resultados de los análisis correspondientes al estudio realizado. En el tipo y diseño de esta investigación, Transeccional descriptiva, se utilizan elementos en donde se cuenta ya sea de un objeto en particular y por ende, su descripción **[SAMP05].**

En el caso de este estudio en particular, se brinda el panorama de creación de la red **WIFI**, mostrando desde la justificación de creación del proyecto hasta si resulta factible o no, por lo tanto son estudios puramente descriptivos. Las características de la categoría No-Experimental se puede apreciar en el cuadro que se muestra a continuación.

ESTUDIO	HIPÓTESIS	DISEÑO
Exploratoria y Descriptiva.	No se establecen, lo que se puede formular son conjeturas iniciales, Descriptivas.	Transeccional descriptiva-Pre experimental.

Cuadro 3.1: Categoría No-Experimental.
Fuente: [SAMP05]

Para este tipo de investigación, existen dos tipos de diseños:

Diseños Transeccionales Descriptivos

Diseños Longitudinales

En donde, se hace referencia los tres tipos de estilos del diseño Transeccional descriptivo: Exploratorio, Descriptivos, y Correlacionales casuales **[SAMP05]**. Para el desarrollo de este estudio de factibilidad, se toma en cuenta, el diseño Transeccional Descriptivo, por tener cualidad de determinar por medio de pruebas de diseño de la red la incidencia de este estudio.

Como señala Kerlinger, citado por Sampieri:

> *"En la investigación no experimental no es posible manejar las variables o asignar aleatoriamente a los participantes o tratamientos"* **[SAMP05].**

La investigación de tipo no experimental, se refiere a un estudio donde no se hace variar en forma intencional las variables independientes. Lo que se hace es observar un fenómeno simplemente **[SAMP05].** En el caso particular de esta investigación, se presenta este tipo de investigación al realizar las pruebas del diseño lógico de la red **WIFI**, tal y como se dan en su contexto natural, para después analizarlas, buscando, establecer las propiedades y características, del escenario estudiado.

CAPÍTULO 4: DISEÑO DE LA RED INALÁMBRICA (WIFI).

En la preparación del modelo de la Red Inalámbrica, para el Edificio A-B del Centro Regional Universitario de Veraguas, se realizaron pruebas de campo, con varios modelos de puntos de acceso. Los resultados obtenidos en dichas pruebas se exponen en las tablas de comparación de Distancia Versus Alcance que se exponen posteriormente en este capítulo.

Los diseños se basan en las características físicas del Edificio, ya que en la intensidad de la señal de la red inalámbrica, influye la estructura del edificio, así como el grosor de sus paredes con respecto a ubicación de los puntos de acceso (**PA**) y de estación (portátiles), con los que se midió la magnitud de dicha señal.

A continuación, se presentan los diseños de las plantas arquitectónicas del edificio A-B, del CRUV:

Ilustración 4.1: Diseño De La Planta A Del Edificio
Fuente: La Autora

Ilustración 4.2: Diseño De La Planta B Del Edificio
Fuente: La Autora

4.1 Pruebas de Cobertura.

Para determinar el diseño de la Red Inalámbrica para el Edificio A-B del CRUV, se realizaron varias pruebas de cobertura, utilizando dos modelos diferentes de **PA**.

Dichas pruebas consistieron en la realización de varios recorridos en todo el Edificio, con el **PA** funcionando y dotando de acceso a la red inalámbrica a todo el Edificio, para así determinar la intensidad de señal captada, al ubicar el equipo portátil en puntos estratégicos y medir la señal recibida.

4.1.1 DISEÑO FÍSICO DE RED WIFI.

En el diseño de la red inalámbrica, se realizaron pruebas técnicas de cobertura, conocidas como: walking driving, en donde se utilizaron 2 **PA**, que tienen las características se exponen a continuación:

CARACTERÍSTICAS TÉCNICAS	Router Nexxt	Router Dlink
Opera con estándares IEEE 802.11b/g (LAN) inalámbrica de 2.4 GHz	*	*
Capaz de trabajar hasta 128 bit WEP, WPA, WPA2	*	*
Un puerto WAN de auto-reconocimiento de 10/100M	*	*
Interruptor de ethernet rápida de 4 puertos 100 Base -TX, iincorporado	*	*
Clientes PPPoE, DHCP e IP estático	*	*
Acepta UPnP	*	*
Hasta 54Mbps de velocidad de trasferencia de datos	*	*
Compatible con dispositivos que operen en 802.11b/g	*	*
Cantidad de Antenas	1	3
Switch de 4 puertos para incorporar a red dispositivos cableados	*	*
Firewall avanzado & Seguridad		*
Soporta VPN Passthrough	*	*
Soporta encriptación WPA (TKIP) y WPA2 (AES)	*	*
Asistente de configuración amigable Quick Router Setup	*	*
Smart QoS (Calidad de Servicio Inteligente)	*	*
Calidad de Servicio Inteligente para priorizar aplicaciones multimedia		*
Verificación automática en línea de actualizaciones de Firmware		*
Puede ser utilizado como Access Point al deshabilitar NAT	*	*

Cuadro 4.1: Características Técnicas De Los Routers de Prueba
Fuente: La Autora

A continuación, se presentan, las ilustraciones y las tablas donde se reflejan los resultados de la intensidad de señal, de cada **PA**, en cuanto a las variables: alcance y estructura física.

Ilustración 4.3: Diagrama De Cobertura De Señal En La Planta A Del Edificio Router Nexxt

Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto	Cantidad de Paredes
19,80m	5,5Mbps	1,34m	4
8,25m	54,0Mbps	0,72m	2
4,5m	54,0Mbps	0,6m	1
1,30m	54,0Mbps	0m	0
18,98m	36,0Mbps	0,48m	4
19,70m	36,0Mbps	0,36m	3
23,48m	5,5Mbps	0,60m	5
23,36m	0Mbps	0,72m	6
17,78m	24,0Mbps	0,36m	3
16,77m	24,0Mbps	0,36m	3
19,11m	24,0Mbps	0,36m	3
21,28m	24,0Mbps	0,36m	3
5,82m	54,0Mbps	0,36m	3
8,47m	54,0Mbps	0,36m	3
11,12m	54,0Mbps	0,36m	3
5,82m	54,0Mbps	0,24m	2
8,47m	54,0Mbps	0,24m	2
11,12m	54,0Mbps	0,24m	2
16,10m	24,0Mbps	0,36m	3
18,45m	24,0Mbps	0,36m	3
16,10m	24,0Mbps	0,36m	3
18,87m	11,0Mbps	0,48m	4

Cuadro 4.2: Cobertura De Señal En La Planta A Del Edificio Router Nexxt
Fuente: La Autora

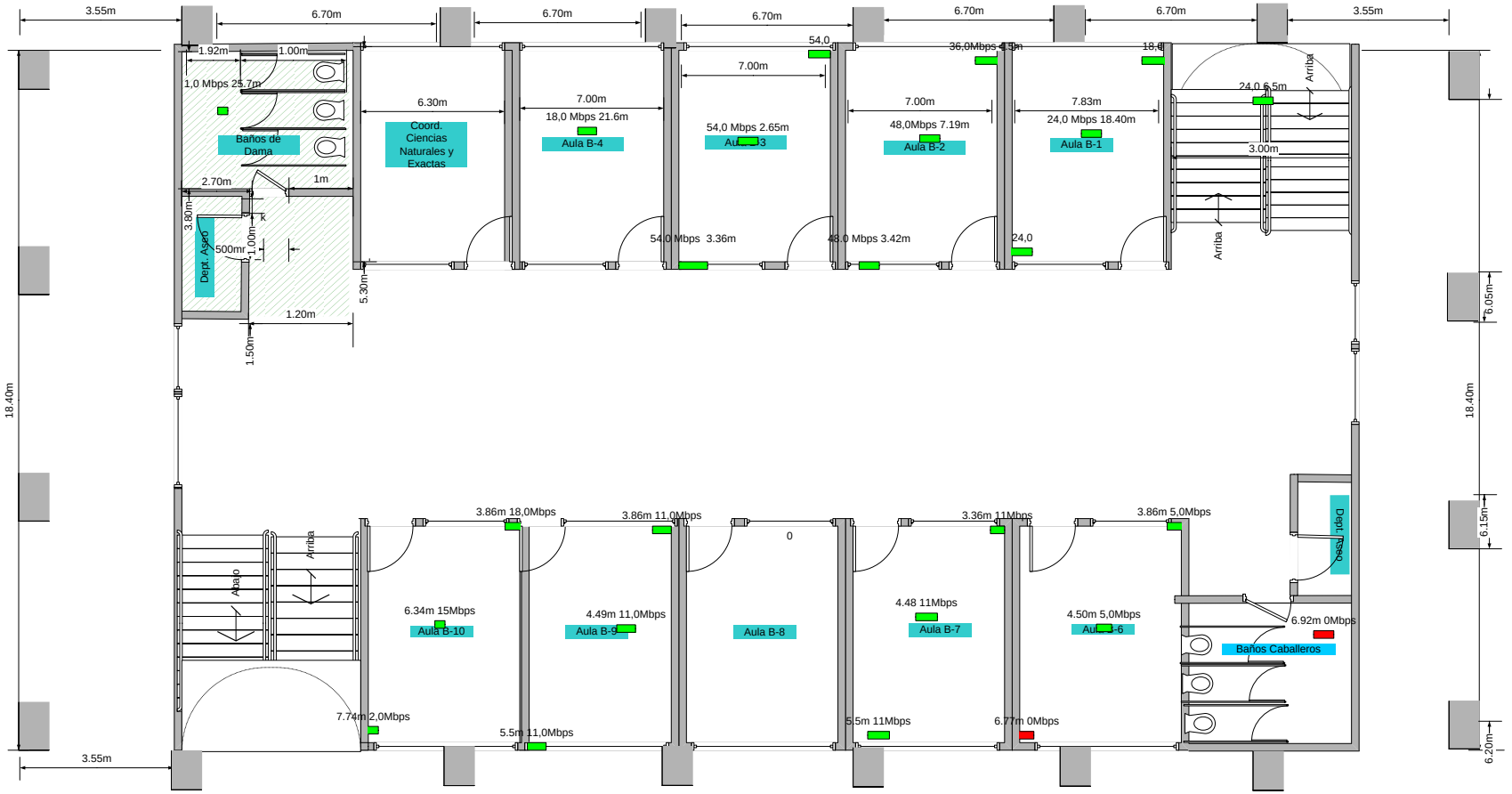

Ilustración 4.4: Diagrama De Cobertura De Señal En La Planta B Del Edificio Router Nexxt
Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto
25.7m	2Mbps	1,99m
21.6m	18 Mbps	1,49m
2.75m	54 Mbps	0,39m
3.42m	54 Mbps	0,39m
7.19m	48 Mbps	0,65m
4.5m	54 Mbps	1,13m
18.40m	24 Mbps	1,01m
23.5m	24 Mbps	1,37m
6.92m	54Mbps	1,01m
6.77m	54Mbps	1,01m
4.50m	54Mbps	1,01m
3.86m	54Mbps	1,01m
5.5m	54 Mbps	1,01m
4.48m	54 Mbps	1,01m
3.36m	54 Mbps	1.01m
4.49m	54 Mbps	0,89m
5.5m	48 Mbps	0,89m
7.74m	24Mbps	0,89m
6.34m	54 Mbps	1,01m
3.86m	54 Mbps	1,01m

Cuadro 4.3: Cobertura De Señal En La Planta B Del Edificio Router Nexxt
Fuente: La Autora

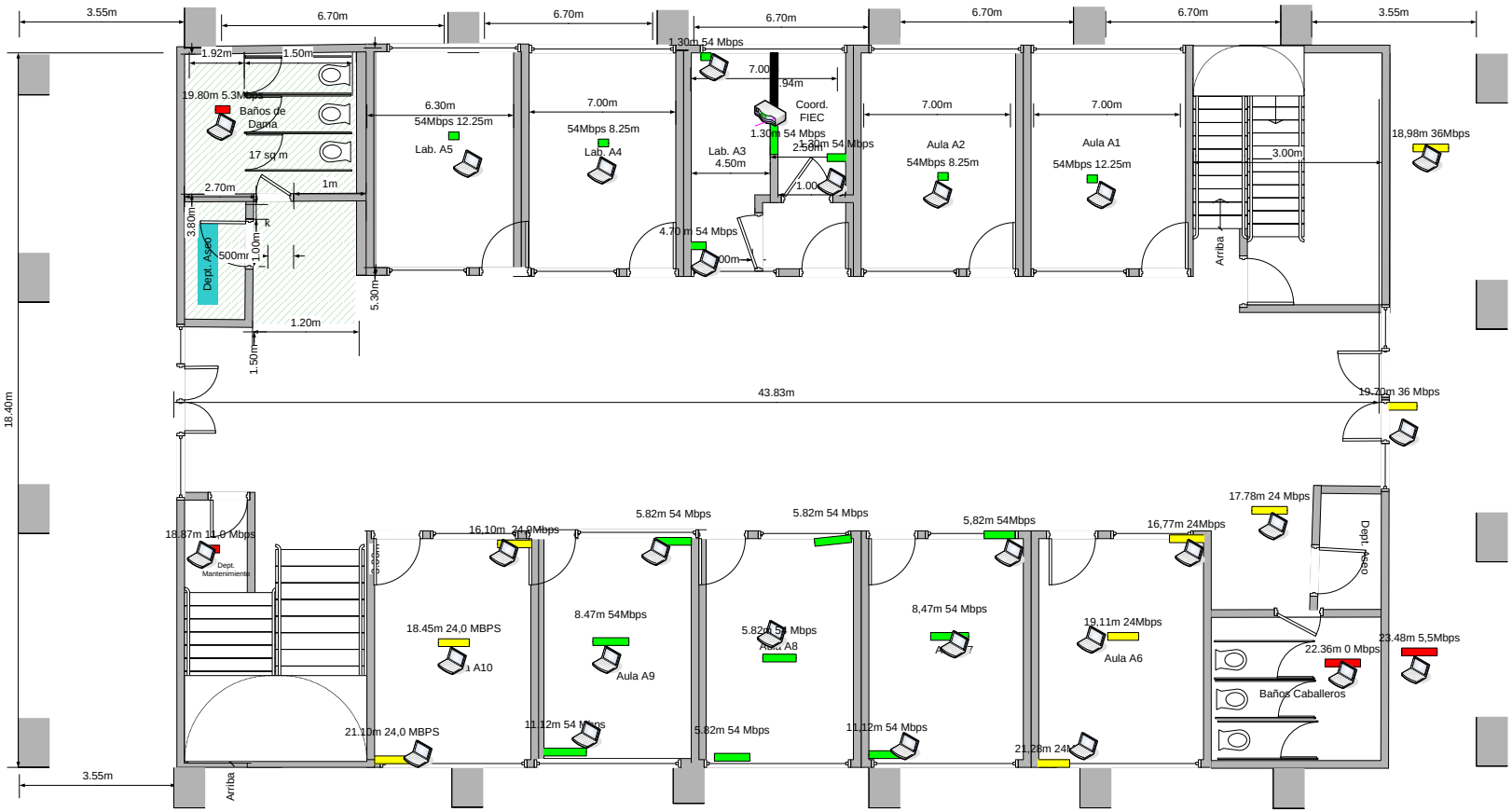

Ilustración 4.4: Diagrama De Cobertura De Señal AP Dlink 1 Antena En La Planta A Del Edificio
Fuente: **La Autora**

Distancia	Alcance	Cantidad de Concreto	Cantidad de Paredes
19,80m	24	1,34m	4
4,5m	54	0,6m	1
4,7m	54	0,6m	1
1,20m	54	0,6m	1
1,30m	54	0m	0
18,98m	54	0,48m	4
19,70m	54	0,36m	3
23,48m	2	0,60m	5
23,36m	0	0,72m	6
17,78m	24	0,36m	3
16,77m	24	0,36m	3
19,11m	24	0,36m	3
21,28m	24	0,36m	3
5,82m	54	0,36m	3
8,47m	54	0,36m	3
11,12m	54	0,36m	3
5,82m	54	0,24m	2
8,47m	54	0,24m	2
11,12m	54	0,24m	2
16,10m	24	0,36m	3
18,45m	24	0,36m	3
16,10m	54	0,36m	3
18,87m	24	0,48m	4

Cuadro 4.4: Cobertura De Señal AP Dlink 1 Antena En La Planta A Del Edificio
Fuente: La Autora

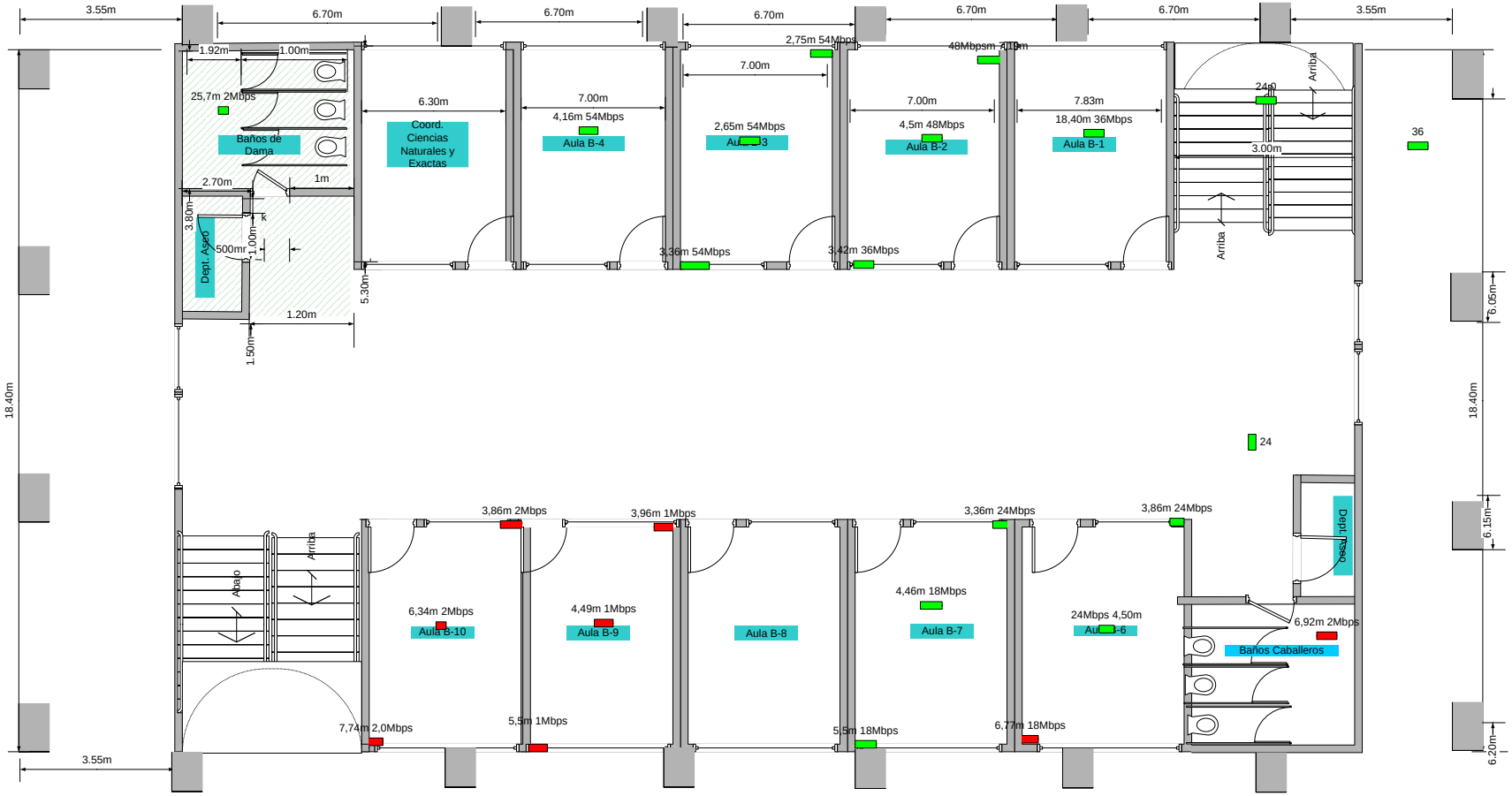

Ilustración 4.5: Diagrama De Cobertura De Señal AP Dlink 1 Antena En La Planta B Del Edificio
Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto
25.7m	1Mbps	1,99m
4.16m	18 Mbps	1,49m
3.36m	48 Mbps	1,37m
2.75m	48 Mbps	0,39m
2.75m	48 Mbps	0,39m
3.42m	48 Mbps	0,39m
7.19m	48 Mbps	0,65m
4.5m	48 Mbps	1,13m
18.40m	18 Mbps	1,01m
23.5m	18 Mbps	1,37m
6.92m	48 Mbps	1,01m
6.77m	0 Mbps	1,01m
4.50m	11 Mbps	1,01m
3.86m	11 Mbps	1,01m
5.5m	11 Mbps	1,01m
4.48m	11 Mbps	1,01m
3.36m	11 Mbps	1.01m
4.49m	11 Mbps	0,89m
5.5m	11 Mbps	0,89m
7.74m	2 Mbps	0,89m
6.34m	15 Mbps	1,01m
3.86m	18 Mbps	1,01m

Cuadro 4.5: Cobertura De Señal AP Dlink 1 Antena En La Planta B Del Edificio
Fuente: La Autora

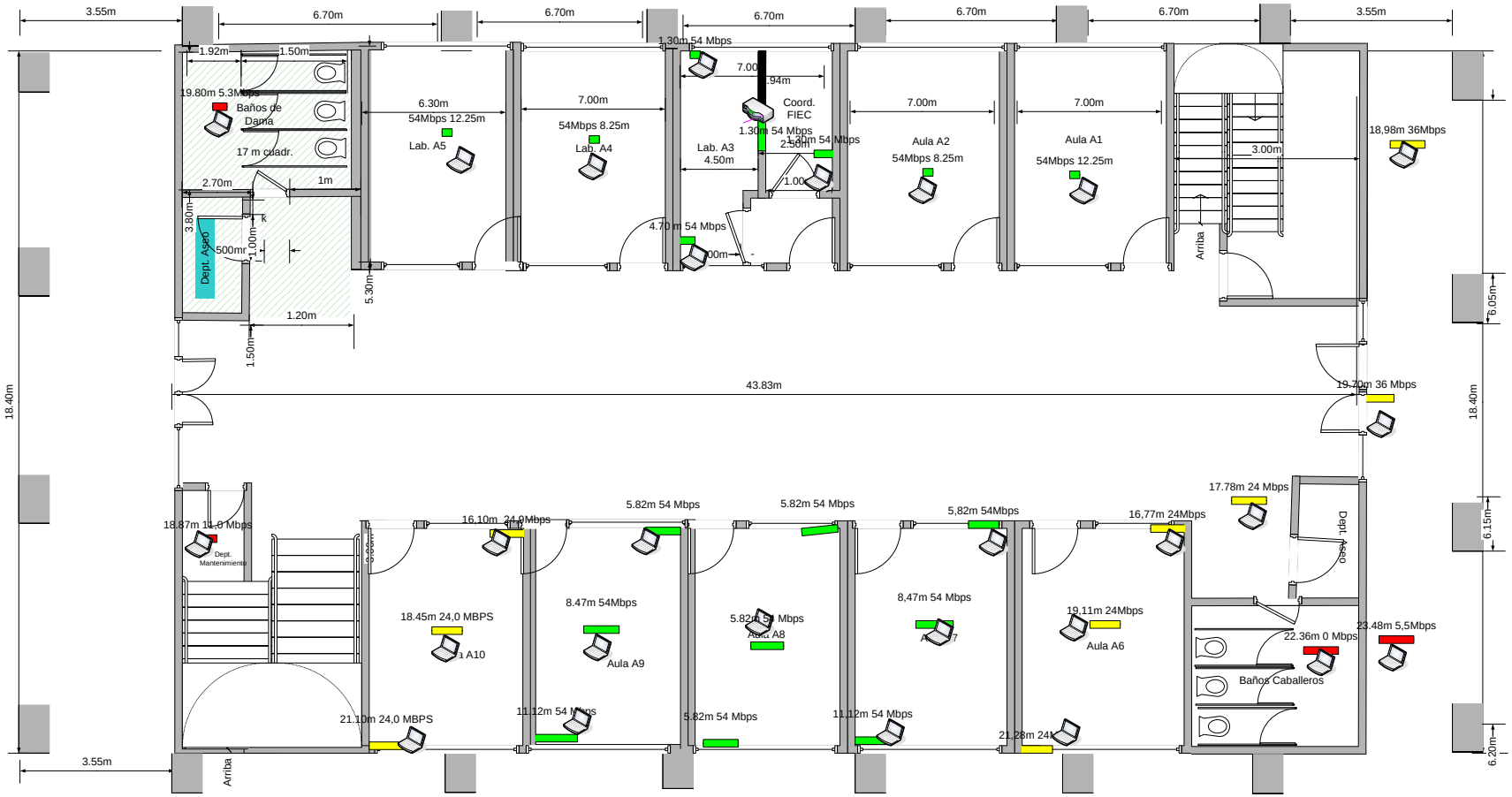

Ilustración 4.6: Diagrama De Cobertura De Señal AP Dlink 2 Antenas En La Planta A Del Edificio
Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto	Cantidad de Paredes
19,80m	5.3Mbps	1,34m	4
12,25m	54Mbps	0,84m	3
8,25m	54Mbps	0,72m	2
4,5m	54Mbps	0,6m	1
4,7m	54Mbps	0,6m	1
1,20m	54Mbps	0,6m	1
1,30m	54Mbps	0m	0
18,98m	36Mbps	0,48m	4
19,70m	5.5Mbps	0,36m	3
23,48m	0Mbps	0,60m	5
23,36m	5.5Mbps	0,72m	6
17,78m	24Mbps	0,36m	3
16,77m	24Mbps	0,36m	3
19,11m	24Mbps	0,36m	3
21,28m	24Mbps	0,36m	3
5,82m	54Mbps	0,36m	3
8,47m	54Mbps	0,36m	3
11,12m	54Mbps	0,36m	3
8,47m	54Mbps	0,24m	2
11,12m	54Mbps	0,24m	2
16,10m	24Mbps	0,36m	3
18,45m	24Mbps	0,36m	3
16,10m	24Mbps	0,36m	3
18,87m	11Mbps	0,48m	4

Cuadro 4.6: Cobertura De Señal AP Dlink 2 Antenas En La Planta A Del Edificio
Fuente: La Autora

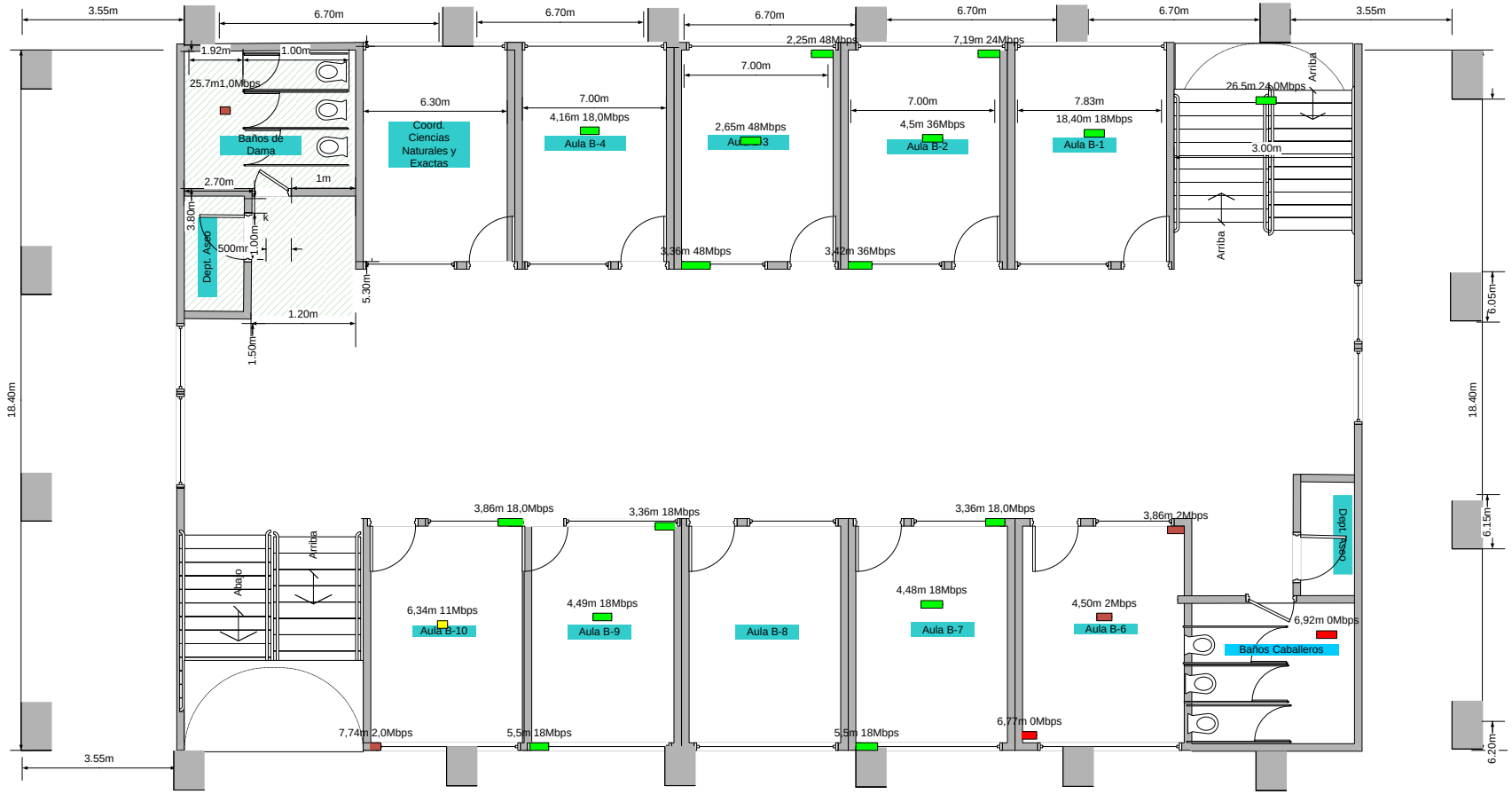

Ilustración 4.7: Diagrama De Cobertura De Señal AP Dlink 2 Antenas En La Planta B Del Edificio
Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto
25.7m	1Mbps	1,99m
21.6m	18 Mbps	1,49m
3.36m	48 Mbps	1,37m
2.75m	48 Mbps	0,39m
2.75m	48 Mbps	0,39m
3.42m	48 Mbps	0,39m
7.19m	48 Mbps	0,65m
4.5m	48 Mbps	1,13m
18.40m	18 Mbps	1,01m
23.5m	18 Mbps	1,37m
6.92m	48 Mbps	1,01m
6.77m	0 Mbps	1,01m
4.50m	11 Mbps	1,01m
3.86m	11 Mbps	1,01m
5.5m	11 Mbps	1,01m
4.48m	11 Mbps	1,01m
3.36m	11 Mbps	1.01m
4.49m	11 Mbps	0,89m
5.5m	11 Mbps	0,89m
7.74m	2 Mbps	0,89m
6.34m	15 Mbps	1,01m
3.86m	18 Mbps	1,01m

Cuadro 4.7: Cobertura De Señal AP Dlink 2 Antena En La Planta B Del Edificio
Fuente: La Autora

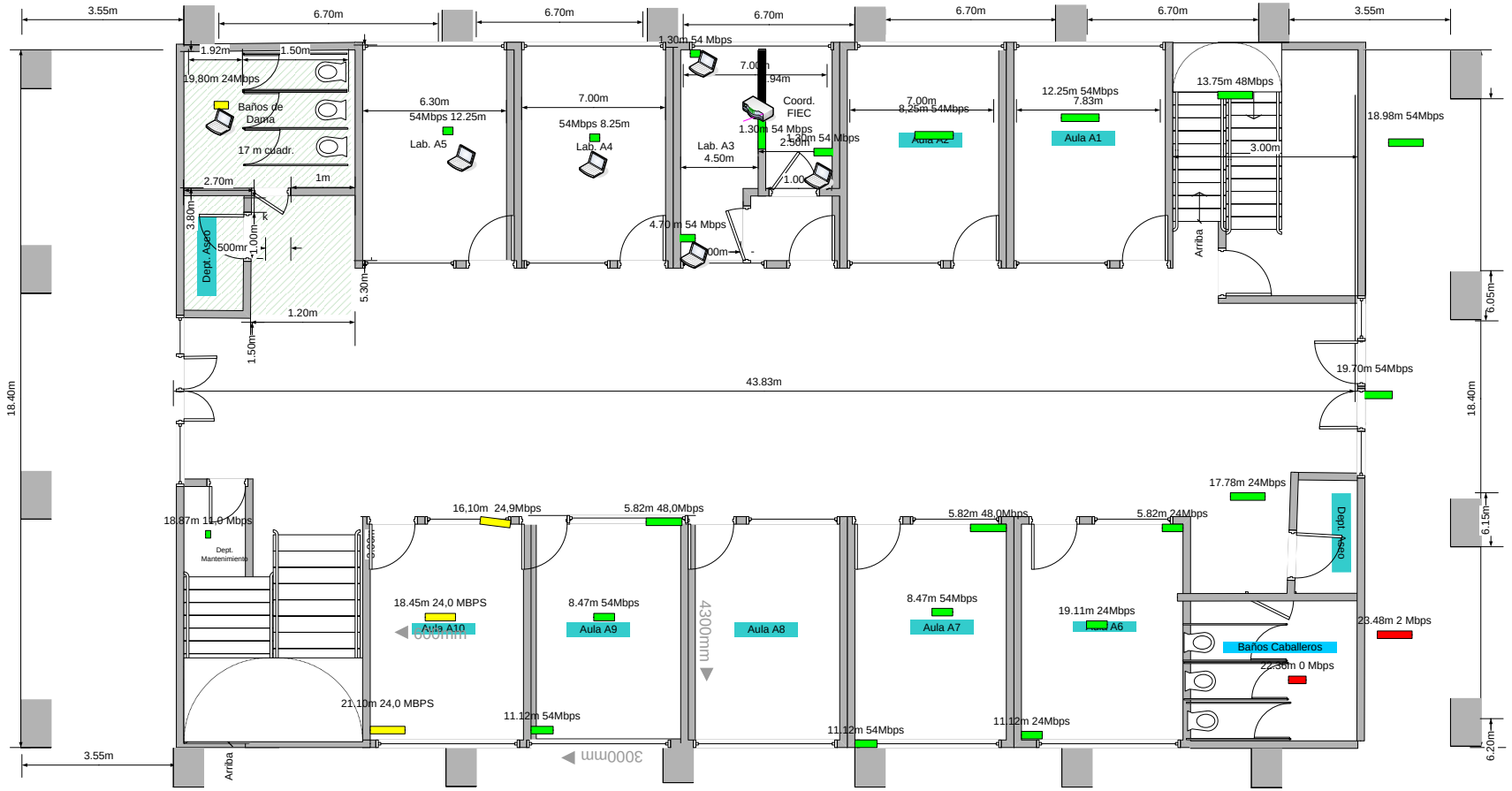

Ilustración 4.8: Diagrama De Cobertura De Señal AP Dlink 3 Antenas En La Planta A Del Edificio
Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto	Cantidad de Paredes
19,80m	18Mbps	1,34m	4
12,25m	54Mbps	0,84m	3
8,25m	54Mbps	0,72m	2
4,5m	54Mbps	0,6m	1
4,7m	54Mbps	0,6m	1
1,20m	54Mbps	0,6m	1
1,30m	54Mbps	0m	0
18,98m	36Mbps	0,48m	4
19,70m	18Mbps	0,36m	3
23,48m	3Mbps	0,60m	5
23,36m	2Mbps	0,72m	6
17,78m	48Mbps	0,36m	3
16,77m	54Mbps	0,36m	3
19,11m	54Mbps	0,36m	3
21,28m	48Mbps	0,36m	3
5,82m	54Mbps	0,36m	3
8,47m	54Mbps	0,36m	3
11,12m	54Mbps	0,36m	3
5,82m	54Mbps	0,24m	2
8,47m	54Mbps	0,24m	2
11,12m	54Mbps	0,24m	2
16,10m	54Mbps	0,36m	3
18,45m	48Mbps	0,36m	3

Cuadro 4.8: Cobertura De Señal AP Dlink 3 Antena En La Planta A Del Edificio
Fuente: La Autora

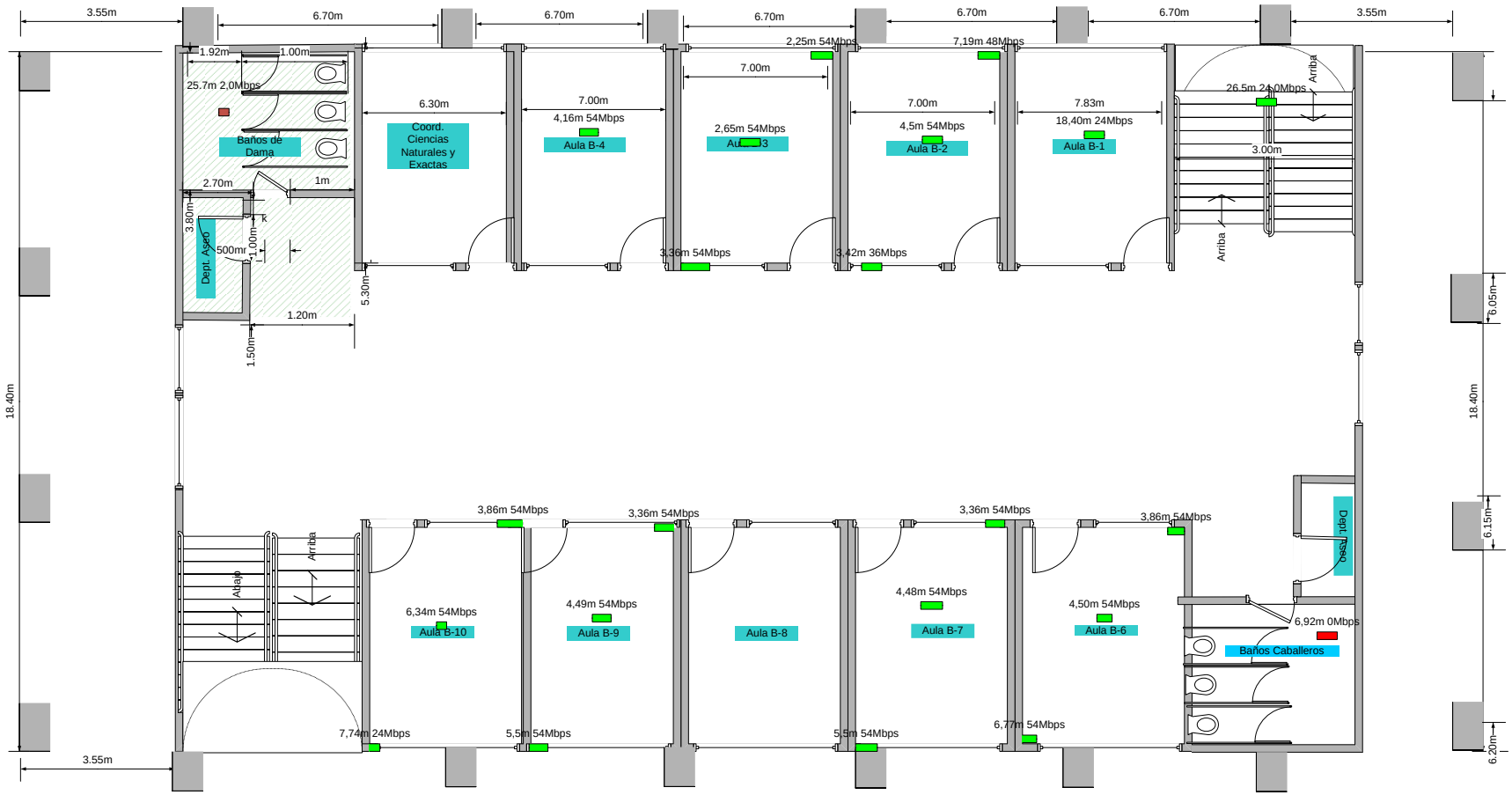

Ilustración 4.9: Diagrama De Cobertura De Señal AP Dlink 3 Antenas En La Planta B Del Edificio
Fuente: La Autora

Distancia	Alcance	Cantidad de Concreto
25.7m	2Mbps	1,99m
21.6m	18 Mbps	1,49m
3.36m	54 Mbps	1,37m
2.75m	54 Mbps	0,39m
2.75m	54 Mbps	0,39m
3.42m	54 Mbps	0,39m
7.19m	48 Mbps	0,65m
4.5m	54 Mbps	1,13m
18.40m	24 Mbps	1,01m
23.5m	24 Mbps	1,37m
6.92m	54Mbps	1,01m
6.77m	54Mbps	1,01m
4.50m	54Mbps	1,01m
3.86m	54Mbps	1,01m
5.5m	54 Mbps	1,01m
4.48m	54 Mbps	1,01m
3.36m	54 Mbps	1.01m
4.49m	54 Mbps	0,89m
5.5m	48 Mbps	0,89m
7.74m	24Mbps	0,89m
6.34m	54 Mbps	1,01m
3.86m	54 Mbps	1,01m

Cuadro 4.9: Cobertura De Señal AP Dlink 3 Antena En La Planta B Del Edificio
Fuente: La Autora

4.2 Diseño Lógico De Red WIFI.

El diagrama que se muestra a continuación, representa el direccionamiento de la red que se propone para el Edificio A, B del CRUV.

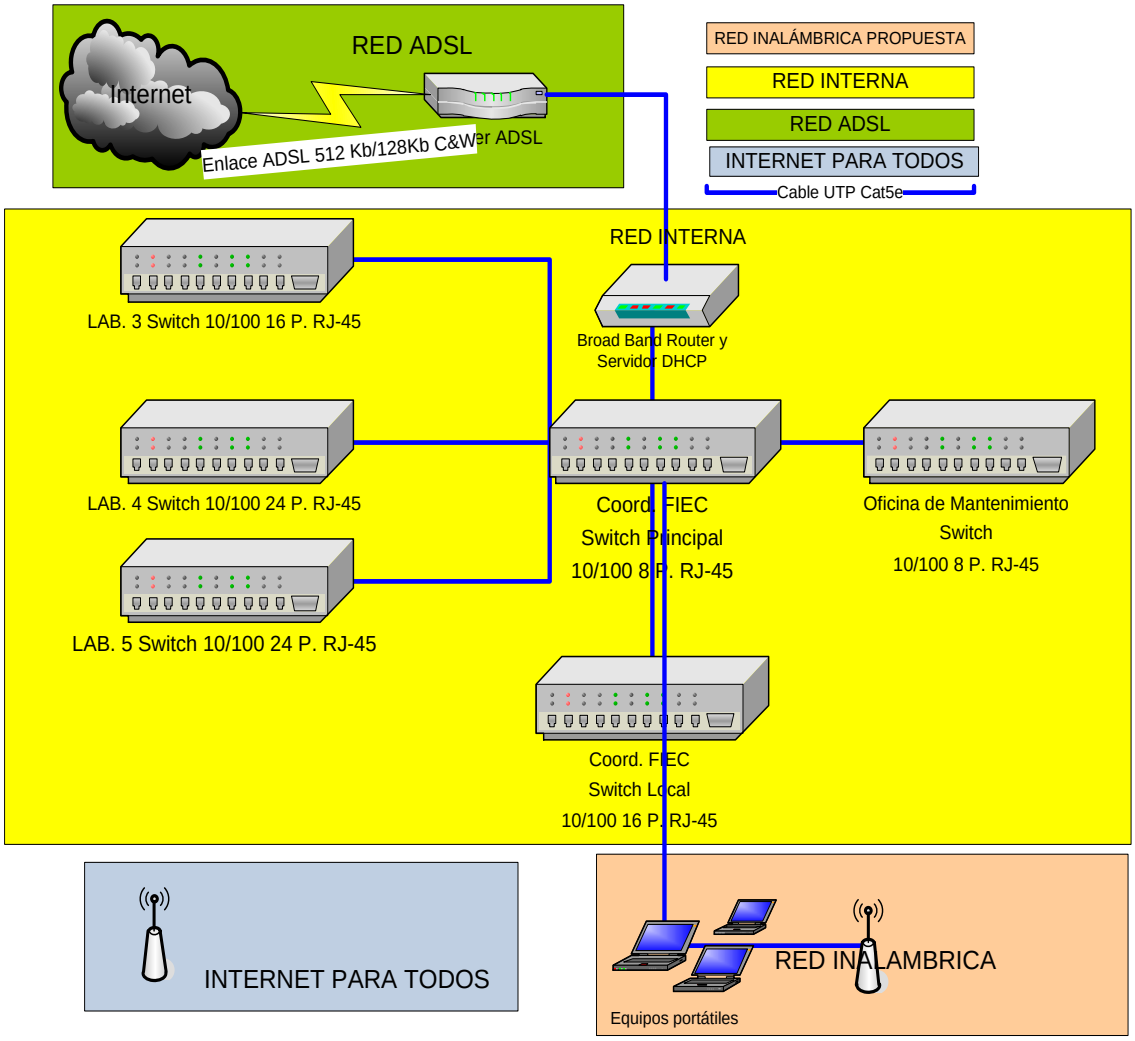

Ilustración 4.10: Diagrama De Diseño Lógico de la Red, Edificio A-B Del CRUV
Fuente: La Autora

Por otro lado, el cuadro que se presenta a continuación detalla el direccionamiento de la red que se propone para el Edificio A, B del CRUV.

Direccionamiento Red ADSL C & W	
Dirección De Red	192.168.1.0
Puerta de Enlace	192.168.1.1
Rango De Direcciones IP	192.168.1.{2,100}
Máscara de Red	255.255.255.0
DNS	201. 225. 225.225
	201. 225. 225.226
	201.224.73.162
Red Interna LAN Cableado	
Dirección De Red	192.168.2.0
Puerta de Enlace	192.168.2.254
Máscara de Red	255.255.255.0
Rango De Direcciones IP	192.168.2.{2,254}
DNS	201. 225. 225. 225
	201. 225. 225.226
	201.224.73.162
	192.168.2.254
Red Inalámbrica	
Dirección de Red	198.162.3.0
Puerta de Enlace	198.162.3.1
Máscara de Red	255.255.255.0
Rango De Direcciones IP	192.168.3.{2,254}
DNS	201. 225. 225. 225
	201. 225. 225.226
	201.224.73.162
	192.168.2.254
	198.162.3.1

Cuadro 4.10: Direccionamiento De Red, Edificio A-B, Del CRUV
Fuente: La Autora

4.3 Políticas De Seguridad De La Red WIFI.

Las Políticas de Seguridad son consideradas, en el marco de las tecnologías de información y comunicación, como un medio para brindar calidad y confiabilidad en cuanto el uso de un recurso informático; ellas se derivan directamente de la filosofía de la organización donde se implementarán, que se

pueden sintetizar en su misión y visión; para el caso particular de este estudio: la Universidad de Panamá.

En consecuencia, se establecerán lineamientos que norman aspectos tales como: el propósito de la red, su privacidad, las responsabilidades, sus condiciones de uso, disponibilidad, conexión, procedimientos de seguridad, ética y moral, autorización, regulaciones y estándares.

A continuación se detallan las políticas de uso y seguridad de la red **WIFI**, en base a la misión y visión de la Universidad de Panamá.

4.3.1 MISIÓN Y VISIÓN DE LA UNIVERSIDAD DE PANAMÁ.

La Universidad de Panamá, en la Gaceta Oficial 26202, donde se publica su Estatuto Universitario, define su visión como:

> *"Ser una institución reconocida y acreditada a nivel nacional e internacional, caracterizada por la excelencia en la formación de profesionales, integrada con la docencia, la investigación pertinente, el desarrollo tecnológico, la producción y la extensión, para contribuir al desarrollo nacional.* **[UNIV10].**

Y su misión como:

> *"Institución de referencia regional en educación superior, basada en valores, formadora de profesionales emprendedores, íntegros, con conciencia social y pensamiento crítico; generadora de conocimiento innovador a través de la docencia, la investigación pertinente, la extensión, la producción y servicios, a fin de crear iniciativas para el desarrollo nacional, que contribuyan a erradicar la pobreza y mejorar la calidad de la vida de la población panameña"* **[UNIV10]**.

Según el Artículo 2 de la Universidad de Panamá, la misión y visión de la Universidad de Panamá, se inspiran en los más altos valores humanos y está dedicada a la generación y difusión del conocimiento, a la investigación y a la formación integral, científica, tecnológica, humanística y cultural, dentro del marco de la excelencia académica, con actitud crítica y productiva **[EUNP08]**.

En el ámbito educativo, los recursos académicos y humanos de la Universidad de Panamá, están orientados a fortalecer la formación de los estudiantes basados en fines académicos, administrativos, de investigación, extensión y producción, por ello, es necesario brindarles a los estudiantes y profesores, todas las herramientas posibles que faciliten y fortalezcan los proceso de enseñanza-aprendizaje **[EUNP08]**.

4.3.2 PROPÓSITO DE LA RED INALÁMBRICA PROPUESTA.

El propósito fundamental de esta red, radica en ofrecer el servicio de comunicación de datos, de forma inalámbrica a estudiantes y profesores del Centro Regional Universitario de Veraguas, sin la necesidad de utilizar un equipo fijo, que les permita utilizar los servicios ofrecidos actualmente en la red pre - existente de la FIEC.

El uso adecuado de la Red Inalámbrica de la FIEC-CRUV, es importante para el beneficio de sus usuarios y de la Universidad de Panamá, ya que se aprovecharán los recursos tecnológicos que brinda la conexión inalámbrica a

dicha red, de manera acorde con los fines de la institución, que se han establecido con anterioridad.

4.3.3 LINEAMIENTOS NORMATIVOS QUE SE DEBEN CONSIDERAR AL MOMENTO DE ESTABLECER LAS POLÍTICAS DE SEGURIDAD.

El propósito final de las normas y políticas en el uso adecuado de la red inalámbrica, busca determinar las responsabilidades y derechos que contrae quien utilice el servicio de la red inalámbrica, en términos de: cómo será utilizada, administrada, asegurada y apoyada en el Centro Regional Universitario de Veraguas.

La red inalámbrica, ofrecerá un servicio específicamente dentro del perímetro del edificio A-B, del Centro Regional Universitario de Veraguas, por lo tanto los usuarios del servicio deben respetar los derechos de otros usuarios. Se debe recalcar que este servicio no es un derecho de los usuarios, es un privilegio que se les otorga. De manera que será su deber, el respetar la integridad de los sistemas y los recursos físicos y lógicos que la integran, así como seguir las normas y políticas de uso de la red.

4.3.3.1 PRIVACIDAD DE DIVULGACIÓN DE DATOS DE LOS USUARIOS.

El Centro Regional Universitario, debe reconocer el derecho a la privacidad de divulgación de los datos del usuario y bajo ninguna circunstancia dará a conocer datos, ni información de cualquier usuario antes de consultarlo con el mismo.

4.3.3.2 POLÍTICAS DE USO ADECUADO DE LOS USUARIOS.

Los usuarios están comprometidos realizar un buen uso de los recursos de la red **WIFI**, de acuerdo a lo establecido en las reglamentaciones internas de la FIEC y siguiendo los lineamientos de la visión y misión de la Universidad de Panamá.

4.3.3.3 RESPONSABILIDADES DE LOS ADMINISTRADORES DE LA RED.

La responsabilidad en el uso y mantenimiento se encuentra bajo el Departamento de Informática del Centro Regional Universitario de Veraguas. Estas responsabilidades son y sin restricción a:

Informar a los usuarios sobre las normas y políticas de seguridad.

- Resolver cualquiera inquietud reportado por los usuarios.

- Proveer de asistencia técnica, orientación y recomendación sobre los equipos a utilizar dentro de la red inalámbrica.

- Crear, mantener y actualizar las normas de seguridad y manejo que se aplicarán dentro de esta red.

- Aprobar la instalación de equipo y configuración para la red **WIFI**, utilizada en la Universidad.

- Mantener registro de las tarjetas inalámbricas, puntos de acceso y direccionamiento físico-lógico dentro de la red **WIFI**.

- Monitorear y optimizar el rendimiento y seguridad de todos los recursos de la red **WIFI**.

4.3.3.4 REGULACIONES Y ESTÁNDARES QUE SE DEBEN SEGUIR.

Todos los equipos que se instalen dentro de la red **WIFI**, deben ser compatibles con los estándares que establece **Modelo OSI**.

Todo equipo debe cumplir como mínimo con el estándar **IEEE** 802.11g, de comunicación inalámbrica, o el estándar que utilice la Universidad de Panamá.

4.3.3.5 SEGURIDAD QUE DEBE OFRECER LA RED.

Para que este lineamiento se cumpla a cabalidad, es necesario acatar una serie de procedimientos que se detallan a continuación:

- Los **PA** deben cumplir con los aspectos técnicos, que se describen en el apartado 4.4 relacionado con la Selección de Componentes, en donde se plantea compatibilidades entre los equipos, para que se minimicé la posibilidad de incompatibilidad entre los equipos.

- Los **PA** deben estar registrados bajo los modelos físicos y lógico de la red, para minimizar la presencia de equipos ilegales dentro de la red.

- La instalación, uso y manejo de los equipos deben estar regulado por las normas vigentes en el Centro Regional Universitario de Veraguas, relacionadas con la materia, ya que este servicio debe estar reglamentado por las normas de la institución.

- El equipo debe ser instalado y configurado por personal autorizado del Departamento de la Facultad de Informática, Electrónica y Comunicación del Centro Universitario de Veraguas, para que asegurar la interoperabilidad de los equipos.

- El equipo debe ser instalado minimizando la interferencia con otros equipos de **RF**, para mantener la calidad de transmisión de datos.

- No se debe permitir ni fomentar el uso del recurso el cual viole la integridad de sus usuarios o de la universidad ya que amenaza el derecho a la privacidad de los usuarios.

- Todo equipo que esté conectado a la red inalámbrica debe ser objeto de una auditoría de seguridad, cuando se detecte violaciones en el uso de la red inalámbrica.

- Cualquier equipo que ponga en peligro la red inalámbrica será desconectado de la misma, para asegurar proteger a los equipos, los usuarios y su información.

4.3.3.6 CONDICIONES DE USO DE LA RED INALÁMBRICA.

Para brindar un servicio de calidad, se requiere que los usuarios de la red actúen responsablemente. Por lo tanto, se describen las condiciones de uso que deben respetar al momento de utilizar este recurso:

- Las personas autorizadas para el acceso a la red son: los estudiantes y docentes de la Facultad de Informática, Electrónica y Comunicación, así como cualquier otra persona que los administradores de la red autoricen.

- Para que un usuario, tenga acceso a la red inalámbrica, es necesario que su equipo sea registrado, bajo un sistema de restricción de

direccionamiento **MAC**. Únicamente, si el **MAC** del usuario está registrado, se le dará el acceso correspondiente.

- El servicio estará disponible, mientras el usuario se encuentre dentro de la cobertura de la red, el sistema de conexión a la red inalámbrica está sujeto a condiciones fortuitas o programadas de no disponibilidad, por situaciones tales como: emergencias, equipos, problemas o limitaciones de la red, interferencia, mantenimiento y reparación del servicio.

- Para controlar el caso de violaciones a las normas y regulaciones de este servicio, los usuarios deben permitir la supervisión de sus equipos, para verificar el buen uso del sistema de red WIFI. Adicionalmente, se procederá a sancionar y restringir el acceso a este servicio, a los usuarios que violen estos procedimientos.

- Todo usuario que acceda a la red tiene la responsabilidad de notificar al Facultad de Informática, Electrónica y Comunicación, cualquier acción descubierta en relación a la violación de cualquiera de las condiciones descritas anteriormente, como el uso inapropiado de los recursos que ofrezca la red.

- La Facultad de Informática, Electrónica y Comunicación podrá limitar o denegar el acceso, contenido del servicio inalámbrico, siempre que se le esté dando un mal uso.

- Todas las medidas que se describen dentro de estos apartados, tienen la finalidad de brindar seguridad y calidad de servicio a los usuarios de la red inalámbrica. Se permite su realización, bajo la supervisión de los administradores de la red.

Por otro lado, dentro de los lineamientos de conexión a la red inalámbrica, los usuarios deben tomar en consideración los siguientes aspectos:

- No deben compartir su conexión a la red con ningún otro individuo.

- No deben acceder a recursos de comunicaciones restringidos, sin la debida autorización.

- Los administradores no deben autorizar ningún acceso a la red, por parte de equipos que no estén registrados previamente.

- No se permite el acceso de los usuarios que están previamente registrados a sitios webs que no estén destinados a fines académicos, de investigación o producción.

- Los administradores se reservan el derecho incondicional de suspender o rescindir el uso de la red inalámbrica, por cualquier violación a esta política, o por cualquier actividad que interfiera con su utilización, a cualquier usuario que realice este tipo de acciones, de acuerdo a la gravedad de las faltas.

En otro orden de ideas, desde el punto de vista de la ética y la moral, los usuarios deben tomar en consideración los siguientes aspectos:

- Se prohíbe la transmisión y la distribución de cualquier material discriminatorio para cualquier persona o grupo de personas.

- Se prohíbe transmitir mensajes que revelen cuestiones personales o privadas relativas a cualquier persona, entre las que se incluyen, pero sin limitación a ellas, mensajes o información que pueda infringir los derechos de las personas a su privacidad.

- No se permite utilizar identidades falsas dentro de esta red.

- Se prohíbe el intercambio o manejo de la pornografía en todos sus géneros dentro de esta red.

Adicionalmente, al considerar a los equipos de la red **WIFI**, los usuarios deben tomar en consideración los siguientes aspectos:

- Los usuarios no deben modificar, dañar o mover los equipos de la red.

- No se debe generar ningún tipo de interferencia que afecte la calidad de la señal de red.

En otro orden, en el aspecto de la información y los programas no autorizados, los usuarios deben tomar en consideración los siguientes aspectos:

- Los usuarios no tienen permitido realizar rastreos de los equipos de la red por medio del direccionamiento de los equipos o cualquier otra técnica.

- Los usuarios no pueden recolectar información que está siendo transmitida por otros usuarios de la red o guardados en cualquier medio de almacenamiento masivo.

- Los usuarios no tienen permitido realizar monitoreo de comunicación, entre los equipos que están utilizando la red.

- Los usuarios no tienen permitido buscar vulnerabilidades de la red inalámbrica.

Finalmente, en el aspecto del apoyo técnico, los usuarios deben tomar en consideración los siguientes aspectos:

El encargado de administrar y dar mantenimiento de la red, será el responsable de registrar la **MAC**, correspondiente a cada equipo, para contar con el acceso a la misma red, y verificar que el equipo adquiera la dirección **IP**, solamente **[UPTO07]**. El encargado del mantenimiento, no tiene la responsabilidad de brindar entrenamiento en cuanto al uso de programas y aplicaciones de la red inalámbrica.

4.3.3.7 IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD.

Procedimiento para asegurar los recursos de la red y de los servicios en el caso de detectar el uso indebido de la red inalámbrica, se define como sigue:

- El administrador de la red, en caso tal que alguien incurra en falta a las normas establecidas, debe desactivar la cuenta o desconectar el equipo del sistema de comunicación de datos, donde se ha cometido dicha falta.

- Verificar y discutir, con el usuario afectado, el supuesto uso indebido del recurso.

- Además, se debe notificar a la Coordinación de la Facultad de Informática, Electrónica y Comunicación del problema.

- De ser necesario, el administrador de la red inalámbrica, toma acciones disciplinarias.

4.4 Selección De Componentes.

Para implementar la red inalámbrica propuesta para el edificio A-B, del Centro Regional Universitario de Veraguas, se ha seleccionado una serie de componentes basado en las pruebas de cobertura de la red. A continuación se detallan dichos componentes en el siguiente cuadro:

EQUIPOS DE LA RED INALAMBRICA						
#	Cantidad	Unidad	Componente	Modelo	Especificación	Funcionalidad
1	2	C/U	Broand Router- Servidor DHCP(Conector, Corriente de Alimentación)	Linksys Router Inalámbrico de banda dual WRT320N	4 puertos Ethernet,1 puerto WAN (Internet),Encripción inalámbrica 128-bit,Firewall,Velocidad Gigabit.	Puntos de Acceso, para cada una de las plantas del Edificio
2	1	C/U	PLANET Content Security Gateway	CS500	1 x WAN, 1 puerto LAN, 1 x zona de despeje, 200 túneles VPN	Filtrado de Contenido entre Internet y Puntos de Acceso
3	45	pie	Cable UTP Cat 5e	Estándar	Cable rígido Categoría 5e, UTP con cubierta PVC	Cable para interconexión de los puntos de acceso
4	30	C/U	Tornillos para soporte de moldura	Estándar	Rosca Tirafondo	Sujetar la moldura en la pared concreto
5	8	metro	Moldura	Estándar	Material:PVC Dimensión: 2mx20mmx75mm	Seguridad para Cable Cat 5
6	10	C/U	Conectores RJ-45	Estándar	RJ-45	Conexión de cables
7	1	Unidad	Cajilla Eléctrica 4"*4"	Estándar	Metálica 4"*4"	Caja de Toma corriente
8	2	metro	Cable Eléctrico Calibre 12	Estándar	Con cubierta PVC	Cable para la conducción de corriente electrica para alimentar a puntos de acceso
9	2	C/U	Empalme Eléctrico	Estándar	Macho-Hembra	Conectores para enroscar cajilla eléctrica y tubo eléctrico
10	1	Unidad	Tapa de Repello	Estándar	Salida Doble	Tapa para sellar el toma corrriente
11	1	Unidad	Tubo Electrico	Estándar	1 Pulgada	Tubo para cubrir y guiar cable eléctrico
12	1	C/U	Cajilla de Seguridad	Estándar	Caja de Metal, Dimensión 20cmx30cm	Caja de protección para los puntos de accesos
13	1	C/U	Breaker de Seguridad	Estándar	Indicador LED	Breaker de Seguridad de corte de eléctrico

Cuadro 4.11: Selección de Componentes para la Red Propuesta
Fuente: La Autora

4.5 Presupuesto.

Al realizar el cálculo para la creación de la red inalámbrica para el Edificio A-B del C.R.U.V, se presenta un estimado de los costos de los componentes y de mano de de obra, que se tienen para este proyecto. A continuación, se presenta este cuadro:

PRESUPUESTO					
#	*Cantidad*	*Unidad*	*Componente*	*Precio Unitario*	*Costo Total*
1	2	Unidad	Broand Router- Servidor DHCP(Conector, Corriente de Alimentación)	B/. 68.90	B/. 137.80
2	15	metro	Cable UTP Cat 5e	B/. 0.45	B/. 6.75
3	30	Unidad	Tornillos para soporte de moldura	B/. 0.30	B/. 9.00
4	8	metro	Moldura	B/. 3.00	B/. 24.00
5	10	Unidad	Conectores RJ-45	B/. 0.25	B/. 2.50
6	1	Unidad	Cajilla 4*4	B/. 5.00	B/. 5.00
7	3.33	metro	Cable Electrico Calibre 12	B/. 1.50	B/. 5.00
8	2	Unidad	Conectores Electricos	B/. 0.20	B/. 0.40
9	1	Unidad	Tapa de Repello	B/. 0.25	B/. 0.25
10	1	Unidad	Tubo Electrico	B/. 4.00	B/. 4.00
11	1	Unidad	PLANET Content Security Gateway	B/. 680.90	B/. 680.90
12	2	Unidad	Cajilla de Seguridad	B/. 20.00	B/. 40.00
13	2	Unidad	Breaker de Seguridad	B/. 25.00	B/. 50.00
				SUB-TOTAL	B/. 965.60
				ITBMS	B/. 67.59
				TOTAL	B/. 1,033.19
14	1	Unidad	Instalación		B/. 150.00
15	1	Unidad	Gastos de Contingencia		B/. 500.00
				SUB-TOTAL	B/. 650.00
				TOTAL	B/. 1,683.19

Cuadro 4.12: Presupuesto para la Red Propuesta
Fuente: La Autora

4.6 Análisis Financiero TIRE y VaN.

El análisis financiero de un proyecto, se puede evaluar mediante Métodos de Análisis de Inversión, para el caso del estudio de factibilidad de creación de la red inalámbrica, se calcula su proyección mediante la Tasa Interna de Retorno Estimada (**TIRE**).

Se denomina **TIRE**, a la tasa de descuento que hace que el Valor Actual Neto (**VAN**) de una inversión sea igual a cero. Es decir, se entiende que la suma de los valores actualizados de todos los flujos netos de caja esperados del proyecto, deducido el valor de la inversión inicial. Si un proyecto de inversión tiene un **VAN** positivo, el proyecto es rentable.

El **VAN,** también puede expresarse como un índice de rentabilidad, llamado Valor neto actual relativo, expresado bajo la siguiente formula:

(VAN de la inversión)/Inversión

O bien en forma de tasa porcentual:

(VAN de la inversión x 100)/Inversión [WIKI10C].

De acuerdo a estos planteamientos, aunado con los materiales y presupuesto de este proyecto, se tiene el cálculo de inversión del proyecto, planteado en el siguiente cuadro:

A continuación, se plantean los valores que representan los gastos de instalación y funcionamiento – o mantenimiento - del proyecto, durante un período de 5 años, en el cuadro que se muestra a continuación:

DETALLES	INDICADOR	COSTO / AÑO	AÑOS				
			1	2	3	4	5
GASTO DE DEPRECIACIÓN / CONTINGENCIA	5	B/. 300.00	B/. 750.00	B/. 750.00	B/. 750.00	B/. 750.00	B/. 750.00
GASTO DE MANTENIMIENTO	10	B/. 25.00	B/. 250.00	B/. 250.00	B/. 250.00	B/. 250.00	B/. 250.00
TOTAL DE BENEFICIOS			B/. 1,000.00	B/. 1,000.00	B/. 1,000.00	B/. 1,000.00	B/. 1,000.00

Cuadro 4.13: Presupuesto de Funcionamiento Red Cableada
Fuente: La Autora

Los desembolsos planteados están dados en base a que sólo se tienen gastos de instalación en el período inicial, cuando se realiza la instalación de la red, y en el caso de funcionamiento es de valor cero, ya que para este tipo de red no se contemplan costos de funcionamiento.

Para el cálculo de los beneficios que se representan en el cuadro anterior, se tiene un indicador de 5. Este valor se establece con base en la cantidad de componentes de la red cableada, que se podrían dañar o depreciar – por año - en algunas de las 20 aulas del Edificio A-B del CRUV **[WIKI10C]**.

Por otro lado, se establece un valor de 10 elementos en gastos de mantenimiento, que representan los componentes de la red cableada que deben ser reparados periódicamente, tales como: cajillas y cableado – esencialmente -, broandrouter, switches, firewall – en menor medida -, que compondría la red cableada, por un período de 5 años de uso, como se representa en el **¡Error! No s e encuentra el origen de la referencia.**.

Por otro lado, la red **WIFI**, representa una inversión económica donde se tendrán, únicamente, gastos de funcionamiento, además del costo de instalación, tal como se representa en el siguiente cuadro:

PRESUPUESTO DE FUNCIONAMIENTO					
DETALLES	**AÑOS**				
	1	**2**	**3**	**4**	**5**
INSTALACIÓN	B/. 150.00	B/. 150.00	B/. 150.00	B/. 150.00	B/. 150.00
SUB-TOTAL	B/. 150.00	B/. 150.00	B/. 150.00	B/. 150.00	B/. 150.00

Cuadro 4.14: Presupuesto Acumulado De Funcionamiento De La Red WIFI
Fuente: La Autora

Los gastos anuales representan la inversión inicial del proyecto, el cual mantiene su valor durante el periodo de evaluación.

Como consecuencia, el análisis **TIRE**-**VAN** de este proyecto se presenta en el siguiente cuadro:

DETALLES	**AÑOS**					
	0	**1**	**2**	**3**	**4**	**5**
BENEFICIOS		B/. 850.00	B/. 850.00	B/. 850.00	B/. 850.00	B/. 850.00
Gastos de Capital o Inversión	B/. 1,683.192					
Valor de Salvamento de los Activos Fijos						B/. 841.60
TOTAL DE BENEFICIOS NETOS	B/. (1,683.192)	B/. 850.00	B/. 850.00	B/. 850.00	B/. 850.00	B/. 850.00
Valor Actual Neto Económico (VANE) (10%)	**$1,399.07**					
Tasa Interna de Retorno Económico	**42%**					

Cuadro 4.14: Beneficios del Proyecto
Fuente: La Autora

En consecuencia:

1. El proyecto es rentable ya que al 10% (Tasa Social de Descuento) el **VAN** es POSITIVO.

2. La Tasa Interna de Retorno Estimada (**TIRE**), es el castigo máximo que soporta el proyecto en forma general.

3. La **TIRE** es de 42% calculado, muy por encima del 10% del **VAN**.

4. Con base en lo anterior, se indica que el proyecto es tiene sustento económico – su implementación resultará beneficiosa a la institución -.

CONCLUSIONES

A continuación, se exponen las conclusiones de este estudio de factibilidad:

En ámbitos académicos, las redes inalámbricas gozan de gran aceptación ya que permiten movilidad, flexibilidad, además son consideradas como mejor opción en entornos en donde se hace inadecuado o imposible la instalación de redes basadas en cable.

Para la implementación de una red inalámbrica, se deben considerar aspectos de muy diversa índole: desde que finalidad tendrá y quiénes serán sus usuarios, hasta el entorno en que hay que montar la red; con el objeto de ofrecer un servicio de calidad, con los niveles adecuados de seguridad y controles apropiados de acceso a los recursos disponibles.

En la asignación de canales para equipos **WIFI**, dentro de los parámetros que pueden configurarse de acuerdo a necesidades particulares, y tomando en cuenta que los 11 canales disponibles no son completamente independientes; en la práctica, sólo se pueden utilizar 3 canales en forma simultánea (1, 6 y 11), para irradiar las señales.

La cobertura y la calidad de señal de una red inalámbrica, dependen de la estructura física en donde se vaya a implementar la red; ya que de este factor

depende la colocación de los puntos de acceso, para así brindar cobertura, exclusivamente, en las zonas que se ha planificado ofrecer este servicio.

Es necesario que, en cualquier ámbito que se vaya a implementar una red WIFI, se tomen en cuenta, la filosofía de la organización o empresa, donde se implementa dicho servicio, de manera que apoye, directamente, el progreso hacia dichos fines. En consecuencia, las políticas de seguridad planteadas en este proyecto, van de la mano con la visión y misión de la Universidad de Panamá.

Para la creación de una red inalámbrica que cubra las necesidades de los usuarios en cuanto a: calidad de servicio, confiabilidad y operacionalidad; es necesario, realizar un análisis exhaustivo de las instalaciones e infraestructura del entorno en el cual se va a montar la red, así como el diseño e implementación de metodologías de uso, calidad de servicio y seguridad, plasmadas en los propósitos de las red y en sus políticas de seguridad.

Para mejorar los niveles de seguridad el sistema de red inalámbrico, se propone un Reglamento de uso, en donde, se describen los pasos a seguir para ofrecer calidad de servicio y seguridad, tomando en cuenta las vulnerabilidades conocidas relacionadas a este medio de trasmisión.

RECOMENDACIONES

Para lograr un efectivo y buen uso de la red inalámbrica propuesta, es necesario implementar las recomendaciones que se exponen a continuación:

- Evaluar periódicamente el reglamento de uso de la red inalámbrica, tomando en cuenta los aspectos relacionados a: la implementación de normas educativas y estándares de uso de la red inalámbrica, para así brindar un servicio cónsono y actualizado a sus usuarios.

- Planificar la asignación de ancho de banda, balance de carga y calidad de servicio de la red inalámbrica, teniendo en cuenta: el tiempo promedio de la carga de las páginas visitadas, como también, la disponibilidad presupuestaria de la institución.

- Planificar la metodología de uso de la red inalámbrica, con base en las necesidades de los usuarios y de los estándares de calidad de servicio y seguridad que se pueden ofrecer dentro de la organización o empresa, a través de un manual de prácticas recomendadas que se sugieren a los usuarios.

- Mantener actualizados los controles de acceso a la red inalámbrica, así como el empleo eficiente de sus recursos, para ofrecer un servicio de calidad, con los controles de seguridad adecuados, a través del reglamento del uso de la red inalámbrica.

- Ofrecer a los usuarios de la red inalámbrica, herramientas de trabajo de actualizadas, que les permitan facilitar los procesos de enseñanza-aprendizaje en que se encuentran involucrados; al dotarlos de mecanismos tecnológicos acordes a la época actual.

REFERENCIAS BIBLIOGRÁFICAS

[BAAR79] **BALLESTEROS Elda C., ARMUELLES Pablo L.** *Senderos de Cultura*, Primera Edición, Órgano Informativo de la Universidad de Panamá, Panamá, 1979.

[BAGU95] **BATES, P Y MCGUFFIN, C.** *Redes de área Local*. Tercera edición, Editorial: McGraw Hill, España, 1995.

[BASU04] **BASURTO F. Lourdes.** *Red Inalámbrica: Nuevo Servicio De Calidad*. Fecha de Actualización: 2004-junio-15. Fecha de Consulta: 2008-Junio-3. Disponible en: http://www.ucol.mx/publicaciones/interfaces/suplemento%2076.pdf

[BASU04] **BASURTO F. LOURDES.** *Red Inalámbrica: Un Nuevo Servicio De Calidad*. Fecha de Actualización: 2004-junio-15. Fecha de Consulta: 2009-Julio-3. Disponible en: http://www.ucol.mx/acerca/coordinaciones/CGSTI/

[CARB07] **CARBALLAR, J.,** *WIFI*. Segunda edición, Editorial: Ra-ma, España, 2007.

[CISC05] **SANKAR, K., SUNDARALINGAM, S Y BALINSKY, A.** *Cisco Wireless LAN Security.* Primera Edición, Editoral: Cisco Press, Estados Unidos, 2005.

[CISYT02] **CISCO SYSTEMS, INC**. *Guía Del Segundo Año.* Segunda Edición. Cisco Systems, Inc. España. 2002.

[CISYT06] **CORPORACIÓN CISCO SYSTEMS, INC.** *Fundamentos De Redes Inalámbricas*. Tercera edición, Editorial: Pearson Educación, S.A., México, 2006.

[DETE04] **DEPARTAMENTO DE TELECOMUNICACIONES DE TECNOLOGÍA DE INFORMACIÓN DE UAG.** *Proyectos Wireless en la UAG*. Fecha de Actualización: 2004-junio-4. Fecha de Consulta: 2008-Junio-7. Disponible en: http://www.uag.mx/servicios/red_proyect.htm.

[DUTA09] **DUTARI, Raúl.** *Estructura De La Red Cableada De La FIEC-CRUV.* Encargado de Mantenimiento de los Laboratorios de Informática (Aulas A4, A5, A3), del Centro Regional Universitario de Veraguas. Fecha de Realización: 2009-Julio-23.

[EUNP08] **ESTATUTO UNIVERSITARIO GACETA OFICIAL 20226.** *Estatuto de la Universidad de Panamá.* Fecha de Consulta: 2010-Mayo-31. Disponible en: http://www.up.ac.pa/ftp/principal/transparencia/ESTATUTO-FINAL.pdf.

[FEFR11] **FRANCOIS, Felix.** *Características Primordiales Del Proyecto Internet Para Todos.* Encargado del Proyecto Internet Para Todos (Santiago, Soná, Ocú). Fecha de Realización: 2011-Mayo-17.

[GATM02] **GAST, M. 802.11** *Wireless Network: The Definitive Guide*. Primera Edición, Editorial O REILLY, Estados Unidos, 2002.

[IEEE09A] **IEEE.** *Status of Project IEEE 802.11 Task Group w* Fecha de Actualización: 2009-mayo. Fecha de Consulta: 2009-octubre-12. Disponible en: http://www.ieee802.org/11/Reports/tgw_update.htmz.

[IEEE09B] **IEEE.** *Wireless Fidelity – WiFi* Fecha de Actualización: 2009. Fecha de Consulta: 2009-octubre-14. Disponible en: http://www.ieee.org/portal/site/emergingtech/index.jsp?techId=4.

[MART04] **MARTÍNEZ, D.** *Comunicaciones Inalámbricas*. Segunda Edición, Editorial: Ra-ma. S.A., México, 2004.

[MART06] **MARTÍNEZ, D.** *Un Enfoque aplicado: Redes WIFI*. Segunda edición, Editorial: Ra-ma S.A., México, 2006.

[MEMO72] **ÁNONIMO.** *Memoria del 7 de febrero de 1972*, Primera Edición, Órgano Informativo de la Universidad de Panamá, Panamá, 1972.

[POWO08] **POOR V., WORNELL G.** *Wireless Communications Signal Processing Perspective.* Segunda Edición, Editorial: Prentice Hall, Estados Unidos, 1998.

[ROLE03] **ROSHAN P., LEARY J.** *802.11 Wireless LAN Fundamentals.* Primera Edición, Editorial: Cisco Press, Estados Unidos, 2003.

[SAMP05] **SAMPIERI, Roberto.** *Metodología de la Investigación*. Tercera edición, Editorial McGraw-Hill, México, 2005.

[STWI97] **STALLING J. WILLIAN.** *Comunicación y Redes de Computadoras*. Quinta Edición. Editorial: McGraw-Hill, México, 1997.

[TSVI04] **TSE D., VISWANATH P.** *Fundamentals Wireless Communications.* Primera Edición, Editorial: Cambridge University Press, Estados Unidos, 2004.

[UACH03] **UNIVERSIDAD AUSTRAL DE CHILE.** *Análisis teórico Practico de Redes Inalámbricas 802.11x y su implementación en base a WIFI.* Chile, 2003.

[UNIV10] **UNIVERSIDAD DE PANAMÁ.** *Visión y Misión* Fecha de Consulta: 2010-Julio-2. Disponible en: http://www.up.ac.pa/PortalUp/index.aspx.

[UPTO07] **UNIVERSIDAD DE PUERTO RICO.** *Política de Uso y Seguridad de la Red Inalámbrica.* Fecha de Consulta: 2010-Junio-11.

Disponible en: http://www.uprb.edu/politicas/PolItica_Uso_Seguridad_Red-Inalabrica.pdf

[WIKI09A] **FUNDACIÓN WIKIMEDIA.** *WIFI*. Fecha de Actualización: 2009-julio-05. Fecha de Consulta: 2009-Julio-3. Disponible en: http://es.wikipedia.org/wiki/WIFI.

[WIKI09B] **FUNDACIÓN WIKIMEDIA.** *IEEE 802.11*. Fecha de Actualización: 2009-julio-05. Fecha de Consulta: 2009-Septiembre-3. Disponible en: http://es.wikipedia.org/wiki/IEEE_802.11.

[WIKI10C] **FUNDACIÓN WIKIPEDIA.** *Tasa Interna de Retorno.* Fecha de actualización: 2010-Septiembre-08. Fecha de Consulta: 2010-Septiembre-28. Disponible en http://es.wikipedia.org/wiki/Tasa_interna_de_retorno.

[XOMB07] **XOMBRA TEAM.** *Seguridad en Wifi: pasos básicos para asegurar una WLAN*. Fecha de Actualización: 2007-octubre-15.Fecha de Consulta: 2009-Septiembre-6. Disponible en: http://www.xombra.com/go_articulo.php?nota=99

CAPÍTULO 5: APÉNDICES.

Tomando en cuenta el objetivo de la creación de la Red Inalámbrica para el Edificio A B del CRUV, se plantea el reglamento correspondiente, que tiene la finalidad de establecer los criterios que se deben respetar al utilizar este servicio educativo los estudiantes, profesores y administrativos del CRUV.

Adicionalmente, se incluye un glosario con las siglas y términos técnicos de uso no cotidiano, que se han utilizado en el desarrollo de esta investigación.

5.1 Reglamento Del Uso De La Red Inalámbrica Del Edificio A-B Del CRUV.

A continuación se detalla el reglamento de uso de la red inalámbrica que se basa en las políticas de uso y seguridad de la red **WIFI**, en base a la misión y visión de la Universidad de Panamá.

5.1.1 MISIÓN Y VISIÓN DE LA UNIVERSIDAD DE PANAMÁ.

La Universidad de Panamá, en la Gaceta Oficial 26202, donde se publica su Estatuto Universitario, define su visión como:

> *"Ser una institución reconocida y acreditada a nivel nacional e internacional, caracterizada por la excelencia en la formación de profesionales, integrada con la docencia, la investigación pertinente, el desarrollo tecnológico, la producción y la extensión, para contribuir al desarrollo nacional.* ***[UNIV10].***

Y su misión como:

> *"Institución de referencia regional en educación superior, basada en valores, formadora de profesionales emprendedores, íntegros, con conciencia social y pensamiento crítico; generadora de conocimiento innovador a través de la docencia, la investigación pertinente, la extensión, la producción y servicios, a fin de crear iniciativas para el desarrollo nacional, que contribuyan a erradicar la pobreza y mejorar la calidad de la vida de la población panameña"* **[UNIV10]**.

5.1.2 PROPÓSITO DE LA CREACIÓN DE LA RED INALÁMBRICA FORMULADA.

El propósito de esta red es el de ofrecer el servicio de comunicación de datos, de forma inalámbrica, a estudiantes y profesores del Centro Regional Universitario de Veraguas, para el área del Edificio A-B, sin la necesidad de utilizar un equipo fijo, de manera que les permita utilizar los servicios ofrecidos actualmente en la red existente de la FIEC.

5.1.2.1 PRIVACIDAD DE DIVULGACIÓN DE DATOS DE LOS USUARIOS.

Todo usuario de la red contará con el derecho de la privacidad y bajo ninguna circunstancia dará a conocer datos ni información de cualquier usuario antes de consultarlo con el mismo.

El derecho antes planteado no restringe que los administradores de la red supervisen el manejo que dan los usuarios a la red, para asegurar el buen uso del recurso.

5.1.2.2 REGULACIONES Y ESTÁNDARES.

- Los equipos que se instalen dentro de la red **WIFI**, deben ser compatibles con los estándares que establece **Modelo OSI**.

- Adicionalmente, los equipos deberán satisfacer el estándar **IEEE 802.11g** de comunicación inalámbrica, o el estándar que utilice la Universidad de Panamá.

5.1.2.3 LINEAMIENTOS DE USO DE LA RED INALÁMBRICA.

- Los estudiantes podrán tener acceso previa cancelación del aporte de B/.5.00 que cubre el semestre vigente.

- La Red Inalámbrica estará habilitada en horario laborable de la Universidad de Panamá.

- Los estudiantes Sigma Lambda, de todas las facultades del CRUV están exonerados del pago por el uso del servicio de la red inalámbrica, previa presentación del recibo de matrícula al Departamento de la Facultad de Informática, Electrónica y Comunicación.

- Se sancionará y restringirá el acceso a este servicio, a los usuarios que violen estos procedimientos.

- La Facultad de Informática, Electrónica y Comunicación podrá limitar o denegará el acceso a la red tanto de cable como la inalámbrica a los usuarios que infrinjan el reglamento de uso de la red.

Por otro lado, dentro de los aspectos que se deben consideran para la conexión de la red inalámbrica se señalan los siguientes:

- Los usuarios no deben compartir su conexión a la red con ningún otro usuario.

- Los usuarios no deben acceder a los recursos de comunicaciones restringidos, sin la debida autorización de los administradores.

- Los administradores no deben autorizar ningún acceso a la red, por parte de equipos que no estén registrados previamente.

- No se permite el acceso de los usuarios que están previamente a sitios webs que no estén destinados a fines académicos, de investigación o producción.

- Los administradores se reservan el derecho incondicional de suspender o rescindir el uso de la red inalámbrica.

En otro orden de ideas, tomando en cuenta aspectos de ética y moral que se deben seguir se tienen los siguientes:

- Se prohíbe la transmisión y la distribución de cualquier material discriminatorio para cualquier persona o grupo de personas.

- No se permite utilizar identidades falsas dentro de esta red.

- Se prohíbe el intercambio o manejo de la pornografía en todos sus géneros dentro de esta red.

Bajo la perspectiva de los equipos **WIFI**, se deben contemplar algunos aspectos:

- Los usuarios no deben modificar, dañar o mover los equipos de la red.

- No se debe generar ningún tipo de interferencia que afecten la calidad de la señal de la red inalámbrica.

Finalmente, desde el enfoque de la información y programas autorizados se deben tomar algunas consideraciones:

- Salvo que se realice bajo la supervisión de los profesores de la Facultad de Informática, Electrónica y Comunicación, dentro del marco de los fines de la Universidad de Panamá:

    - Los usuarios de la red no tienen permitido realizar rastreos de los equipos de la red inalámbrica.

- ❖ Los usuarios no pueden recolectar información que está siendo transmitida por otros usuarios de la red.

- ❖ Los usuarios no tienen permitido realizar monitoreos de comunicación entre los equipos que están utilizando la red.

- ❖ Los usuarios no tienen permitido buscar vulnerabilidades de la red inalámbrica.

5.2 Glosario.

- **ADSL**: En inglés, ADSL, son las siglas de Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica). La tecnología ADSL permite transformar el hilo de cobre del teléfono tradicional en una línea de gran capacidad de transmisión de datos y, al mismo tiempo, conservar el servicio de voz **[CISC05].**

- **AES**: También conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el Data Encryption Standard (DES) **[CISC05].**

- **Banda ISM**: Son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial,

científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WIFI **[CISC05].**

- **Card-Bus:** PC Card (originalmente **PCMCIA**), es un periférico diseñado para computadoras portátiles. En un principio era usado para expandir la memoria, pero luego se extendió a diversos usos como disco duro, tarjeta de red, tarjeta sintonizadora de TV, puerto paralelo, puerto serial, módem, puerto USB **[CISC05].**

- **CCK**: Es un sistema de modulación utilizado con las redes inalámbricas que emplean el IEEE 802.11b pliego de condiciones. En 1999, CCK fue adoptada para sustituir el código de Barker en redes inalámbricas digitales **[CISC05].**

- **CSMA/CA**: Acceso múltiple por detección de portadora con evasión de colisiones, es un **protocolo** de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión **[CISC05].**

- **DFS**: Frecuencia Dinámica de Selección, es una funcionalidad requerida por las WIFI que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles **[CISC05].**

- **DHCP**: Protocolo Configuración Dinámica de Servidor, es un protocolo de red que permite a los nodos de una red obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después **[STWI97].**

- **DNS**: En las consultas recursivas, consisten en la mejor respuesta que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. Las consultas iterativas, o resolución iterativa el servidor no tiene la información en sus datos locales, por lo que busca un servidor raíz y repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la respuesta a la pregunta **[CISC05].**

- **DSSS**: El espectro ensanchado por secuencia directa, en inglés: direct sequence spread spectrum, también conocido en comunicaciones móviles, acceso múltiple por división de código en secuencia directa, es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan **[CISC05].**

- **EDCA**: Sistema distribuido de control. Se basa en prioridades de tráfico. El tráfico más prioritario espera menos tiempo antes de emitir y utiliza marcos de tiempo de envío, más largos que el tráfico menos prioritario, que espera más antes de emitir y emite por menos tiempo **[CISC05].**

- **ESSID**: es un código incluido en todos los paquetes de una red inalámbrica, para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos **[CISC05].**

- **Estándar IEEE X**: es un estudio de estándares perteneciente al **IEEE**, que actúa sobre Redes de Ordenadores, concretamente y según su propia definición sobre redes de área local y redes de área metropolitana. También se usa el nombre IEEE 802 X para referirse a los estándares que proponen, y algunos de los cuales son muy conocidos: Ethernet (IEEE 802.3), o WIFI (IEEE 802.11), incluso está intentando estandarizar Bluetooth en el 802.15 **[CISC05].**

- **Ethernet:** es un estándar de redes de computadoras de área local con acceso al medio por contienda, mejor conocido como **CSMA/CA**. El nombre viene del concepto físico de *ether* **[CISC05]**. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo **Modelo OSI [STWI97].**

- **ETSI**: El Instituto Europeo de Normas de Telecomunicaciones, es una organización independiente, sin fines de lucro, organización de normalización en la industria de las telecomunicaciones fabricantes de equipos y operadores de red en Europa, con proyección a nivel mundial **[STWI97].**

- **FCC:** Es una agencia del gobierno de Estados Unidos. La FCC fue establecida por la Ley de Comunicaciones de 1934 y se encarga de regular las comunicaciones interestatales e internacionales por radio, televisión, cable, satélite y cable. La jurisdicción de la FCC cubre los 50 estados, el Distrito de Columbia, y posesiones de los EE.UU**[CISC05].**

- **HCCA:** Hybrid Coordinador de la función, llamado al Acceso al Canal Controlado HCF (HCF Hybrid Controlled Channel Access, HCCA), este controla el acceso al canal con el fin de proveer una calidad de servicio basada en parámetros **[CISC05].**

- **IEEE 802.11**: El estándar IEEE 802.11 o WIFI de IEEE que define el uso de los dos niveles inferiores de la arquitectura de capas física y de enlace de datos, especificando sus normas de funcionamiento en una red inalámbrica. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana **[CISC05].**

- **IEEE**: Corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos,

una asociación técnico-profesional mundial dedicada a la estandarización entre otras cosas **[STWI97].**

- **ITU**: La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras **[STWI97].**

- **MAC**: El control de acceso al medio, es un conjunto de mecanismos y protocolos por los que varios "interlocutores", ya sean dispositivos en una red, como ordenadores, teléfonos móviles, etc.; se ponen de acuerdo para compartir un medio de transmisión común **[STWI97].**

- **MIMO**: Múltiples entradas Múltiples Salidas, se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores. En el formato de transmisión inalámbrica tradicional la señal se ve afectada por reflexiones, lo que ocasiona degradación o corrupción de la misma y por lo tanto pérdida de datos **[CISC05].**

- **Mini-PCI**: Interconexión de Componentes Periféricos, consiste en un bus de ordenador estándar para conectar dispositivos periféricos directamente a su placa base. Es común en PC, donde ha desplazado al bus estándar, pero también se emplea en otro tipo de ordenadores **[STWI97].**

- **Modelo OSI:** El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection), fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones **[STWI97].**

- **NIC:** Se le denomina como, Tarjeta de red, se suele asociar a una tarjeta de expansión insertada en una ranura interna de un ordenador o impresora, se suele utilizar para referirse también a dispositivos embebidos en la placa madre del equipo, como las interfaces presentes en la videoconsola Xbox o los modernos notebooks **[STWI97].**

- **OFDM**: Es una tecnología que transmite múltiples señales simultáneamente sobre un solo medio de transmisión, como un cable o el aire. Cada señal viaja con su propio y único rango de frecuencia (portadora), el cual es modulado por los datos (sean de texto, voz, vídeo, etc.)**[STWI97].**

- **PA**: es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un cifrado **WAP**. también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos **[CISC05].**

- **PCMCIA:** es el acrónimo de *Personal Computer Memory Card International Association*, una asociación Internacional centrada en el desarrollo de tarjetas de memoria para ordenadores personales que permiten añadir al ordenador nuevas funciones. Existen muchos tipos de dispositivos disponibles en formato de tarjeta PCMCIA: módems, tarjeta de sonido, tarjeta de red **[WIKI10C].**

- **PHY**: Se refiere al nivel físico provee el servicio de transmisión de datos sobre el medio físico propiamente dicho, así como la interfaz con la entidad de gestión del nivel físico, por medio de la cual se puede acceder a todos los servicios de gestión del nivel y que mantiene una base de datos con información de redes de área personal relacionadas **[STWI97].**

- **QoS**: Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput) **[CISC05].**

- **RC4**: Dentro de la criptografía RC4 o ARC4 es el sistema de cifrado de flujo Stream cipher 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**. Fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a

ser un sistema de criptografía muy inseguro, incluyendo su uso en **WEP [CISC05].**

- **Router:** Enrutador, encaminador. Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del **Modelo OSI**. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red **[CISC05].**

- **SNMP**: El Protocolo Simple de Administración de Red o **SNMP** es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red **[TSVI04].**

- **SSID:** Service Set IDentifier, es un código incluido en todos los paquetes de una red inalámbrica (WIFI) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID **[TSVI04].**

- **Switch:** Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame **[CISC05].**

- **TCP:** Protocolo de Control de Transmisión, garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir

distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto **[STWI97].**

- **VPN:** La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet **[CISC05].**

- **WIFI:** Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica, que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz. es una marca de la *WIFI Alliance* (anteriormente la *WECA: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local **[CISC05].**

- **WRAP:** The Wireless Router Application Platform**,** es un formato de ordenador, definido por la empresa suiza de PC Engines. Esto es especialmente diseñado para el enrutador inalámbrico, firewall, balanceador de carga, **VPN** o de otros dispositivos de red. Tres partes han presentado en materia de patentes para WRAP. Estas cuestiones de propiedad intelectual patentado en **IEEE** para introducir **CCMP** en el estándar 802.11i WRAP **[CISC05].**

- **XOR**: La puerta lógica **O-exclusiva**, más conocida por su nombre en inglés *XOR*, realiza la función booleana A'B+AB'. Su símbolo es el más (+) inscrito en un círculo. En la figura de la derecha pueden observarse sus símbolos en electrónica **[CISC05].**

- **TFTP:** Es un protocolo de transferencia muy simple semejante a una versión básica de **FTP** a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red **[CISC05].**

- **FTP**: File Transfer Protocol, Protocolo de Transferencia de Archivos, en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red basado en la arquitectura cliente-servidor **[STWI97].**

- **TKIP:** Temporal Key Integrity Protocol, es también llamado hashing de clave **WEP** y **WPA**, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. **WPA** tiene TKIP, que utiliza el mismo algoritmo que **WEP**, pero construye claves en una forma diferente **[CISC05].**

- **TPC:** Transmitter Power Control, es una funcionalidad requerida por las WIFI, que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite **[STWI97].**

- **UDP:** Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera **[[CISC05].**

- **WECA:** Wireless Ethernet Compatibility Alliance, es una empresa creada en 1999 con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse WIFI Alliance. **[CISC05].**

- **WEP:** (Privacidad Equivalente a Cableado), es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite **[CISC05].**

- **RADIUS:** Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 **UDP** para establecer sus conexiones **[CISYT06].**

- **WPA:** Sus siglas corresponden a: acceso inalámbrico protegido, una solución de seguridad inalámbrica, ofrecida por: WiFi Alliance para solucionar las carencias de **WEP**. Definida bajo el protocolo 802.11i que depende de protocolos de autenticación y de un algoritmo de cifrado cerrado: El **TKIP** genera claves aleatorias y, para lograr mayor seguridad, puede alterar varias veces por segundo una clave de cifrado **[CISC05].**

- **WAP:** Protocolo de aplicaciones inalámbricas, es un estándar internacional abierto para la aplicación de comunicaciones de red de capa en un ambiente de comunicación inalámbrica. La mayoría de uso de WAP incluye el acceso a la web móvil desde un teléfono móvil. Un navegador WAP proporciona todos los servicios básicos de un equipo basado en navegador web **[CISC05].**

- **CCMP:** Se le conoce como parte de IEEE 802.11i, un protocolo de cifrado creado para reemplazar tanto **TKIP**, el protocolo obligatorio en **WPA** y **WEP**, cuanto antes, el protocolo inseguro. CCMP es una parte obligatoria del estándar WPA2: una segunda parte de **WPA** , una parte opcional del estándar **WPA**, y una opción necesaria para Robust Security Network**[STWI97]**.

- **RF:** La Radio Frecuencia, se define por medio de la forma que se presente: por modulación y radiación de ondas electromagnéticas, transmisor-receptor utilizado para la comunicación o en términos generales aplicados al uso de ondas de radio **[CISYT06].**

- **UTP:** El cable de par trenzado, es una forma de conexión en la que dos aisladores son entrelazados para darle mayor estética al terminado del cable y aumentar la potencia y la diafonía de los cables adyacentes **[STWI97].**

- **VLAN:** Son redes de área local virtuales o VLAN. Las VLAN permiten a los administradores de red evitar la transmisión de mensajes de multicast y broadcast innecesarios a través de una red **[CISYT06].**