



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

**Diseño técnico – económico de un sistema de video vigilancia IP,
mediante el uso de una red de internet comunitaria que utiliza
tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil.**

AUTOR:

Moncayo Quispe, Victor Emilio

Trabajo de Titulación previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES

TUTOR:

Alvarado Bustamante, Jimmy Salvador

Guayaquil, Ecuador

07deMarzodel 2018



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr.
Moncayo Quispe, Victor Emilio como requerimiento para la obtención del
título de **INGENIERO EN TELECOMUNICACIONES.**

TUTOR

Alvarado Bustamante, Jimmy Salvador

DIRECTOR DE CARRERA

Heras Sánchez, Miguel Armando

Guayaquil, a los 7 días del mes de Marzo del año 2018



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Moncayo Quispe, Victor Emilio**

DECLARO QUE:

El trabajo de titulación “**Diseño técnico – económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil**” previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 07 días del mes de Marzo del año 2018

EL AUTOR

MONCAYO QUISPE, VICTOR EMILIO



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Moncayo Quispe, Victor Emilio**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **“Diseño técnico – económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil”**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 07 días del mes de Marzo del año 2018

EL AUTOR

MONCAYO QUISPE, VICTOR EMILIO

REPORTE URKUND

URKUND

Documento	Tesis Victor Moncayo .docx (D36531680)
Presentado	2018-03-14 15:40 (-05:00)
Presentado por	victor.94.a@outlook.com
Recibido	edwin.palacios.ucsg@analysis.orkund.com
Mensaje	victor moncayo Mostrar el mensaje completo 2% de estas 31 páginas, se componen de texto presente en 6 fuentes.

Lista de fuentes	Bloques		
+	Categoría	Enlace/nombre de archivo	☐
+		http://www.cedatos.com.ec/detal...	☑
+		tesis Rosa Vinueza para el urk.docx	☑
+		http://pleasenetworks.com/blog/...	☑
+		Tesis Final Klvr.docx	☑
+		tesis final.docx	☐

Reiniciar Exportar Compartir

0 Advertencias

UNIVERSIDAD CATÓLICA DE SANTIAGO DE
GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA
PARA EL DESARROLLO CARRERA DE INGENIERÍA EN
TELECOMUNICACIONES

TEMA:

Diseño técnico – económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza la tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil.

AUTOR: Victor Emilio Moncayo Quispe

Trabajo de Titulación previo a la obtención del grado de INGENIERO EN TELECOMUNICACIONES

TUTOR: Alvarado Bustamante, Jimmy Salvador

AGRADECIMIENTO

Quiero agradecer profundamente a Dios, por regalarme la vida y salud para culminar con éxito uno de mis sueños anhelados, el poder culminar mis estudios universitarios.

Mis más sinceros agradecimientos a la Universidad Católica de Santiago de Guayaquil en especial a la Facultad Educación Técnica para el Desarrollo y a cada uno de los profesores que supieron guiarme a través de todo este tiempo con sus enseñanzas, para poder culminar con éxito mi carrera universitaria.

Al Ing. Jimmy Alvarado Bustamante con su acertada dirección para poder culminar con éxito el presente proyecto.

A mis familiares y en especial a mi querida madre quien ha sido mi apoyo y mi soporte en cada situación adversa que he tenido en este largo camino.

Reconocimiento especial a la Comunidad de la Ciudadela Álamos Norte por la apertura brindada para la realización de este trabajo de Titulación.

EL AUTOR

MONCAYO QUISPE, VICTOR EMILIO

DEDICATORIA

A Dios, por haberme guiado correctamente en este camino tan arduo a la obtención del título.

A mi familia, por darme las fuerzas y el ánimo en el momento justo que más lo necesitaba.

De igual manera, a los docentes por brindarme los conocimientos necesarios a lo largo de la carrera.

EL AUTOR

MONCAYO QUISPE, VICTOR EMILIO



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ROMERO PAZ, MANUEL DE JESÚS

DECANO

f. _____

PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DE TITULACIÓN

f. _____

PALAU DE LA ROSA, LUIS EZEQUIEL

OPONENTE

Índice General

Índice de Figuras	XII
Índice de Tablas	XIV
Resumen.....	XV
Abstract.....	XVI
CAPITULO 1: DESCRIPCIÓN DEL TRABAJO DE TITULACIÓN	17
1.1. Introducción.	17
1.2. Antecedentes.....	18
1.3. Justificación del problema.....	18
1.4. Definición del problema.	19
1.5. Objetivos.....	19
1.5.1. Objetivo general	19
1.5.2 Objetivos específicos.....	19
1.6. Hipótesis.....	19
1.7. Metodología de investigación.....	19
CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA.....	21
2.1. Conceptos de radiocomunicación.	21
2.1.1. Radiofrecuencia.....	21
2.1.2. Frecuencia.....	21
2.1.3. Interferencia.	21
2.2. Onda Electromagnética	21
2.2.1. Características fundamentales.	22
2.3. Redes Inalámbricas.	22
2.3.1. Tipos de Redes Inalámbricas.	22
2.4. Redes inalámbricas de área local (Wlan).....	24
2.4.1 HistoriaWlan.	24
2.4.2. Estándar IEEE 802.11.	25
2.4.3 Protocolos.	27
2.5. Arquitecturas con Redes WI-FI.	29
2.6 Arquitecturas básicas de despliegues.	30
2.7. Topologías de las redes Inalámbricas.....	31
2.8. Definición de Antena.....	33
2.8.1. Clasificación de las Antenas.....	34
2.9. Antenas Inteligentes.	34

2.10. Principios de Funcionamiento.	35
2.11. Tipos de antenas inteligentes.	35
2.12. Antenas MIMO.	36
2.13. Ventajas redes inalámbricas.	37
2.14 Seguridad Redes Inalámbricas.	38
2.14.1. Cifrado WEP.	39
2.14.2. Cifrado WPA.	39
2.14.3. Cifrado WPA2.	39
2.15. Concepto video vigilancia.	39
2.16. Tipos de cámara.	40
2.17. Aplicaciones.	41
2.18. Funciones cámaras IP.	42
2.19. Sistemas NVR / DVR.	43
2.19.1. Características similares de DVRs Y NVRs.	43
2.19.2. Características Contrastantes de un NVR y DVR.	44
2.20. Comparando los sistemas DVR / NVR.	44
CAPÍTULO 3: ANÁLISIS DE LA PROPUESTA DEL PROYECTO	46
3.1. Análisis de la situación delincriminal actual del país y de la ciudad.	46
3.2. Datos Estadísticos a nivel delincriminal en el Ecuador.	46
3.3. Uso de la tecnología en el Ecuador.	49
3.4. Criterios técnicos y de ingeniería para el diseño técnico - económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza la tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil.	52
3.5. Calculo de ancho de banda que se necesitara.	53
3.6. Calculo de la capacidad de almacenamiento para la elección de NVR.	55
3.7. Análisis de proveedor de servicio.	56
3.8. Criterio y análisis técnico para la elección de equipos.	57
3.8.1. Antena Tp-Link modelo TL-ANT2415D.	58
3.8.2. POE Ubiquiti.	59
3.8.3. Access point Ubiquiti modelo Bullet M2-HP.	59
3.8.4. Cámaras IP Hikvision modelo DS-2CD2020F-I (W).	62
3.8.5. NVR Hikvision modelo DS-7600NI-I2 / 16P.	63
3.9. Configuración de parámetros del Bullet M2-HP.	65

3.10. Configuración de NVR con las cámaras IP.	67
3.11. Esquema de equipos a implementar para abarcar el área total.	71
3.12. Diseño final de la Red comunitaria con camaras IP.	72
3.13. Aplicaciones para monitorear las cámaras online	74
3.14. Procedimiento en caso de un robo.....	74
3.15. Costo aproximando de equipos a utilizarse.....	75
CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES.....	77
4.1. Conclusiones.	77
4.2. Recomendaciones.	78
REFERENCIAS BIBLIOGRÁFICAS.....	79

Índice de Figuras

Capítulo 2

Figura 2.1: Vinculación entre Amplitud, Longitud de onda y Frecuencia.	22
Figura 2.2: Tipo de redes inalámbricas	23
Figura 2.3: Enlace Punto a Punto entre dos edificios.....	32
Figura 2.4: Enlace Punto a Multipunto	32
Figura 2.5: Enlace Multipunto a Multipunto	33
Figura 2.6: Formación de haz de antena inteligente	36
Figura 2.7: Router WI-FI con tres antenas	37

Capítulo 3

Figura 3.1: Porcentaje de personas que han sufrido algún tipo de delito.	46
Figura 3.2: Porcentaje de personas que consideran su barrio seguro	47
Figura 3.3: Porcentaje de principales problemas de seguridad.....	48
Figura 3.4: Porcentaje de posibles soluciones por parte de la población	48
Figura 3.5: Estadísticas de robos en la ciudadela Álamos Norte de Guayaquil.....	49
Figura 3.6: Porcentaje de hogares con teléfono fijo y móvil a nivel nacional	50
Figura 3.7: Porcentaje de hogares con acceso a internet a nivel nacional ...	51
Figura 3.8: Área de la red Comunitaria con Cámaras IP	53
Figura 3.9: Antena omnidireccional TP-Link modelo TL-ANT2415D.	59
Figura 3.10: POE de Ubiquiti.	59
Figura 3.11: Bullet M2 Hp para exterior de Ubiquiti.....	60
Figura 3.12: Diagrama de la conexión de los quipos.....	61
Figura 3.13: Cámara IP Hikvision modelo DS-2CD2020F-I (W).....	62
Figura 3.14: NVR de la marca Hikvision modelo DS-7600NI-I2 / 16P	63
Figura 3.15: Conexión de equipos al NVR modelo DS-7600NI-I2 / 16P.....	65
Figura 3.16: Configuración del Bullet M2-HP interfaz WIRELESS	66
Figura 3.17: Interfaz de seguridad del Bullet M2-HP	67
Figura 3.18: Ingreso de clave para NVR.	67
Figura 3.19: Habilitación del monitoreo por App.	68
Figura 3.20: Grabación entre continua o por detección de movimiento.....	68
Figura 3.21: Configuración de parámetros del NVR.....	68

Figura 3.22: Configuración de cámara IP.....	69
Figura 3.23: Establecimiento de parámetros de cámaras IP.	69
Figura 3.24: Visualización de cámaras en el NVR.	70
Figura 3.25: Ubicación estratégica de equipos.	71
Figura 3.26: Cobertura total del área	72
Figura 3.27: Diseño final de la Red comunitaria con cámaras IP	73

Índice de Tablas

Capítulo 2

Tabla 2.1: Frecuencias y alcances del estándar 802.11	26
Tabla 2.2: Tabla con la clasificación de las antenas	34

Capítulo 3

Tabla 3.1: Formato de trama Ethernet	53
Tabla 3.2: Campo de datos de la trama Ethernet.....	54
Tabla 3.3: Especificaciones antena TP-Link modelo TL-ANT2415D.	58
Tabla 3.4: Especificaciones Bullet M2-HP	60
Tabla 3.5: Especificaciones cámara IP DS-2CD2020F-I (W).	62
Tabla 3.6: Especificaciones NVR DS-7600NI-I2/16P	64
Tabla 3.7: Direcciones IP de cada cámara IP.	70
Tabla 3.8: Costos aproximado de equipos para el proyecto.....	75

Resumen

La inseguridad en la ciudad de Guayaquil es una realidad que se vive en el sector de Los Álamos, entre los delitos que destacan están robos, asaltos y asesinatos, siendo un tema de preocupación para la población, demandando un sistema de aviso efectivo en caso de que se produce el delito, capturando a los causantes y con ello bajar el índice delictivo en la zona. Este trabajo de titulación tiene el objetivo principal de diseñar un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza la tecnología de acceso WI-FI para que la comunidad se sienta más segura en sus hogares y por medio de la red de internet este más comunicados, se abordaran temas como las redes inalámbricas, seguridad de las redes, cámara IP, equipos de almacenamiento, comparaciones, topología de redes y antenas. En este proyecto se decidió utilizar doce cámaras IP para monitoreo, una antena TP-Link con un equipo Bullet M2-HP el cual será nuestro punto de acceso una vez configurado, usaremos una red con un ancho de banda de 50 Mbps para que a su vez tenga la capacidad de soportar las cámaras IP a usar, el costo de la propuesta es asumido por los moradores del sector con una cuota por dos meses de \$ 37.40 con una participación de 37 familias.

Palabras Clave: **WI-FI, RED, COMUNITARIA, INALÁMBRICA, VIDEO VIGILANCIA, IP.**

Abstract

The insecurity in the city of Guayaquil is a reality that lives in the Los Alamos sector, among the crimes that stand out are robberies, assaults and murders, being a subject of concern for the population, demanding an effective warning system in case it produces the crime, capturing the perpetrators and thereby lowering the crime rate in the area. This title work has the main objective of designing an IP video surveillance system, through the use of a community internet network that uses WI-FI access technology to make the community feel more secure in their homes and through of the Internet network this more communicated, will address issues such as wireless networks, network security, IP camera, storage equipment, comparisons, network topology and antennas. In this project we decided to use twelve IP cameras for monitoring, a TP-Link antenna with a Bullet M2-HP device which will be our access point once configured, we will use a network with a bandwidth of 50 Mbps so that its Once it has the capacity to support the IP cameras to use, the cost of the proposal is assumed by the residents of the sector with a fee for two months of \$ 37.40 with a participation of 37 families.

Keywords: **WI-FI, NETWORK, COMMUNITY, WIRELESS, VIDEO VIGILATION, IP.**

CAPITULO 1: DESCRIPCIÓN DEL TRABAJO DE TITULACIÓN

1.1 Introducción.

La tecnología de redes inalámbricas ofrece un servicio eficaz y rápido, principalmente si se la usa como una herramienta que ayude a alertar a los moradores de una comunidad, en un problema en común que tienen relacionado a la inseguridad de sus alrededores, a raíz de ese suceso se propone el diseño de un sistema de video vigilancia con cámara IP, destinado para la Ciudadela Álamos Norte de la Ciudad de Guayaquil, identificado como el sujeto de estudio.

Una red inalámbrica es una tecnología que permite conectar equipos sin la necesidad de cables o algún material físico, empleando ondas electromagnéticas para entablar una comunicación, propuesta ideal si se espera contar con un sistema de vigilancia que pase desapercibido frente a personas extrañas o ajenas a una comunidad.

En el proyecto se hace uso de la red comunitaria inalámbrica de área local por sus siglas WLAN, que emplea la tecnología WI-FI, siendo la abreviatura de Wireless Fidelity (Fidelidad Inalámbrica). WI-FI es la tecnología de comunicación inalámbrica más popular en la actualidad debido a que es compatible con la mayoría de equipos inalámbricos, esta tecnología se propaga por medio de ondas electromagnéticas, se puede encontrar dos tipos de comunicación: WI-FI: 802.11b, que emite a 11 Mb/seg., y 802.11g, más rápida, a 54 Mb/seg.

Un sistema de video vigilancia IP, el cual se trata de tener equipos de monitoreo (cámaras IP, NVR, etc.), en puntos estratégicos para poder captar en video lo que esté ocurriendo, en el área que se requiera cubrir. Como propósito de estudio se planeó diseñar un sistema de video vigilancia IP, mediante el uso de una red comunitaria WI-FI para la ciudadela Álamos Norte de Guayaquil, que ayude a la seguridad y comunicación de la comunidad.

1.2 Antecedentes.

En la actualidad las comunicaciones caracterizan su importancia, por la rapidez con la que se puedan brindar y facilitar el intercambio de información, lo cual posibilita que las personas reaccionen ante cualquier eventualidad, más aún si se enfrentan ante un problema de inseguridad, cuya reacción debe ejecutarse al instante, para salvaguardar la integridad de la persona agredida; con el presente proyecto se trata de demostrar la utilidad del internet como parte de un sistema que mejora la calidad de vida de los habitantes de una población, las cuales son víctimas de actos delincuenciales, evitando que los moradores puedan desarrollar sus actividades con normalidad y mantengan un ambiente de incertidumbre ante la falta de vigilancia de las autoridad de control. La lejanía de Unidad de Policía Comunitaria por sus siglas UPC en el sector Los Álamos ha generado que personas inescrupulosas, conviertan a la comunidad en víctima de sus fechorías, siendo catalogada como una de las zonas más peligrosas en el sector.

1.3 Justificación del problema.

Los moradores de los Álamos aportan con \$20.00 por concepto de pago de seguridad, fondo que es administrado por un Comité Barrial con la finalidad de contar con protección privada, ya que en los alrededores de la zona no cuentan con un UPC de Policía Comunitaria que acuda en su auxilio frente a robos y asaltos ocurridos en el sector, los cuales son cada vez más frecuentes.

Ante esta situación en la actualidad se ha implementado una puerta eléctrica, la cual trataba de servir como un sustituto a la contratación de la seguridad privada debido a su alto costo por concepto de guardianía, sin embargo, los resultados han sido poco efectivos, la reacción frente al tema delictivo es lenta, los moradores salen una vez que el delito ha sido cometido, sin que se atrape a los culpables. Por lo cual los habitantes del sector están buscando una alternativa que evite incrementar un gasto

mensual pero que sea del todo efectivo para que reduzca el problema de la inseguridad en el sector.

1.4. Definición del problema.

La ciudadela Álamos Norte de la ciudad de Guayaquil, carece de un sistema de video vigilancia IP, mediante el uso de una red comunitaria de acceso WI-FI, que permita facilitar la comunicación, seguridad, y atención oportuna en el momento de un acto delictivo, teniendo como resultado la tranquilidad y el confort los habitantes de la ciudadela.

1.5. Objetivos

1.5.1. Objetivo general

Realizar un diseño técnico – económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza la tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil.

1.5.2. Objetivos específicos

- Analizar las necesidades de los Álamos en tema de seguridad para la implementación de un sistema de video vigilancia IP.
- Definir el número de equipos necesarios para el diseño de la red WI-FI y cámaras de seguridad IP.
- Realizar un análisis costo beneficio del sistema de video vigilancia IP en la ciudadela Álamos Norte de Guayaquil.

1.6. Hipótesis.

La propuesta de un sistema de video vigilancia IP dentro de la ciudadela Álamos Norte de Guayaquil, permitirá que disminuya su índice delincencial, porque pone en alerta a toda una comunidad ante cualquier acto de robo que ocurra con un morador, además beneficiará proporcionando un ambiente de tranquilidad y mejoramiento de la calidad de vida en el tema de seguridad a los hogares.

1.7. Metodología de investigación.

La metodología que se utilizó en este trabajo de titulación tendrá una visión: descriptivo, deductivo y explicativo.

- Descriptivo, se considerará la situación actual tanto en la seguridad como en el uso de la tecnología para enfocarse en puntos específicos.
- Deductivo, determinaremos equipos y tecnología necesarios para diseñar la red comunitaria con sistema de video vigilancia IP.
- Explicativo, en este trabajo de titulación se propondrán soluciones al problema de inseguridad.

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA.

2.1. Conceptos de radiocomunicación.

2.1.1. Radiofrecuencia.

Las señales de radio de particulares ejemplo radio pueblan el espectro de radio en ocho bandas de frecuencia, comenzando en 3 Kilo Hertz, y extendiéndose hasta frecuencia extremadamente alta, terminando en 300 Giga Hertz (EncyclopediaBritannica, 2013).

2.1.2. Frecuencia.

Según el (Instituto Federal de Telecomunicaciones, 2015), se puede definir a la frecuencia como el número de ciclos por segundo que ejecuta una onda del espectro radio eléctrico, la frecuencia se la mide en Hertz.

2.1.3. Interferencia.

Es cualquier perturbación en la recepción de una señal en forma natural o artificial (hecha por el hombre) causada por señales indeseables (Regalado, 2013).

2.2. Onda Electromagnética

Se denomina a la onda como la transmisión de energía sin la necesidad del desplazamiento de materia (Orange, 2016). También, se la define como una perturbación que se desplaza de forma normal en un ambiente determinado, que luego volverá a su estado inicial (Weston & Lewis, 2005).

En la vida cotidiana la energía que se transporta sin la necesidad de algún tipo de materia es más común de lo que se cree, un ejemplo de esto sería, que si en un lago totalmente en calma sin nada de viento, la superficie se encontrara completamente lisa, de repente una ave sale volando de una árbol y hace caer una rama al agua, lo que provoca un impacto y como consecuencia inmediatamente genera ondulaciones que parecen alejarse circularmente del punto de impacto, luego de un momento el agua del lago estará nuevamente lisa e inmóvil.

2.2.1. Características fundamentales.

Según (Orange, 2016) se puede describir a todas las ondas por medio de tres características las cuales tienen un vínculo como se muestra en la figura 2.1 a continuación:

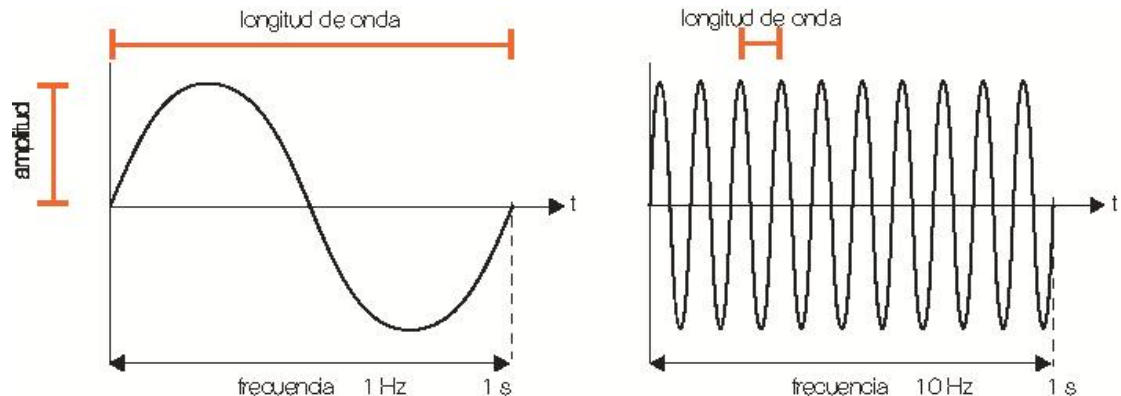


Figura 2.1: Vinculación entre Amplitud, Longitud de onda y Frecuencia.

Fuente: (Orange, 2016)

- **amplitud** nos dará la altura de las ondulaciones.
- **longitud de onda** nos permite medir el recorrido entre dos ondulaciones.
- **frecuencia** básicamente es el número de ondulaciones por segundo.

2.3. Redes Inalámbricas.

Comunicación inalámbrica se llama a aquella que se lleva sin el uso de cables de interconexión entre los usuarios; por ejemplo, un intercambio de información con teléfono móvil por medio de bluetooth que es transmisión de datos inalámbrica, mientras que una comunicación que se lleva a cabo con teléfono fijo tradicional no lo es (Orange, 2016).

2.3.1. Tipos de Redes Inalámbricas.

Para (Camargo, 2014), las redes inalámbricas se las pueden clasificar de algunas maneras esto dependerá del criterio al que se desee. En este caso, se clasifican dependiendo de su alcance como se muestra en la figura 2.2, las comunicaciones inalámbricas de acuerdo con su alcance se dividen en los siguientes grupos:

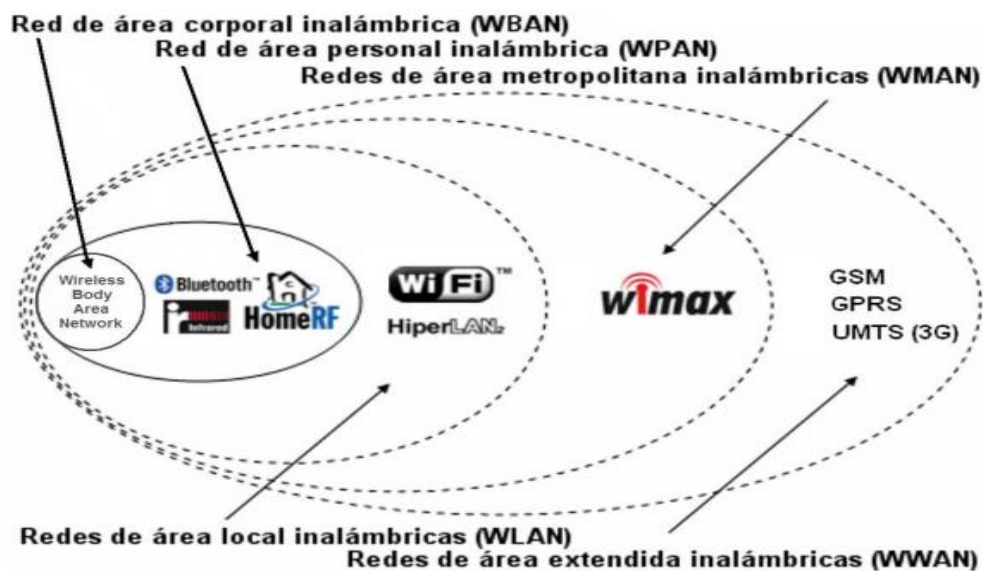


Figura 2.2: Tipo de redes inalámbricas

Fuente: (Camargo, 2014)

- Redes inalámbricas de área corporal (Wireless Body Area Network, WBAN) cubren distancias de 1 o 2 metros.
- Redes inalámbricas de área personal (Wireless Personal Area Network, WPAN) son las que cubren distancias por debajo de los 10 metros. Estas soluciones están pensadas para interconectar los distintos dispositivos de un usuario (por ejemplo, la laptop con la impresora). Éste es el caso de la tecnología Bluetooth o de IEEE 802.15.
- Redes inalámbricas de área local (Wireless Local Area Network, WLAN) cubren distancias de unos cientos de metros. Estas redes fueron creadas con el fin de tener una relación de red local entre ordenadores o terminales situados en un mismo lugar o en varios lugares. Éste es el caso de WI-FI.
- Redes inalámbricas de área metropolitana (Wireless Metropolitan Area Network, WMAN) pretenden cubrir el área de una ciudad o entorno metropolitano. Los protocolos de sistema de distribución local multipunto (Local Multipoint Distribution Service, LMDS) o el servicio multicanal de distribución multipunto (Multichannel Multipoint Distribution Service, MMDS) ofrecen soluciones de este tipo.
- Redes inalámbricas de área extensa (Wireless Wide Area Network, WWAN), también conocidas como de área global, pueden cubrir toda

una región (ciudades o países). Estas redes se basan en tecnología celular y han aparecido como evolución de las redes de comunicaciones de voz. Éste es el caso de las redes de telefonía móvil más conocidas como 2,5G o 3G y en la actualidad 4G LTE. En este trabajo de investigación estará más enfocado en lo que es la red inalámbrica Wlan. La cual estudiara más a fondo.

2.4. Redes inalámbricas de área local (Wlan).

Las Redes inalámbricas de área local o WLAN, como ya se ha estado diciendo en esta investigación cubren ciertas distancias. Esta más enfocada para una red de un mismo sitio o de un grupo, en este caso WI-FI.

2.4.1 Historia Wlan.

En 1888 el físico alemán Rudolf Hertz fue el primero que ejecuto una transmisión totalmente libre de cables por medio de ondas electromagnéticas con en uso de un oscilador, el cual tuvo la función de emisor y un resonador que hacía de receptor. Después de seis años, las ondas de radio fueron tomando popularidad y comenzaron a ser un medio de comunicación (Garreta, 2017).

Se dice que en 1899 Marconi fue quien implemento las primeras comunicaciones inalámbricas las cuales fueron realizadas por el canal de la Mancha. Así mismo en 1907, fue la fecha en donde se pudo transmitir atravesando el Atlántico el primer mensaje completo. Por otra parte, el primer sistema de comunicación que se desarrolló en las instalaciones de la Universidad de Hawái, esto lo pudieron lograr gracias a una red de comunicación por radio, en el año de 1971. Aquella comunicación es considerada la primera red local inalámbrica (WLAN) (Garreta, 2017).

En la actualidad vivimos en una sociedad rodeada con las tecnologías inalámbricas de comunicaciones aquello desde principios de los 90, aunque al principio se pensó que sería una pérdida de tiempo y un total desastre, esto debido a que los fabricantes desarrollan los modelos a su gusto, lo cual no hacia incompatible con otros modelos. Y es algo que gasta en la

actualidad no existe un estándar universal, para que puedan trabajar todos los equipos bajo un mismo sistema, la única solución es acoplar la App de cada equipo a las diversas clases del lenguajes y de los diferentes sistemas operativos que sean necesarios(Garreta, 2017).

2.4.2. Estándar IEEE 802.11.

IEEE 802.11 es un estándar para redes inalámbricas definido por el Institute of Electrical and Electronics Engineers (IEEE). Se trata de un instituto de investigación y desarrollo, de gran reconocimiento y prestigio, cuyos miembros pertenecen a decenas de países entre profesores y profesionales de las nuevas tecnologías. En referencia a (Yunquera, 2014), en su tesis Diseño de una red WI-FI para la E.S.I. Define a el estándar IEEE 802.11, como un estándar en continua evolución, debido a que existen muchos grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales.

La primera versión del estándar fue creada en el año de 1997, aunque el comité evaluador fue creado en 1990. Esta versión se trataba de ofrecer algunas alternativas para interconectar computadoras y otros tipos de dispositivos, sin el requisito de utilizar cables. Esta primera versión de 1997 vista hoy, está obsoleta, pero ha marcado un principio para una tecnología prometedora.

Al principio, el 802.11 se creó pensando para únicamente para redes locales inalámbricas (WLAN) de corto alcance, pero la necesidad de comunicar dispositivos portátiles a gran velocidad de transmisión ha generado el plantear e incluso llegar a la creación de redes inalámbricas que permitan llegar a una mayor extensión, en la tabla 2.1 se muestran las frecuencias y los alcances del estándar 802.11.El estándar IEEE 802.11 se la puede clasificar en dos capas fundamentales: la capa MAC (Media Access Control) y la capa física. Estas dos capas permiten haya una separación funcional del estándar y, lo más importante, permite que un único protocolo de datos pueda usarse con distintos métodos de transmisión (Yunquera, 2014).

Tabla 2.1: Frecuencias y alcances del estándar 802.11.

Proto- colo 802.11	Aproba- do	Frecu- encia	Ancho de Banda	Tasa de datos por flujo	Alcance aproxi- mado en interiores		Alcance aproxima- do en interiores	
					(m)	(ft)	(m)	(ft)
-	Jun 1997	2.4	20	1,2	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	35	115	120	390
b	Sep 1999	2.4	20	1,2,5.5,1 1	35	115	140	460
g	Jun 2003	2.4	20	6,9, 12, 18, 24, 36, 48, 54	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	70	230	250	820
			40	15, 30, 45, 60, 90, 120, 135, 150				
ac	Nov 2011	5	20	Up to 87.6				
			40	Up to 200				
			80	Up to 433.3				
			160	Up to 866.7				

Fuente: (Flickenger,2013)

2.4.3 Protocolos.

Los protocolos que se explicarán a continuación serán los que se rigen al estándar 802.11 para las redes inalámbricas.

- **802.11a:** Según (Romero, 2013), en la tesis Redes inalámbricas y simulación de WLAN mediante OPNET, la revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos base que el estándar original, opera en la banda de 5GHz y utiliza 52 subportadores de multiplexación por división de frecuencia ortogonales (Orthogonal Frequency Division Multiple Access, OFMD), cual brindara una velocidad máxima de 54Mbps, lo que lo hace un estándar practico para redes inalámbricas con velocidades reales de aproximadamente 20Mbps.

La velocidad de datos se reduce a 48, 32, 24, 12, 9 o 6Mbps en caso necesario. 802.11a tiene 12 canales no soportados, los cuales se dividen en 8 que son para red inalámbrica y los otros 4 para relaciones punto a punto. Los cuales no podrán relacionarse con los equipos que tengan el estándar 802.11b, con la excepción que los equipos trabajen bajo los dos estándares (Romero, 2012).

Dado que la banda de 2,4 GHz tiene una gran utilidad, el utilizar la banda de 5GHz representará un beneficio que sacaremos del estándar 802.11a, puesto que nos va a presentar menos perturbaciones o interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a únicamente puntos en línea de vista, con lo representara un uso mayor de equipos de punto de acceso. Esto significa también que todos los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b, dado que sus ondas son más fácilmente absorbidas (Romero, 2012).

- **802.11b:** La sustentación original de este protocolo fue ratificada en 1999. 802.11b va a tener una transmisión máxima de 11Mbps y utiliza el mismo método de acceso, en la práctica la velocidad máxima de

transmisión con este estándar es aproximadamente 5,9Mbps sobre el protocolo de control de transmisión (Transmission Control Protocol, TCP) y 7,1Mbps sobre el protocolo de datagrama de usuario (User Datagram Protocol, UDP) (Romero, 2012).

Los productos de la 802.11b aparecieron en el mercado muy rápido debido a que la 802.11b es una extensión directa de la técnica de modulación de espectro ensanchado por secuencia directa (Direct Sequence Spread Spectrum, DSSS), está definida en el estándar original. Por lo que los chips y productos pudieron ser actualizados de manera mucho más fácil para soportar las mejoras que se dieron del 802.11b. El abismal incremento en el uso del 802.11b junto con sustanciales reducciones de precios fue una de las ventajas para la aceptación del 802.11b como la tecnología WLAN definitiva (Romero, 2012).

Las tarjetas 802.11b mejoraron por lo que pueden operar a 11Mbps y tiene la ventaja o desventaja que se pueden reducirse hasta 5.5, 2 o 1Mbps en el caso de que la calidad de la señal se convierta en un problema. Muchas compañías llaman a estas versiones mejoradas 802.11b+. Estas extensiones han sido ampliamente obviadas por los desarrolladores del 802.11g que tiene tasas de transferencia a 54Mbps y es compatible con 802.11b (Romero, 2012).

- **802.11g:** En junio de 2003, fue la fecha donde se certificó un tercer estándar de modulación: 802.11g. La cual utiliza la banda 2,4GHz (igual que el estándar 802.11b) pero la diferencia es que esta va a operar en velocidades hablando teóricamente máxima de 54Mbps, o cerca de 24,7Mbps de velocidad real de transferencia, lo que tiene una similitud al estándar 802.11a. Este tercer estándar es totalmente compatible con el estándar b y utiliza las mismas frecuencias. El mayor rango de los dispositivos 802.11g es ligeramente mayor que en los 802.11b pero el rango en que el cliente puede alcanzar 54Mbps es

mucho más corto que en el caso del estándar 802.11b (Romero, 2012).

Los equipos que trabajan bajo el estándar 802.11g se fueron integrando al mercado muy rápidamente, incluso antes de su lanzamiento ya era una expectativa. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Muchos de los productos de banda dual 802.11g sufren de la misma interferencia de 802.11b en el rango ya saturado de 2,4Ghz por dispositivos como antenas, dispositivos bluetooth y teléfonos inalámbricos (Romero, 2012).

- **802.11n:** En enero de 2004, fue cuando la IEEE anuncio la formación de un grupo de trabajo 802.11 con el fin de poder investigar y desarrollar una nueva versión del estándar 802.11. La velocidad real en la que transmitiría podría llegar a los 500Mbps, y tendría que ser hasta 10 veces más rápida que una red que esté sujeta a los estándares 802.11a y 802.11g, También tendría que estar cerca de 40 veces más rápida que una red bajo el estándar 802.11b. Se siguen desarrollando otros estándares los cuales se siguen desarrollando (Romero, 2013).

802.11n se construyó basándose en las versiones previas del estándar 802.11 añadiendo antenas inteligentes MIMO o Múltiple Entrada Múltiple Salida (Multiple-Input Multiple-Output). MIMO utiliza múltiples transmisiones y antenas receptoras permitiendo incrementar el tráfico de datos (Romero, 2012).

2.5. Arquitecturas con Redes WI-FI.

En un comienzo, las redes inalámbricas fueron creadas para la creación de redes de área local de empresa y hogares, únicamente para redes pequeñas con poco alcance. Así mismo su arquitectura era realmente sencilla. Lo que, con el paso del tiempo han logrado ir evolucionando hacia redes de área extendida, principalmente en sitios urbanos. Eso es debido al

hecho de que, a pesar una arquitectura muy básica, son sencillamente escalable.

- **Modo Ad-hoc:** este es el modo en el que el punto de acceso no existe. Por ello las funciones son asumidas de forma aleatoria por alguna de las estaciones presentes. En la transmisión de la información simplemente estarán implicados los dos equipos en cuestión, sin en uso de alguna jerarquía superior, de esta manera se podrá aprovechar del canal de comunicación al máximo (Yunquera, 2014).
- **Modo infraestructura:** En este modo es donde interviene el punto de acceso, el cual se encargará de las funciones de coordinación. Entonces lo que sucederá es una clara pérdida de calidad debido a que todo el tráfico pasara por el punto de acceso, una ventaja con la que se contara con su uso es el ahorro de energía (Yunquera, 2014).

2.6 Arquitecturas básicas de despliegues.

Según (Yunquera, 2014), una vez entendidos los modos y servicios internos que proporciona la recomendación 802.11, se pueden describir los principales modelos de arquitecturas que se pueden emplear en los despliegues de redes inalámbricas.

- **Modo punto de acceso básico:** Es considerado el principal modo de infraestructura por medio del cual un punto de acceso irá conectado a una red local y en su parte inalámbrica este va a estar compartiendo un conjunto de estaciones. Este es el modo más popular para realizar pequeñas instalaciones.
- **Modo hot stand-by:** Este modo se basa en la configuración de dos puntos de acceso que estarán en la misma ubicación y así mismo con parámetros similares y por su puesto tienen que estar conectados a la misma red local. Uno del punto de acceso estará configurado en modo activo y el otro en modo stand-by.
- **Modo repeater:** En este modo estará configurado con un punto de acceso que se conecta a otro mediante el sistema de distribución inalámbrico (Distribution System Wireless, WDS) y ambos estarán

acoplados en el mismo canal y al identificador del conjunto de servicios (Service Set Identifier, SSID). De esta forma el segundo punto de acceso extiende la cobertura del primero lo que nos permitirá que las estaciones que estén más distantes puedan acceder a la red local cableada.

- **Modo bridge:** Este modo nos permite conectar dos o más redes cableadas por medio de un segmento inalámbrico. Uno de los bridges actúa en modo root, mientras que los otros actuarán simplemente como estaciones.
- **Modos híbridos:** Este modo se configura combinando algunas de las anteriores, como por ejemplo un modo de punto de acceso básico con estaciones y a la vez con un bridge conectado con equipos fijos en su red cableada. Actualmente la mayoría de los equipos inalámbricos pueden operar en múltiples modos.

2.7. Topologías de las redes Inalámbricas.

Según (Flickenger, 2013), Las redes inalámbricas se las puede clasificar por medio de tres configuraciones lógicas estas pueden ser:

- **Enlace punto a punto:** Estos enlaces son principalmente utilizados para que el internet pueda llegar en lugares en los cuales el acceso no esté disponible. Básicamente este enlace funciona teniendo un punto conectado a internet mientras que el otro para poder conectarse tendrá que utilizar el enlace.

Escogiendo un tipo de antena idónea y existiendo línea vista entre los sitios para la comunicación, se pueden hacer enlaces punto a punto totalmente seguros por encima de los treinta kilómetros. En la figura 2.3 encontraremos una conexión punto a punto entre dos edificios los cuales se encuentran alejados, pero sin ningún tipo de obstáculo que no permita la conexión, además se puede seguir extendiendo la red incorporando más redes.

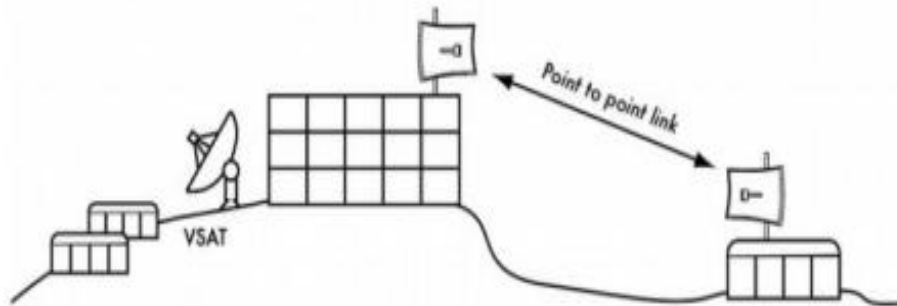


Figura 2.3: Enlace Punto a Punto entre dos edificios.
Fuente: (Flickenger, 2013)

- **Enlace punto a multipunto:** Este tipo de enlaces son casualmente visualizados en diversos sitios de un entorno, cuando se observa que hay múltiples nodos los cuales están interactuando en una red con un punto de acceso central aquí es donde nos podemos dar cuenta que existe una red punto a multipunto (Flickenger, 2013).

Esta clase de enlaces se los utiliza comúnmente en áreas en las cuales no se puede tener una línea de vista entre ellos por motivo de algún tipo de obstáculo ya sea natural o creada por el hombre, pero con la condición que se pueda instalar una antena la cual tiene que estar por encima de cualquier obstáculo que pueda interferir el enlace, a continuación en la figura 2.4 se observa un enlace punto a multipunto.

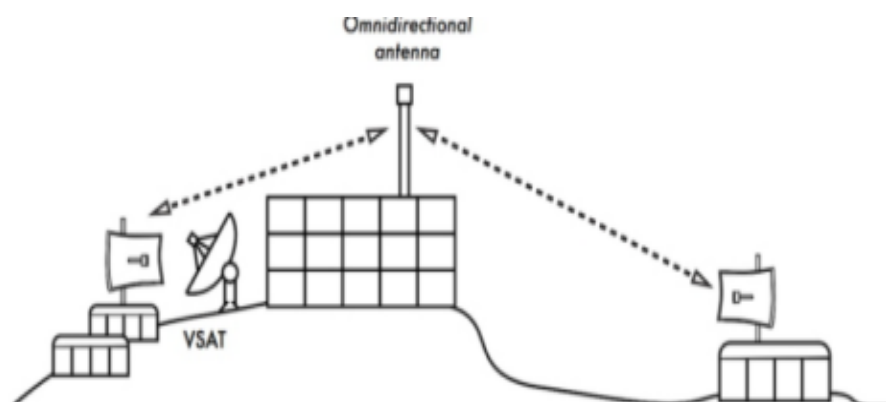


Figura 2.4: Enlace Punto a Multipunto
Fuente: (Flickenger, 2013)

- **Enlace multipunto a multipunto:** Esta clase de conexión de red multipunto a multipunto se la puede llamar también red Ad-hoc o de

En una red en malla, esta clase de enlace no espera la ayuda de alguna clase de equipo, debido a que el transporte del tráfico será realizado por cada nodo de la red obligatoriamente a los nodos que sean, gracias a eso estarán comunicados entre sí, sin algún tipo de problema. En la figura 2.5 se muestra un enlace multipunto a multipunto.

La característica principal de esta conexión de red es que puede autorrepararse, es decir, al momento de encontrarse con algún tipo de inconveniente con el enrutamiento, este simplemente se lo corrige (Flickenger, 2013).

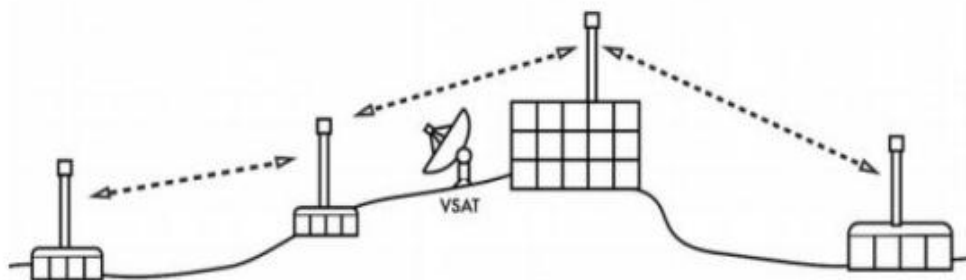


Figura 2.5: Enlace Multipunto a Multipunto
Fuente: (Flickenger, 2013)

2.8. Definición de Antena.

Las Antenas son una de las partes fundamentales de los sistemas de telecomunicación específicamente diseñadas para radiar o recibir ondas electromagnéticas, y por medio de estas se puede realizar una conexión o enlace desde cualquier lugar que se desee.

Con relación a (Ferrando, 2014), define a las antenas como los dispositivos que adaptan las ondas guiadas, que se transmiten por conductores o guías, a las ondas que se propagan en el espacio libre. Para realizar un sistema de Comunicaciones se utilizan antenas para realizar ya sea para enlaces punto a punto, difundir señales de televisión o radio, o bien transmitir o recibir señales en equipos portátiles.

2.8.1. Clasificación de las Antenas.

Debido a la gran cantidad de antenas que hay actualmente, es muy difícil poder dar detalle de cada una de ellas, por lo cual, las vamos a clasificar de esta manera como se muestra en la tabla 2.2:

Tabla 2.2: Tabla con la clasificación de las antenas

	TIPO DE ANTENA	CARACTERÍSTICAS
Según su forma de radiación	Antenas omnidireccionales	Dipolos eléctricos y magnéticos (<i>loops</i>), antenas de parche.
	Antenas direccionales	Yagi-Uda, reflectores parabólicos, helicoidales, arreglos dipolares. A su vez, pueden ser <i>endfire</i> o <i>broadside</i> ; es decir, radiar en dirección del eje de la antena o en dirección perpendicular a ella.
	Antenas independientes de la frecuencia (de gran ancho de banda)	Logarítmicas, espirales, espirales cónicas.
	Antenas electrónicamente direccionables y adaptivas	Arreglos de antenas de fase controlada (AAFC) y arreglos de antenas activas de fase controlada (AAAFC). Sus elementos pueden ser dipolos, antenas de parche, hélices, etcétera.
Según su geometría y/o construcción	Antenas delgadas (<i>wire antennas</i>)	Dipolos eléctricos y magnéticos, logarítmica, Yagi-Uda, helicoidal, arreglo de dipolos.
	Antenas de abertura	Guía de onda, corneta, reflectores parabólicos e hiperbólicos.
	Antenas autodefinidas	Logarítmicas, espirales, espirales cónicas.
	Antenas planares	Antenas de parche (diversas geometrías), espirales.
	Antenas cuasi-ópticas	Aberturas (<i>slots</i>), antenas de Fresnel.

Fuente: (Hernández, 2012)

2.9. Antenas Inteligentes.

En la actualidad, la demanda de las redes inalámbricas ha aumentado abismalmente por lo que la capacidad es lo que se quiere mejorar mediante la implementación de nuevas fórmulas, algoritmos y estándares con las que se pueda sacar el mayor provecho al espectro radioeléctrico de manera acertada. Los sistemas de antenas inteligentes brindan la función de poder aumentar el espacio de su sistema, lo cual ayuda a incrementar la calidad del servicio, teniendo la capacidad de intervenir en la potencia y aumenta la capacidad de las baterías.

2.10. Principios de Funcionamiento.

Para (Huidobro,2013), una antena inteligente es la agrupación de algunas mejoras de antenas con el apartado de Procesamiento Digital de Señales, lo cual incrementa considerablemente los diagramas de transmisión y por consecuencia los de recepción. Por otro parte, este tipo de antenas son capaces de crear haces a su voluntad por lo que no tiene un diagrama de radiación única, dirigiéndolas en la dirección que desee o al usuario que quiera, incluso se puede adaptar a los cambios radioeléctricos. Estas capacidades son muy esenciales al momento de compartir por mandato regulatorio las infraestructuras de torres y sitios elevados.

“El principio básico de funcionamiento de las antenas inteligentes es que cada antena recibe una señal separada y definida. Dependiendo de cómo está configurado el sistema inalámbrico, el receptor puede usar una señal para mejorar la calidad de otra señal, o podría combinar los datos de señales múltiples para ampliar el ancho de banda disponible. Las Smart Antenas, como suelen ser llamadas también, se diferencian de las antenas convencionales ya que pueden trabajar de dos modos distintos los que se describen brevemente a continuación: Modo omnidireccional. La antena en este modo funciona exactamente igual que las antenas convencionales, es decir, emite señal con la misma intensidad hacia todas direcciones y el Modo direccional. En este modo, la antena emite señal en una sola dirección y con un cierto ángulo de apertura”(Huidobro, 2013).

2.11. Tipos de antenas inteligentes.

Para ver los tipos de antena primero se tiene que saber que existe una fase de transmisión previa de datos la cual es una relación del sistema de gestión y los usuarios. Se puede deducir que el hallar usuarios que estén ubicados en la zona y llevar un control es lo de lo que se encarga esta fase. En referencia a (Huidobro, 2013), explica que actualmente están disponibles tres tipos de antenas inteligentes, las de Haz Conmutado, las de Haz de Seguimiento y las de Haz Adaptativo.

- **Haz conmutado:** Este sistema es el encargado de crear algunos haces a ángulos previamente asignados lo que dará como resultado escaneo silencioso del área de cobertura siempre y cuando se hayan conmutado de manera ordena en posiciones angulares específicas.

- **Haz de seguimiento:** Esta clase de haz es más complicado que el haz conmutado debido a que está formado por un array de antenas que tiene una red por medio de la cual se podrá tener un control de las corrientes que van apareciendo en los componentes del mismo para poder variar el rumbo del haz eficazmente y decretar la comunicación con el usuario respectivo. La diferencia que se puede encontrar entre las antenas de haz conmutado y de haz de seguimiento es que el de haz conmutado tiene posiciones angulares fijas (prefijadas) y el de seguimiento no. En la figura 2.6 se puede observar cómo se forma un haz.

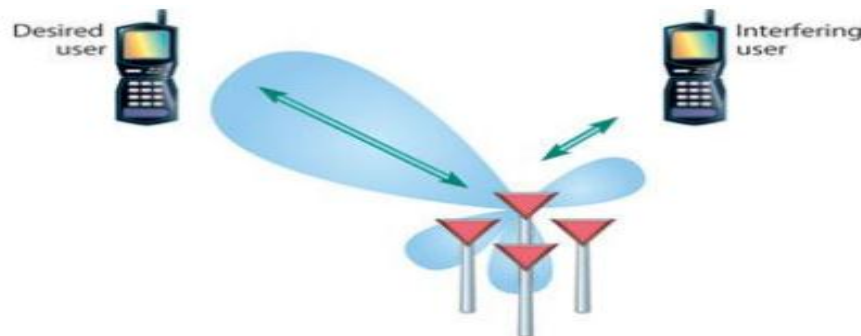


Figura 2.6: Formación de haz de antena inteligente
Fuente: (Huidobro, 2013)

- **Haz adaptivo:** En este tipo de haz las salidas de cada uno de los componentes de las antenas se incrementan con una cantidad de peso esta cantidad será estipulada dinámicamente con lo que se puede construir un diagrama de radiación hasta el sitio que el usuario haya requerido por medio del haz principal y los secundarios hasta trayectorias de las componentes del multitrayecto de la señal deseada y mínimos o nulos de la radiación en las direcciones de las fuentes de interferencia.

2.12. Antenas MIMO.

Las antenas MIMO (Múltiple-Input Múltiple-Output) o (entradas múltiples, salidas múltiples), una tecnología que se utiliza en equipo actuales, así mismo en redes como en tecnologías como WI-FI, la cual usa el fenómeno de multipropagación y radiocomunicaciones en diversidad de

espacio para poder alcanzar una mayor velocidad y una mejor cobertura del que se consigue con las antenas tradicionales, en la figura 2.7 podemos darnos cuenta como los router en la actualidad tienen las antenas MIMO.



Figura 2.7: Router WI-FI con tres antenas
Fuente: (Huidobro, 2013)

Es tan beneficiosa esta tecnología que actualmente la tenemos en la vida diaria, esto lo podemos ver en autos por medio de las antenas captamos la señal emitida por la estación de radio. Pero la radio también recibe señales no deseadas de la misma emisión que van llegando de diferentes direcciones, ya sea por los edificios, árboles, accidentes geográficos y otras estructuras de la zona.

2.13. Ventajas redes inalámbricas.

De acuerdo a una investigación realizada por (Ramírez, 2013), docentes de la Universidad de Veracruzana de México indican que las principales ventajas de las redes inalámbricas son:

- **Basada en estándares y con certificación WI-FI:** El WI-FI es una de las principales tecnologías de estándar de redes, que permite la transmisión de datos, que nos ratifica que los productos inalámbricos se comunicaran sin problema con otra clase de productos certificados de WI-FI de otros fabricantes de redes. Con un sistema basado en WI-FI, los usuarios contarán con la compatibilidad con la mayor parte de productos inalámbricos lo cual ayuda a evitar los alto costos y la selección limitada de las soluciones patentados por un sólo fabricante.

- **Instalación simple:** Los sistemas inalámbricos son más fáciles a la hora de configurarlos, lo que ayuda d manera más rápida a la instalación. Por otro lado, al conectarla, los usuarios de una manera

inmediata contasen con los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soportar el protocolo denominado (Dynamic Host Configuration Protocol, DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos.

- **Robusta y confiable:** Considera soluciones inalámbricas robustas que tienen alcances de por lo menos 100 metros. Estos sistemas brindan a las personas una movilidad más significativa, así mismo dentro de una compañía el empleado tendría más movilidad en las instalaciones.
- **Facilidad de uso:** Si un usuario planea conectar múltiples puntos de acceso inalámbricos a una red existente de cables es la opción más factible para poder tener totalmente cubierta las instalaciones, por lo que con la movilidad se puede seguir conectado a la red sin interrupciones y se debe considerar una solución que ofrezca conexiones automáticas a la red.
- **Costo de propiedad reducido:** En una red LAN se requiere una inversión mayor debido a el cableado, en el caso de la red inalámbrica se ahorra este costo adicional, aparte el mantenimiento del cable es un costo que llegara tarde o temprano.
- **Facilidad de configuración para el usuario:** La persona que se quiera conectar a la red inalámbrica simplemente necesitara de una clave para poder acceder a la red.

2.14 Seguridad Redes Inalámbricas.

La forma más utilizada para conectarse a Internet es por medio de una conexión WI-FI, un sistema que permite al usuario importantes ventajas a diferencia de la conexión que se realiza por medio de cable. Pero este sistema tiene también inconvenientes, y uno de ellos hay que tenerlo muy presente es la seguridad de nuestra red, la cual podemos protegerla por algunos métodos entre los que tenemos:

2.14.1. Cifrado WEP.

En la seguridad de redes inalámbricas una de las pioneras es el cifrado WEP (Wired Equivalent Privacy), la cual brinda soluciones de seguridad que se puedan presentar si se dejan una red abierta. Básicamente este cifrado funciona con una verificación del usuario usando una contraseña. El algoritmo de cifrado RC4, es la base del cifrado WEP que puede generar claves tanto de 64 o hasta de 128 bits (ACENS, 2012).

2.14.2. Cifrado WPA.

Este sistema de cifrado WAP (Wireless Application Protocol) apareció con el simple hecho de poder solucionar los problemas de seguridad que tenía el WEP. Entonces se utilizó TKIP (Temporal Key Integrity Protocol), el cual es un protocolo que utiliza el mismo cifrado del WEP, pero asigna claves en forma aleatoria (ACENS, 2012).

2.14.3. Cifrado WPA2.

De igual manera como apareció la WAP para solucionar problemas de la WEP, la WAP2 surge para solucionar problema que dejó la WAP. Este sistema presenta dos cambios principales respecto a WPA: El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo "Counter Mode/CBC-Mac" que es considerado criptográficamente seguro. Reemplazo del algoritmo RC4 por el algoritmo AES, uno de los más seguros actualmente (ACENS, 2012).

2.15. Concepto video vigilancia.

Un CCTV (circuito cerrado de TV) es un sistema de tecnología de vigilancia visual que se trata de tener equipos de monitoreo (cámara IP, NVR, etc.), en puntos estratégicos para poder captar en video lo que esté ocurriendo, en el área que se requiera cubrir, las cámaras se podrán monitorear ya sea en el mismo punto o desde otro lado.

Esta Red nos servirá como base para poder implementar un sistema de video vigilancia IP, el cual se trata de tener equipos de monitoreo (cámaras IP, NVR, etc.), estas imágenes grabadas se las puede almacenar

en quipos ya sean NVR o DVR, esto dependerá del tipo de sistema que se implemente (Grupo TCR, 2016).

Cuando el equipo está conectado a una red IP, tenemos la disponibilidad de acceder a las imágenes, desde cualquier lugar en el que se encuentre por medio de cualquier red de internet. Un sistema ideal de CCTV debe proporcionar imágenes de gran calidad tanto de día como en condiciones de baja luminosidad, ser versátil y fácil de usar. La principal función de unas cámaras de seguridad es permitirnos la detección temprana de alguna acción peligrosa que esté sucediendo.

Según Grupo TCR(2016), La instalación de los dispositivos se realiza con objetivo de asustar a ciertos delincuentes potenciales que quieran amedrentar en algún punto. Un sistema vídeo vigilancia IP es una tecnología que coge los beneficios analógicos y los complementa con los tradicionales CCTV con las ventajas digitales de las redes de comunicación IP.

2.16. Tipos de cámara.

Con relación al (Grupo TCR , 2016), indica los diferentes tipos de cámaras que se pueden encontrar en el mercado, entre las que están:

- **Interior:** Son el tipo de cámara más sencillas que hay en el mercado. No necesitan carcasa.
- **Infrarrojo:** Es el tipo de cámara que tiene incorporado la visión nocturna, un ejemplo de su uso seria en empresas que por la noche pasen cerradas, y puedan captar lo que sucede durante esas horas.
- **Antivandalística:** Estas cámaras tiene incorporada una carcasa resistente a golpes y se mantienen fijas para seguir grabando todo lo que ocurre. Ejemplos para su uso seria en parqueos, almacenes, discotecas o bares o exteriores de tiendas.
- **Cámaras IP:** Son las más completas ya que se conectan directamente a Internet y nos pueden mostrar la imagen del lugar

donde está colocada. La imagen que capta una cámara IP se puede visualizar desde el móvil desde cualquier parte del mundo, sin necesidad de utilizar otros equipos.

- **Cámaras en movimiento y zoom:** Este tipo de cámara permite el acercarse y alejarse en el video para poder captar mejor o reconocer mejor lo que se visualiza.

Hay cámaras que reúnen varias de las características al mismo tiempo. Se pueden encontrar cámaras anti vandálicas con infrarrojos y lente de varios focos, cámaras de exterior con movimiento o zoom, cámaras IP con sistema de grabación interno, etc.

2.17. Aplicaciones.

El (Grupo TCR,2016), expresa las diferentes aplicaciones que se les pueden dar a las cámaras de video vigilancia, entre las cuales se menciona.

- **Comercio:** Reducen en cierto porcentaje los atracos, ayuda a que el personal se sienta más seguro en el trabajo, y optimiza la gestión de los locales.
- **Transporte:** Ayuda a proteger a los pasajeros, el personal y la mercancía en cualquier sistema de transporte, ya sea taxi, urbano, trenes, etc.
- **Actividades bancarias y financieras:** Control de oficinas, sucursales y los cajeros automáticos dese una localización específica.
- **Vigilancia urbana:** Se instalan en parques, centros deportivos, calles principales, sedes de conciertos y de exposiciones públicas.
- **Educación:** Las cámaras ayudan a contrarrestar actos vandálicos y mejorar la seguridad del personal y los estudiantes en guarderías, colegios, institutos, universidades.

- **Seguridad ciudadana:** Se emplea en asuntos relacionados con el cumplimiento de la ley, militares, control fronterizo, protección de turistas. También sirve para asegurar todo tipo de edificios.
- **Asistencia sanitaria:** Mejora la seguridad del personal y de los pacientes: salas de urgencias, sala de suministros médicos, etc.
- **Industrial:** Protección de grandes perímetros como aparcamientos, en grandes terrenos agrícolas, donde la supervisión remota es importante con capacidad de visión en tiempo real.
- **Residencial:** Garantizar la seguridad de hogares y que no sean vulnerables.
- **Marketing:** Análisis de persona que ingresen a locales comerciales o centros comerciales.

2.18. Funciones cámaras IP.

Así mismo el (Grupo TCR, 2016), explica las principales funciones que cumplen las diferentes clases de cámaras IP tales como:

- **Registro y control en vivo:** Las cámaras IP permiten el monitoreo remoto de vídeo, la grabación digital y el almacenamiento masivo.
- **Vigilancia remota a través de internet:** Se puede acceder a cámara IP y observar en vivo desde cualquier ordenador en red con acceso a Internet.
- **Monitoreo con el software de vídeo IP:** Existen herramientas para el monitoreo simultáneo de algunas cámaras al mismo tiempo.
- **Grabación del vídeo en red:** Se puede programar la grabación continua, programada, o determinada para un evento eso dependerá de la configuración que se desee.

- **Detección de movimiento:** Se puede programar la cámara de seguridad IP para que comience a grabar simultáneamente se pueden realizar otras funciones como llamar a las autoridades, enviar mensaje por WhatsApp o por correo electrónico apenas se detecta algún movimiento en una escena.
- **Grabación de audio:** Se puede acceder a las grabaciones de audio desde lugares remotos.
- **Reconocimiento biométrico facial:** Consiste en identificar a las personas que aparecen en la imagen a partir de una base de datos creada previamente.

2.19. Sistemas NVR / DVR.

Un DVR (Digital Video Recorder) es considerado por algunos como el alma de un circuito cerrado de televisión (CCTV) sistema de vigilancia. Este sistema cuenta con algunas entradas o también llamados canales que son utilizados para la conexión de las cámaras. Las cámaras actúan de manera individual y se las puede configurar de forma distinta si se deseara, esto ayudaría a optimizar su ubicación y ganar cobertura (Sance Group, 2017).

Un NVR (Network Video Recorder), como el DVR, es también la base de un sistema de CCTV. Es un componente central que está vinculado a todas las cámaras IP a través de una red que utiliza el protocolo de control de transmisión TCP / IP. En este caso, cada cámara tendría su propia dirección IP y se comunica con el NVR.

2.19.1. Características similares de DVRs Y NVRs.

Según (Sance Group, 2017), hay varias características similares de DVRs y NVRs. Entre ellos están:

- Ambos tienen la capacidad de brindar la revisión del material guardado.
- Ambos tienen características de visualización remota.
- Tienen funciones de superposición de texto.

- Poseen características de vista de pantalla de matriz.
- Tienen capacidades de detección de movimiento.
- Tienen funciones de disparo de alarma.
- Pueden producir informes de eventos.
- Ambos tienen funciones de grabación de audio.
- Ambos tienen controles de panorámica, inclinación y zoom.

2.19.2. Características Contrastantes de un NVR y DVR.

Según (Sance Group, 2017), las diferencias más importantes que existen entre NVRs y DVRs son las siguientes:

- En el NVR, se procederá a la codificación de un video de forma continua en la cámara, con DVRs, la codificación de video no se realizará en la cámara sino en el dispositivo.
- A la hora de seleccionar que tipo de cámara es más factible utilizar para NVR es más complicado que seleccionar cámaras para DVRs debido que hay una mayor diversidad de cámaras compatible al DVRs.
- Un DVR solo puede recibir un video y ya en cambio en el NVR se puede modificar a como se desee.
- Las imágenes capturadas por un NVR se la podrán ver des cualquier lugar sin ningún tipo de problema mientras que del DVR únicamente donde esté ubicado el dispositivo.

2.20. Comparando los sistemas DVR / NVR.

Los sistemas DVR / NVR tienen un mayor condición de instalación y en algunos casos, el costo es más significativo esto dependerá del tipo de sistema que se escoja para implementar, así mismo el número de cámaras incluidas (Sance Group, 2017).

Para un sistema de seguridad de nivel de entrada rápida, las cámaras IP autónomas pueden ser una solución sencilla y rápida. Pero para los

hogares y negocios se necesita un sistema de seguridad más robusto, un sistema DVR/NVR sería la opción más idónea. La mejor manera de determinar qué sistema implementar se tiene que realizar cálculos teniendo en cuenta la resolución de cámara, cantidad de cámaras, entre otras (Sance Group, 2017).

CAPÍTULO 3: ANÁLISIS DE LA PROPUESTA DEL PROYECTO

3.1. Análisis de la situación delincencial actual del país y de la ciudad.

Para poder tener un análisis de la situación actual en la que se encuentra el país y la ciudad de Guayaquil se tomarán en cuenta otros puntos de vista como a la situación de seguridad y uso de la tecnología con estos datos se podrá justificar la realización de diseño técnico - económico de una red de internet comunitaria mediante tecnología de acceso WI-FI a través de un sistema de video vigilancia IP en la ciudadela Álamos Norte de Guayaquil.

3.2. Datos Estadísticos a nivel delincencial en el Ecuador.

El sentimiento de inseguridad tiene mucho que ver, con la comunicación interpersonal o intergrupala, con el estilo de vida poco comunitario que impera en nuestra sociedad y que está llevando a los ciudadanos a abandonar paulatinamente los espacios públicos por esta razón, la delincuencia va tomando más fuerza en las calles en la siguiente figura 3.1 se observa los porcentajes de personas que han sufrido alguna clase de delito.

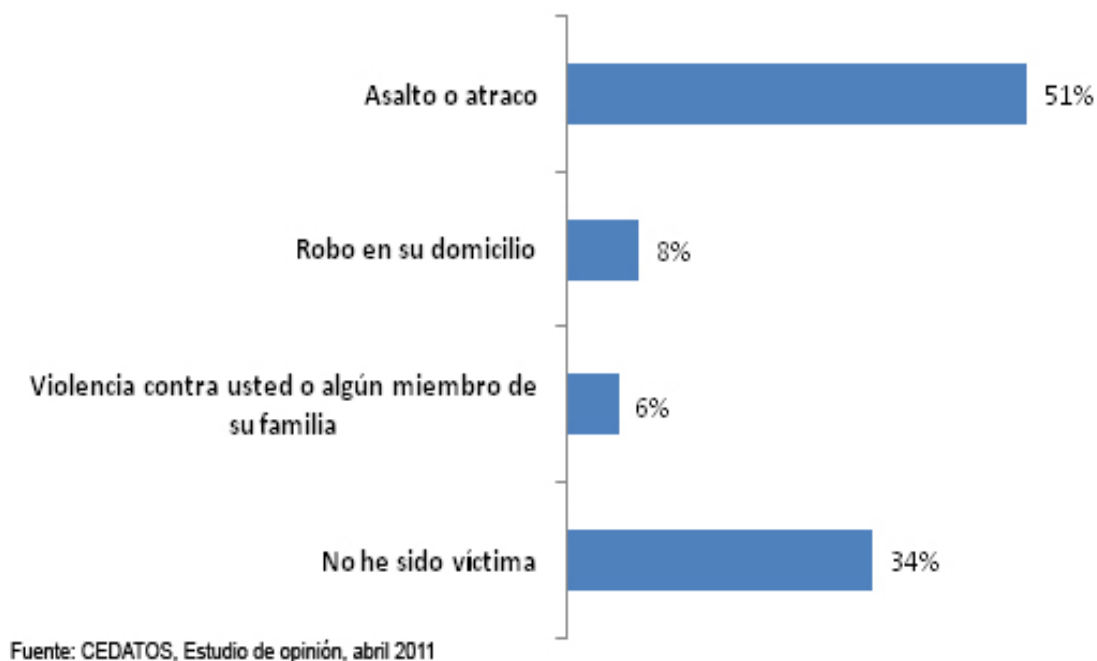


Figura 3.1: Porcentaje de personas que han sufrido algún tipo de delito.
Fuente: (CEDATOS, 2011)

Como ya se mencionó la delincuencia sigue aumentando con la falta de comunicación entre vecinos ya que la mayoría de ellos desean resolver sus problemas por sí solo. De igual manera en una encuesta realizada por el INEC (Instituto Nacional de Estadística y Censo), donde preguntan a la comunidad que tan seguros se sienten en sus barrios a nivel nacional se revelan cifras preocupantes en la figura 3.2 se detalla por provincia.

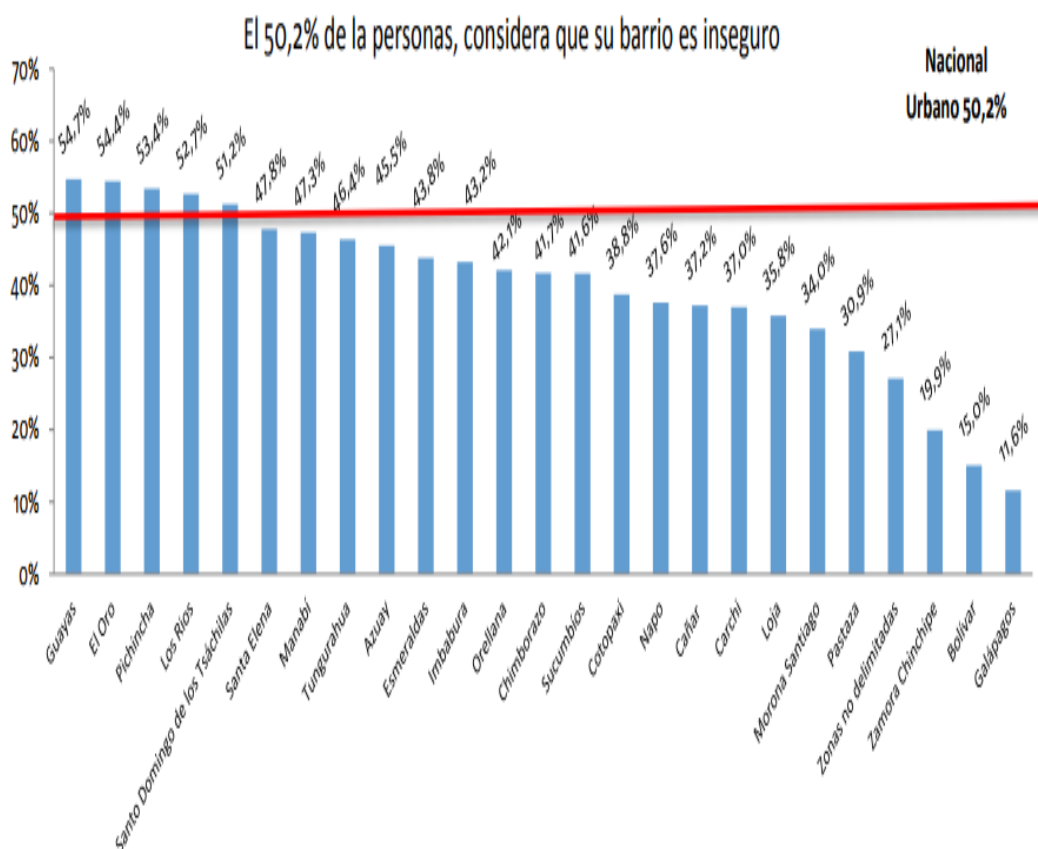


Figura 3.2: Porcentaje de personas que consideran su barrio seguro
Fuente: (INEC, 2011)

En este estudio realizado por (CEDATOS, 2011) da a conocer los problemas que cada vez aquejan más a los ciudadanos con su respectivo porcentaje. En otra encuesta realizada por (CEDATOS, 2011) la ciudadanía da su opinión con respecto a cuáles serían los principales problemas de seguridad como se muestra en la figura 3.3, el 60% considera que el principal problema de seguridad que aqueja a su ciudad es el robo o asaltos, le sigue con el 16% la venta de drogas, el 12% los robos a domicilios y un 8% la violencia contra personas.

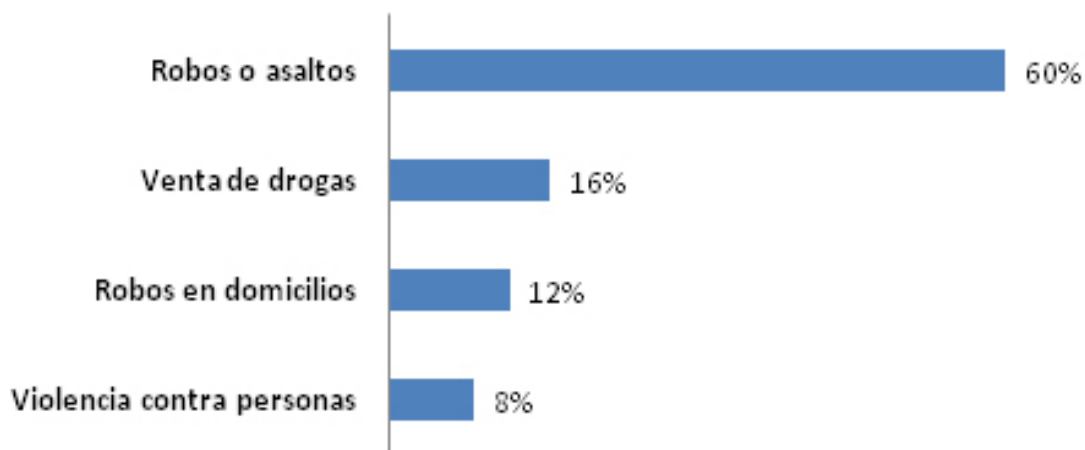


Figura 3.3: Porcentaje de principales problemas de seguridad
Fuente: (CEDATOS, 2011)

Hay varias maneras por las cuales se podrían ir solucionando estos problemas de seguridad como se muestra en la figura 3.4. Por parte de la población el 28% está de acuerdo con que la solución es implementar programas para generar empleo, el 23% considera importante que exista un mayor involucramiento de las Fuerzas Armadas, un 23% además cree que se requiere mayor número de efectivos policiales, el 15% concuerda en que se requiere una mayor capacidad de respuesta de las autoridades, finalmente un 10% ve como solución crear más programas sociales.



Figura 3.4: Porcentaje de posibles soluciones por parte de la población
Fuente:(CEDATOS, 2011)

Según datos que se tomaron a través de una observación directa en la ciudadela Álamos durante dos semanas, se registraron 22 casos ocasionados por la delincuencia, entre los cuales se muestran en la figura 3.5 a continuación:

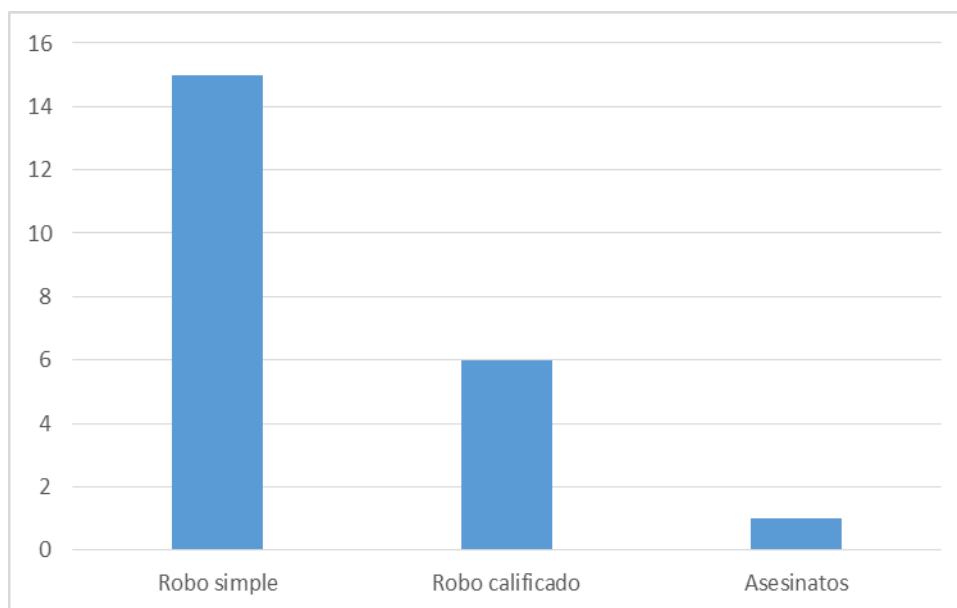


Figura 3.5: Estadísticas de robos en la ciudadela Álamos Norte de Guayaquil.
Elaborado por: el autor

De acuerdo con la figura 3.5, el índice delincencial lo lleva encabezado por el robo simple con 15 casos catalogados como actos donde la víctima no es agredida, seguido del robo calificado con 6 casos, cuando la víctima ha sufrido lesiones en su cuerpo a causa del acto del robo y finalmente 1 asesinato por cuestiones de forzar el robo ante sus agresores. Estos datos parten de una población de 37 familias que habitan en la zona, lo que indica que durante dos semanas casi el 30% de las viviendas han sido víctimas del robo.

3.3. Uso de la tecnología en el Ecuador.

En la actualidad somos una sociedad digital, a que me refiero con esto, a que la tecnología cada vez se vuelve algo esencial en la vida cotidiana, ya sea por comunicación o por estudios, esto ya dependerá del uso que le de cada persona, a continuación, en la figura 3.6 vemos una encuesta en la

cual revela porcentaje de hogares con teléfonos móvil y fijo.

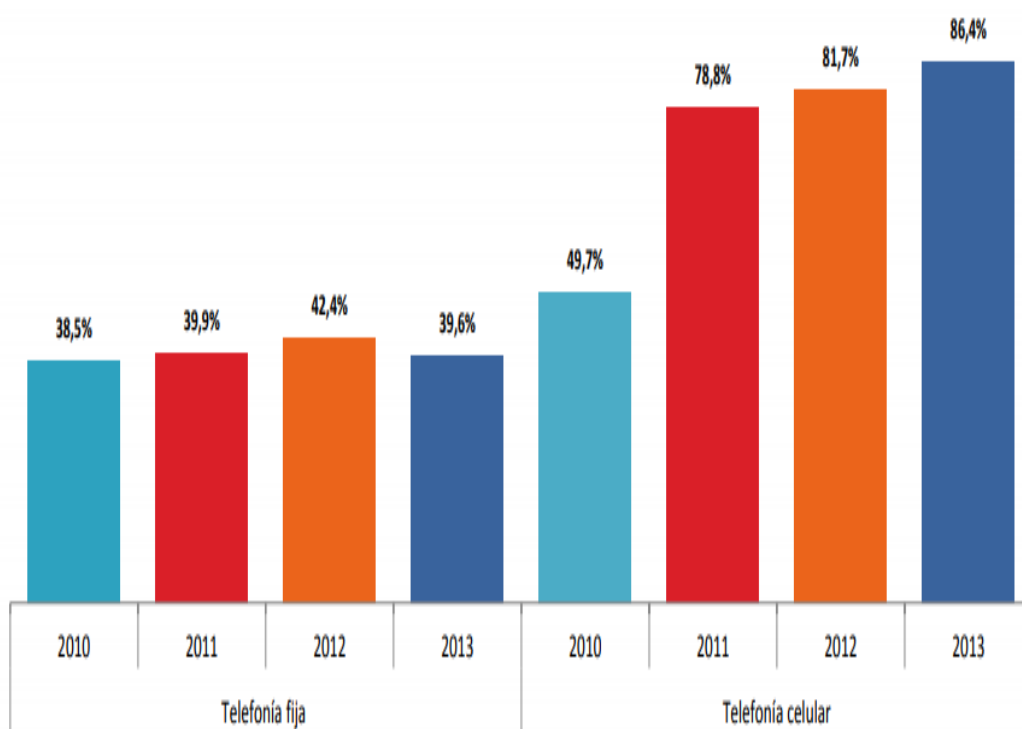


Figura 3.6: Porcentaje de hogares con teléfono fijo y móvil a nivel nacional
Fuente: (INEC, 2014)

Así mismo el teléfono móvil y fijo son unos de los equipos tecnológicos que últimamente se los considera importante tener en el hogar. De igual manera presento una encuesta realizada por el INEC con respecto de estos equipos los Smartphone son los quipos tecnológicos sin duda alguna más utilizados por las personas, debido a que con estos se puede conectar en cualquier lugar, en cualquier momento y de manera más práctica.

Una tecnología que sin duda pienso que es la más importante en la actualidad es el internet, ya que por medio de este podemos usar diversos equipos tecnológicos como los antes mencionados. Uno de los problemas que hay es que la mayoría de las personas no usan el internet para total beneficio ya que el internet es una herramienta tan amplia y muy útil, que lamentablemente no todas las personas le sacan todo el provecho a esta tecnología. A continuación, mostrare una encuesta de los hogares que tienen acceso a internet realizada por el INEC.

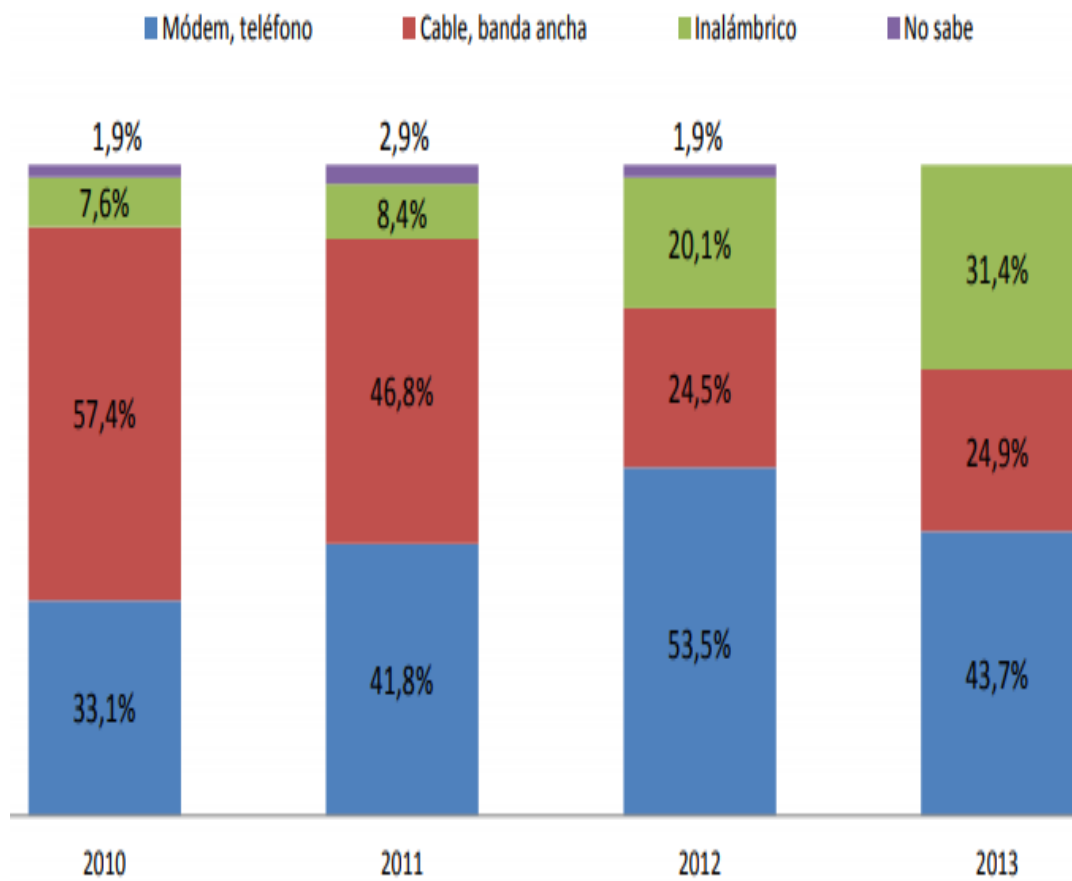


Figura 3.7: Porcentaje de hogares con acceso a internet a nivel nacional
Fuente: (INEC, 2014)

Con todas estas gráficas e indicadores podemos darnos cuenta de cómo la tecnología ha surgido para nuestro bienestar, pero la situación actual de las personas al no saber cómo aprovechar de esto al cien por ciento, da la iniciativa a proceder con la realización de este trabajo de investigación para poder darle otro uso a estas herramientas y poderlas aprovechar mejor.

El internet podría ser usado para poder brindar seguridad a las familias complementando esta herramienta con equipos, tales como cámaras IP con sus DVR, computadoras y Smartphone con sus aplicaciones de acceso a las imágenes online, teniendo todo esto complementado podemos tener un servicio más robusto que es lo que se quiere llegar con esta tesis.

3.4. Criterios técnicos y de ingeniería para el diseño técnico - económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza la tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil.

En el apartado sobre la seguridad del país se evidencia que existe una preocupación en los ciudadanos a nivel nacional, debido a algunos factores, uno de estos sería que el 51% de las personas han sido asaltadas, otro factor sería que el 50.2% siente que su barrio no es seguro, por lo cual hace pensar que se necesita una plataforma por la cual las personas se sientan más tranquilas.

En el punto de uso de la tecnología se observa que una gran parte de la población tiene acceso a internet, cuenta con un equipo tecnológico actualizado (computadora, Smartphone, etc.), variables importantes para la implementación de un sistema que ayude a solucionar problemas de seguridad en la ciudadela.

Este trabajo de titulación tiene como objetivo brindar una red comunitaria de internet mediante tecnología WI-FI con un sistema de video vigilancia IP para un sector de la ciudadela Álamos Norte de la ciudad de Guayaquil, que actualmente tiene a los moradores como víctimas de robos, y que debido a la falta de conocimiento y altos costos de estudios previos que se necesita para la instalación de esta red comunitaria y cámaras IP.

Se presenta una solución en cuanto a herramientas que ayuden a actuar de manera rápida frente a cualquier inconveniente, esta iniciativa comenzara en las manzanas 18 y 19 de la ciudadela, llegando aproximadamente 750.08 m lo que nos da un aproximado del área de 25,182.641 m² tal como lo muestra el siguiente gráfico.

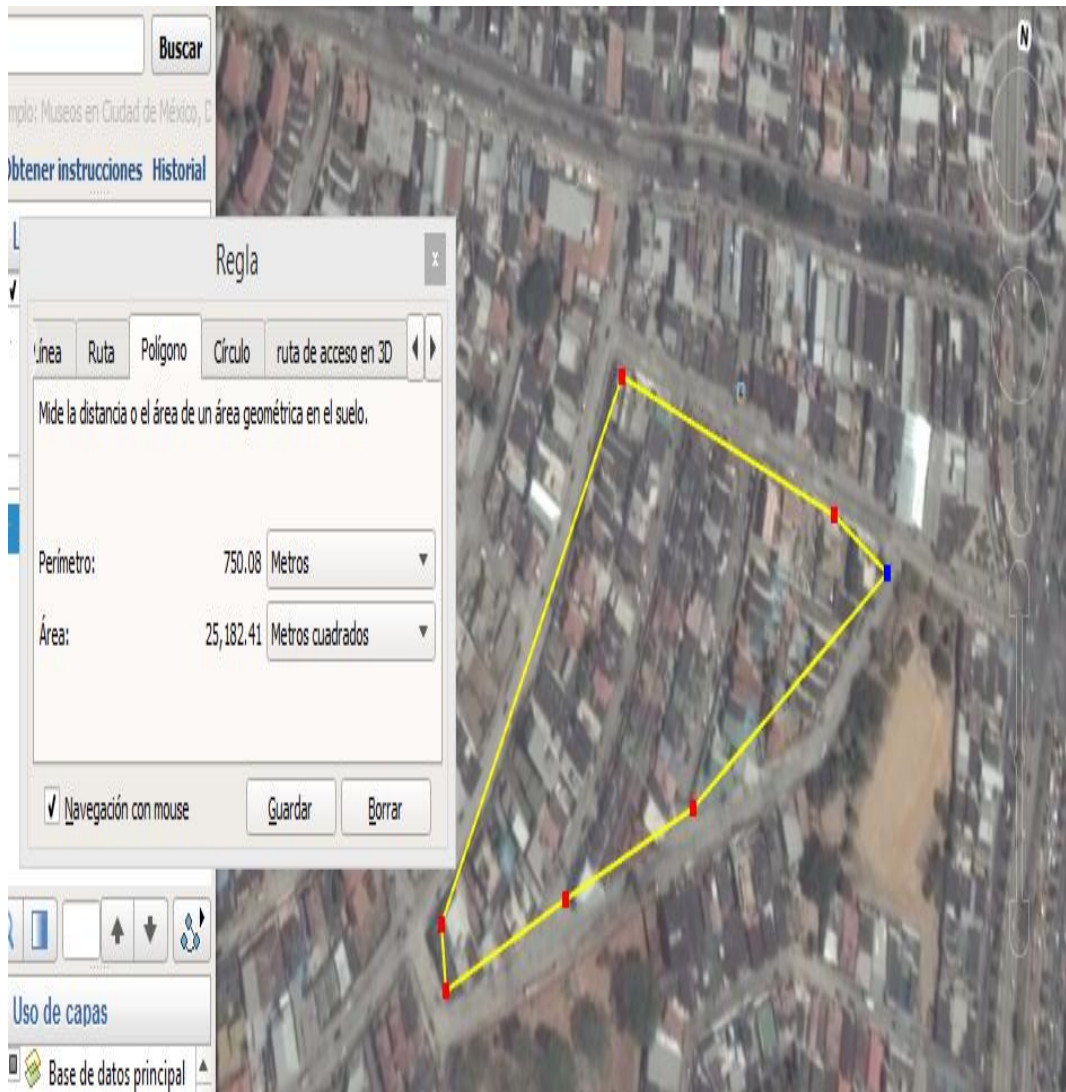


Figura 3.8: Área de la red Comunitaria con Cámaras IP
Elaborado por: Autor

3.5. Calculo de ancho de banda que se necesitara.

Para hacer un cálculo de ancho de banda tomaremos en cuenta las tramas Ethernet, puesto que usaremos este tipo de cable para este proyecto de titulación, se tiene que tener en cuenta que la trama Ethernet tiene un máximo de 1500 bytes de transmisión de datos, pero las Cabecera IP y TCP restan un total de 40 Bytes, por lo que nos que un total de 1460 Bytes para transmitir los datos como se lo detallas en la tabla 3.1.

Tabla 3.1: Formato de trama Ethernet

Cabecera IP	Cabecera TCP	Campo de Datos
20 bytes	20 bytes	1460 bytes

Elaborado por: Autor

Por lo tanto, tendremos un total de 1460 Bytes para transmitir los datos. Por otra parte, cada trama Ethernet tiene una sobrecarga total de 66 Bytes, la cual se detallará en la siguiente tabla 3.2:

Tabla 3.2: Campo de datos de la trama Ethernet

Preámbulo	SOF	MAC destino	MAC origen	Longitud	Cabecera IP	Cabecera TCP	FC S
7	1	6	6	2	20	20	4

Elaborado por: Autor

Entonces la sobrecarga será:

$$\text{Total sobrecarga de la trama} = 7+1+6+6+2+20+20+4$$

$$\text{Total sobrecarga de la trama} = 66 \text{ Bytes}$$

Ahora para poder calcular el ancho de banda primero tendremos que calcular el número de tramas teniendo en cuenta la resolución 640 * 480 (43 Kbytes) en el formato que estamos transmitiendo MPEG, la cual va por medio de 10 imágenes por segundo, que tiene una composición de imagen de 10 Kbits que son las características de la cámara HIKVISION modelo DS-2CD2020F-I (W).

- Calculo número de tramas de la siguiente manera:

$$\text{Numero de tramas} = \text{tamaño de la aplicación / datos útiles de la trama Ethernet:}$$

$$\text{Numero de tramas} = 43 \text{ Kbytes} / 1460 \text{ Kbytes}$$

$$\text{Numero de tramas} = 29,45$$

$$\text{Numero de tramas} = 30$$

- Ahora vamos a determinar la sobrecarga que nos dará el paquete de datos a transmitir la cual la calcularemos de la siguiente manera:

$$\text{Sobrecarga total} = \text{número de tramas} * \text{sobrecarga Ethernet}$$

$$\text{Sobrecarga total} = 30 * 66 \text{ bytes}$$

$$\text{Sobrecarga total} = 1980 \text{ bytes}$$

- Luego calcularemos los datos transmitidos totales (1 imagen):

Datos totales transmitidos = tamaño de la aplicación * sobrecarga total

$$\text{Datos totales transmitidos} = 43 \text{ Kb} * 1,98 \text{ Kb}$$

$$\text{Datos totales transmitidos} = 44,98 \text{ Kbytes} = 359,84 \text{ Kbits}$$

- Después calcularemos el ancho de banda que se requerirá para una cámara:

Ancho de Banda de una cámara =

$$359,84 \text{ Kbits} / 1 \text{ cámara} * 10 \text{ imágenes} / 1 \text{ seg}$$

$$\text{Ancho de Banda de una cámara} = 3,5984 \text{ Mbps}$$

- Finalmente calcularemos el ancho de banda con el número total de cámaras a utilizarse:

Ancho de Banda total = No. cámaras * Ancho de Banda 1 cámara

$$\text{Ancho de Banda total} = 12 * 3,5984 \text{ Mbps}$$

$$\text{Ancho de Banda total} = 43,18 \text{ Mbps}$$

Como se puede apreciar en el cálculo del ancho de banda se necesitara un total de 43,18 Mbps solo para las cámaras IP, como se propuso al inicio del tercer capítulo se recomienda una velocidad a contratar de 50 Mbps, con lo cual abarcaremos en su totalidad lo que se necesita para el correcto funcionamiento de la cámaras IP, por consecuencia nos queda un promedio de 6 Mbps para la red comunitaria, lo cual es suficiente para la navegación ya que el promedio de contratación en un hogar para navegar es aproximadamente entre 4 – 6 Mbps.

3.6. Calculo de la capacidad de almacenamiento para la elección de NVR.

Se debe tener en cuenta algunos factores para que podamos calcular la capacidad de almacenamiento que necesitamos en nuestro NVR los cuales son:

- El número de cámaras
- El número de horas por día en que la cámara estará grabando.
- Tiempo de almacenamiento de los videos.

- Velocidad de imagen, tipo de compresión, calidad de la imagen y complejidad.

En el caso de nuestra red de video vigilancia en la Ciudadela Álamos Norte, se tiene estimado el almacenar las grabaciones de las 12 cámaras por 30 días durante las 24 horas del día, lo que se desea con esto es tener un respaldo de por lo menos un mes de grabación por cualquier evento que pueda ocurrir. Este cálculo se lo realizara para una resolución de 640 x 480 pixeles en el formato MJPEG, a 10 imágenes por segundo y con una compresión de imagen de 10 Kbits que son las características que la cámara Hikvision modelo DS-2CD2020F-I(W). A continuación, realizaremos los cálculos:

- Capacidad de almacenamiento por hora

$$\text{Capacidad / hora} = \text{tamaño de imagen} * \text{imágenes}$$

$$\text{Capacidad / hora} = 10\text{kbits} / \text{imagen} * 10 \text{ imágenes} / 1\text{s} * 3600\text{s} / 1\text{h}$$

$$\text{Capacidad / hora} = 360 \text{ Mb/h}$$

- Capacidad de almacenamiento por día

$$\text{Capacidad / día} = 360 \text{ Mb/h} * 24$$

$$\text{Capacidad / día} = 8640 \text{ Mbps}$$

- Capacidad de almacenamiento por mes (30 días)

$$\text{Capacidad total} = \text{capacidad día} * \text{días de grabación}$$

$$\text{Capacidad total} = 8640 \text{ Mbps} * 30$$

$$\text{Capacidad total} = 259,2 \text{ Gb}$$

- Capacidad de almacenamiento por total de cámaras (12)

$$\text{Capacidad por total de cámaras} = 259,2 \text{ Gb} * 12$$

$$\text{Capacidad por total de cámaras} = 3110,4 \text{ Gb}$$

3.7. Análisis de proveedor de servicio.

Una vez que ya hemos calculado el ancho de banda que se requerirá vamos analizar el proveedor de servicio de internet, para lo cual se tiene en consideración, como proveedores del servicio de internet, a las compañías

Netlife y CNT debido a que brindan el servicio de FTTH (Fiber To The Home), de igual manera por la toda la infraestructura con la que cuentan estas compañías y la cobertura a gran parte de la ciudad, por lo que serían una buena opción para esta tesis.

La velocidad apropiada para que este servicio vaya sin ningún tipo de problema sería de 50 Mbps, con este plan se tendría una velocidad asimétrica con las misma ventajas y velocidad tanto como para bajar y subir tus archivos y así poder tener una buena imagen de las cámaras, debido a que si no se tiene una buena subida de datos perjudicaría a la hora que se desee ver las cámaras desde un ordenador o Smartphone.

Gracias a la tecnología FTTH tecnología de nueva generación que utiliza haces de luz para transmitir datos y comunicación a una gran distancia. Una de sus ventajas es inmune a interferencias electromagnética. Por otra parte, si no se pudiese realizar ya sea por decisión o preferencia de la comunidad con la tecnología FTTH, este proyecto se lo podría realizar con claro o Tv Cable con su tecnología HFC (Hybrid Fiber Coaxial), la que es una tecnología que aun da una buena transmisión de datos. Entre estas 4 compañías con sus diferentes tipos de tecnología se escogería a Netlife por los siguientes puntos:

- Gran infraestructura confiable que garantiza un excelente proyecto.
- Experiencia en la implementación de otros proyectos.
- Cuenta con cobertura de la tecnología FTTH.
- Opera sobre la amplia red de TELCONET.

3.8. Criterio y análisis técnico para la elección de equipos.

Teniendo en claro el área que se requiere cubrir utilizaremos una antena omnidireccional para el internet y unas cámaras IP para la seguridad. Se repartirá el internet comunitario usando una antena omnidireccional y un Bullet que es un equipo el cual podremos configurarlo como un punto de acceso de la compañía Ubiquiti una de las mejores del mercado, esto se decide ya que la antena reparte la señal a unos 360° la cual da una potencia de 15dBi, al tenerla conectada al Bullet podremos administrar la red muy

aparte del router que nos de nuestro proveedor. Las cámaras IP se las escogió ya que por medio de estar las familias podrán entrar a ellas desde cualquier lugar donde se encuentre.

3.8.1. Antena Tp-Link modelo TL-ANT2415D.

En el mercado existen antenas omnidireccionales de todo tipo de diferentes fabricantes tales como TP-Link, Mikrotik, Ubiquiti, etc. En este proyecto se utilizará una antena omnidireccional TP-Link para exterior de 15 dBi a 2,4 GHz modelo TL-ANT2415D, a continuación, en la figura 3.9 se puede observar la antena y en la tabla 3.3 se muestran sus especificaciones técnicas de la misma.

Tabla 3.3: Especificaciones antena TP-Link modelo TL-ANT2415D.

Temperatura de funcionamiento	-40°C~65°C(-40°F~149°F)
Temperatura de almacenamiento	-40°C~80°C (-40°F~176°F)
Humedad de funcionamiento	10%~90% sin condensación
Humedad de almacenamiento	5%~90% sin condensación
Seguridad, emisión y otros	CE, FCC, conforme con la normativa RoHS
Contenidos del paquete	Antena omnidireccional para exterior de 15 dBi Kits de montaje para la instalación Manual de usuario
Dimensiones	1500mm
Temperatura de funcionamiento	-40°C~65°C(-40°F~149°F)
Temperatura de almacenamiento	-40°C~80°C (-40°F~176°F)
Humedad de funcionamiento	10%~90% sin condensación
Humedad de almacenamiento	5%~90% sin condensación
Seguridad, emisión y otros	CE, FCC, conforme con la normativa RoHS
Contenidos del paquete	Antena omnidireccional para exterior de 15 dBi Kits de montaje para la instalación Manual de usuario
Dimensiones	1500mm

Fuente: (TP-Link, 2018)

Elaborado por: Autor



Figura 3.9: Antena omnidireccional TP-Link modelo TL-ANT2415D.
Fuente: (TP-Link, 2018)

3.8.2. POE Ubiquiti.

De igual manera se utilizará un POE (Power Over Ethernet), es una tecnología que a día de hoy podemos encontrar en prácticamente cualquier sitio, con la creciente demanda de las tecnologías Wireless y VoIP. Esta tecnología lo que nos permitirá es que a través del cable de red o Ethernet podamos alimentar nuestro equipo y a su vez transmitir datos sin ninguna clase de inconveniente. Ejemplo de algunos dispositivos de red serían los switches, los puntos de acceso, los routers, los teléfonos o las cámaras IP, etc. En la figura 3.10 se puede observar un equipo POE.



Figura 3.10: POE de Ubiquiti.
Fuente: (Ubiquiti, 2018)

3.8.3. Access point Ubiquiti modelo Bullet M2-HP.

También se utilizará un Bullet M2 el cual va conectado a la antena el cual ira configurado como Access Point, en la figura 3.11 se muestra el equipo y en la tabla 3.4 se puede observar las especificaciones tecinas del equipo.

Tabla 3.4: Especificaciones Bullet M2-HP

BULLET M2-HP	
Procesador	Atheros SOC, MIPS de 24 KC, 400MHz Información
Memoria	8MB SDRAM de 32 MB, Flash
Interfaz de red	1X 10/100 BASE-TX (Cat. 5, RJ-45) Interfaz Ethernet
Certificaciones	FCC Parte 15.247, IC RS210, CE
Cumplimiento de las normas RoHS	Sí
Conector RF	Integrado N-macho tipo Jack (se conecta directamente a la antena)
Método de la energía	Energía pasiva a través de Ethernet (pares de 4,5 +; 7,8 y vuelta)
Temperatura de operación	-40c a + 80c
Dimensiones	15,2 cm. de largo x 3,1 cm. de altura x 3.7 cm. Peso 0.18kg

Fuente: (Hikvision, 2018)

Elaborado por: Autor



Figura 3.11: Bullet M2 Hp para exterior de Ubiquiti

Fuente: (Ubiquiti, 2018)

A continuación, en la figura 3.12 se mostrará un diagrama de la conexión de los equipos antes mencionados, de igual manera se darán los pasos que se realizaron para la configuración de los mismos, para la red de internet comunitaria.

- El cable de alimentación se conecta directamente al inyector POE.
- El Puerto LAN del inyector se conecta al router.
- El puerto POE del Inyector se conecta al puerto Ethernet de Bullet. M2-HP.
- El Bullet va conectada a la antena.

Para esta conexión del Router al puerto LAN del POE y del puerto Ethernet del dispositivo Ubiquiti al puerto Ethernet del adaptador POE se utilizará cable blindado UTP de categoría 6 o superior en todas las conexiones Ethernet, si vamos a colocarlos lejos del adaptador y en el exterior es conveniente utilizar de igual manera UTP categoría 6, y se debe conectar a tierra mediante la toma de tierra de CA del POE, ahora ya podemos colocar nuestra antena en su posición final.

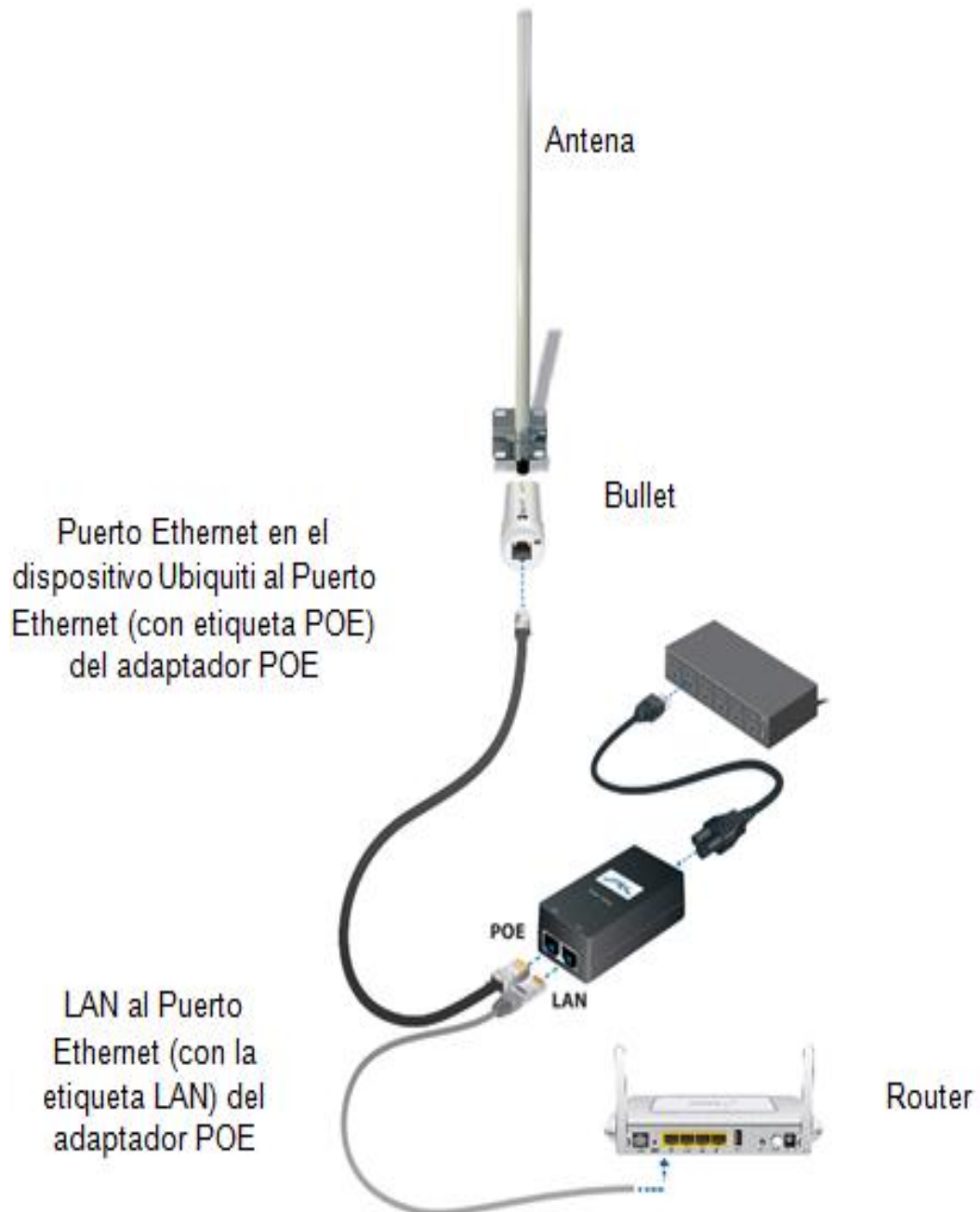


Figura 3.12: Diagrama de la conexión de los equipos.

Fuente: (Ubiquiti, 2018)

Elaborado por: Autor

3.8.4. Cámaras IP Hikvision modelo DS-2CD2020F-I (W).

En cuanto a la elección de las cámaras se utilizarán serán las Hikvision modelo DS-2CD2020F-I (W) en la figura 3.13 se muestra la cámara y en la tabla 3.5 se muestran sus especificaciones técnicas.

Tabla 3.5: Especificaciones cámara IP DS-2CD2020F-I (W).

Cámara IP	
Sensor de imagen:	1/2.8" barrido progresivo CMOS
Resolución:	3MP
Video	Tiempo real
Compresión de video	MJPEG
Cuadros por segundo	30 Hz: 10 fps (640 x 480), 50 Hz: 25 fps (1920 x 1080), 25 fps (1280 x 960), 25 fps (1280 x 720)
Protección	IP67
POE	Integrado
Min. Iluminación:	0.01Lux@ (F1.2, AGC ON), 0 Lux con IR 0.028Lux@ (F2.0, AGC ON), 0 Lux con IR
Tiempo de obturación:	1/3 s a 1/100,000 s
Lente:	4 mm @ F2.0, ángulo de visión: 85 ° (6 mm opcional)
Montura del lente:	M12
Día y noche:	Filtro de corte IR con detector magnético
Amplio rango dinámico:	WDR digital
Reducción de ruido digital:	3D DNR
Protocolo	TCP / IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPNP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv6

Fuente: (Hikvision, 2018)

Elaborado por: Autor



Figura 3.13: Cámara IP Hikvision modelo DS-2CD2020F-I (W).

Fuente: (Hikvision, 2018)

Se toma la decisión de utilizar esta cámara del fabricante (Hikvision, 2018), debido a su experiencia en el mercado fabricando todo tipo de cámaras y por su gran producto final, técnicamente este producto nos ayudara mucho ya que se necesitará que sea resistente ya que estarán a expuestas al sol, la lluvia, viento, etc. La protección IP67 con la que cuenta esta cámara es una de las mejores, por otro lado, la resolución de 3MP nos dará una gran visión de la ciudadela, también el tiempo sería casi real tan solo se tendría un retraso de 1/3s.

También por los protocolos que soporta y el resto de especificaciones ya mencionadas hace que sea el equipo ideal para este proyecto. La velocidad que nos permite transmitir también es una ventaja a la hora que queramos ver las cámaras en vivo, así mismo el soporte a la mayoría de los protocolos establecidos por la IEEE es un gran punto a favor ya que se podrán conectarlos equipos sin ningún tipo de problema.

3.8.5. NVR Hikvision modelo DS-7600NI-I2 / 16P.

Un elemento esencial para este proyecto será el NVR (Network Video Recorder), es fundamental que el equipo sea de los mejores ya que tendrá guardado todo lo que las cámaras graben. Por lo que se decide utilizar el modelo DS-7600NI-I2 / 16P de la marca Hikvision en la figura 3.14 se muestra el equipo y en la tabla 3.6 se pueden observar las especificaciones técnicas.



Figura 3.14: NVR de la marca Hikvision modelo DS-7600NI-I2 / 16P
Fuente: (Hikvision, 2018)

Tabla 3.6: Especificaciones NVR DS-7600NI-I2/16P

NVR	
Entrada de Video IP	16-ch
Entrada de Audio de dos vías	1-ch, RCA
Ancho de banda entrada	160 Mbps
Ancho de banda salida	256 Mbps
Salida de video	HDMI
Resolución de grabación:	12MP / 8MP / 6MP / 5MP / 4MP / 3MP / 1080p / UXGA / 720p / VGA / 4CIF / DCIF / 2CIF / CIF / QCIF
Disco duro SATA	2 interfaces SATA para 2 discos duros
Capacidad	Hasta 6 TB de capacidad para cada HDD
Interfaz POE	16 interfaces Ethernet POE independientes a 10/100 Mbps
Max poder	200W
Temperatura trabajo	-10 °C ~ +55 °C (+14 °F ~ + 131 °F)
Humedad de trabajo:	10 % ~ 90 %

Fuente: (Hikvision, 2018)

Elaborado por: Autor

Este equipo nos brinda la posibilidad desconectar las cámaras sin la necesidad de utilizar un equipo extra (POE, Fuente de alimentación, etc.), entonces con este NVR tendremos conectadas todas las cámaras a la red y a la energía por medio de sus 16 puertos POE, los puertos nos permitirá nos ahorra cableado para alimentación, sí no se usará este equipo se tendría que buscar la manera de conectar a la energía lo cual sería un problema ya que tendremos las cámaras en el exterior.

La resolución de las cámaras se complementa muy bien con la salida de video de Interfaz Multimedia de Alta Definición (High-Definition Multimedia Interface, HDMI) del equipo ya que ayuda mucho a la calidad de imagen y poder apreciar mejor el video. Los 6 TB con los que se cuentan son suficiente para tener grabado más de un mes sin problemas ya que aproximadamente se ocupa 121Gb para tener un mes de grabación por cámara esto también dependerá de la resolución en la que se guarden los

videos. A continuación, en la figura 3.15 se muestra cómo queda la conexión de los equipos al NVR:

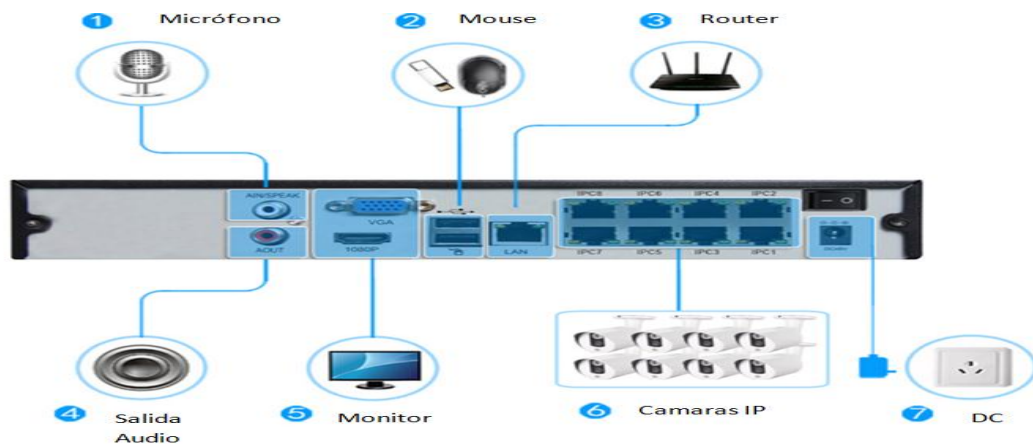


Figura 3.15: Conexión de equipos al NVR modelo DS-7600NI-I2 / 16P

Fuente:(Hikvision, 2018)

Elaborado por: Autor

3.9. Configuración de parámetros del Bullet M2-HP.

Para poder acceder a la configuración de este **Bullet** lo primero que se hace es a través del navegador, ingresamos poniendo la IP por defecto **192.168.1.20**, luego lo primero que nos pide será usuario y contraseña para poder ingresar a la configuración del equipo, entonces podremos lo siguiente:

Usuario: ubnt

Contraseña: ubnt

Una vez iniciamos sesión tendremos la interfaz completa para poder configurar el equipo como se desee en este caso lo usaremos como un punto de access point acoplado con una antena omnidireccional de 15 dbi entre otro parámetro, en la figura 3.16 se muestra la pantalla en la cual estableceremos los parámetros de este equipo, los pasos a seguir para la configuración serán de la siguiente manera:

- En modo inalámbrico seleccionamos que es como tendremos nuestro equipo Punto de Acceso.
- En SSID, ponemos el nombre de la red inalámbrica que queremos crear.

- En el ancho de canal, vamos a seleccionar 20MHz lo máximo permitido en lugares donde existen otras redes WI-FI y así evitar problemas.
- Frecuencia, aquí se escogerá un canal que no esté saturado de redes, este caso está el canal 8, a 2 447MHz.
- Ganancia de la Antena, en este caso es de 15 dBi.
- El resto de parámetros los dejamos en su estado por defecto.

BULLET M2 TITANIUM **airOS™**

MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM Herramientas: Cerrar sesión

Configuración Inalámbrica Básica

Modo inalámbrico:

WDS (Modo Puente Transparente): Habilitar

SSID: Ocultar SSID

Código de País:

Modo IEEE 802.11:

Ancho del canal:

Movimiento de canal:

Frecuencia, MHz:

Extensión de Canal:

Lista de Frecuencias, MHz: Habilitar

Ajustar automáticamente el límite de EIRP: Habilitar

Ganancia de la Antena: dBi Pérdida del cable: dB

Potencia de salida: dBm

Data Rate Module:

Máxima Tasa de Transmisión (Tx), Mbps: Automático

Figura 3.16: Configuración del Bullet M2-HP interfaz WIRELESS
Elaborado por: Autor

Pasamos a la seguridad de nuestra red, seleccionamos nuestro tipo de seguridad WPA, WEP etc. Y escribimos nuestra clave que se desee, este dispositivo también permite el filtrado MAC, pero lo haremos por WPA2, en la figura 3.17 veremos la interfaz de seguridad del equipo. Por último, pulsamos Cambiar, aplicamos los cambios y de esta manera tendremos la configuración de nuestro Bullet como un punto de acceso.

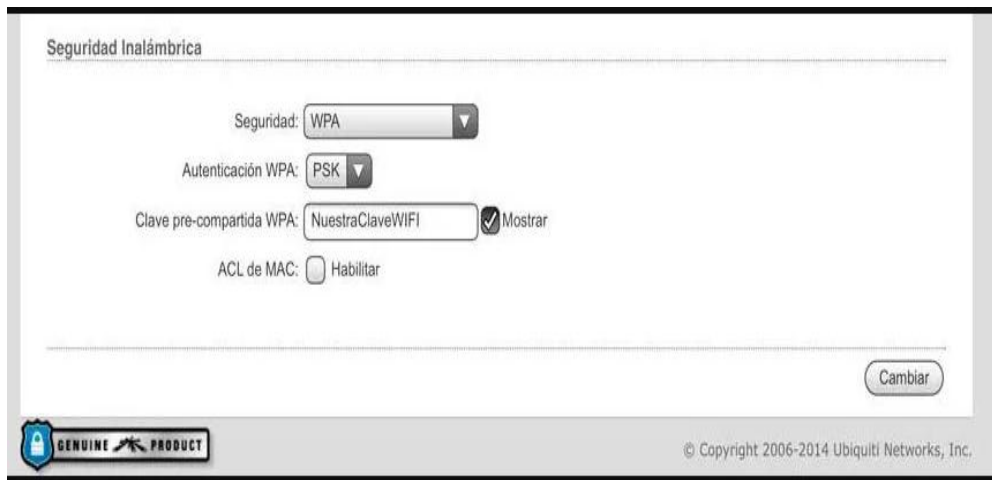


Figura 3.17: Interfaz de seguridad del Bullet M2-HP
Elaborado por: Autor

3.10. Configuración de NVR con las cámaras IP.

Lo primero que haremos será tener conectado el equipo a un monitor y al router del proveedor, una vez que ya cargué el equipo tendremos que designar un usuario y una contraseña para el equipo como se ve en la figura 3.18 y le damos a siguiente.

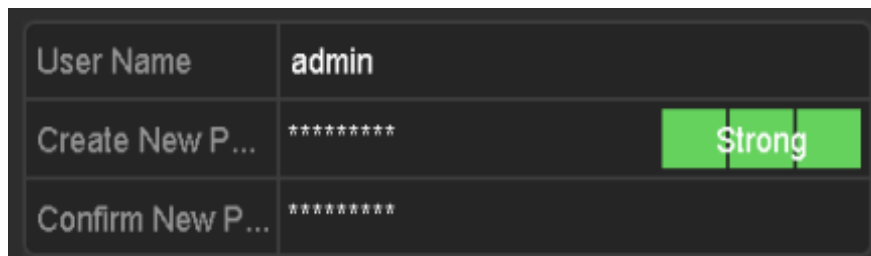


Figura 3.18: Ingreso de clave para NVR.
Elaborado por: Autor

Luego tendremos una interfaz por la cual se habilitará el acceso a las cámaras por medio de la App de Hikvision como se ve en la imagen, ya estando habilitado le damos a siguiente.

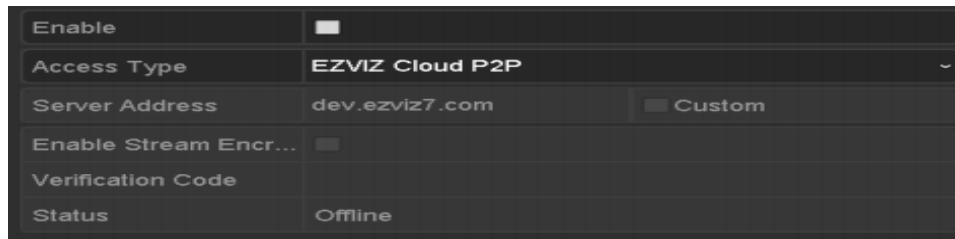


Figura 3.19: Habilitación del monitoreo por App.
Elaborado por: Autor

Después nos saldrán algunas interfaces como idioma, también información sobre el equipo entre otras, después de esas interfaces saldrá la de poder determinar si se desea que el equipo grave de forma continua o por detección de movimiento como se ve en la figura 3.20, este caso como se pondrá en continua y aceptar:

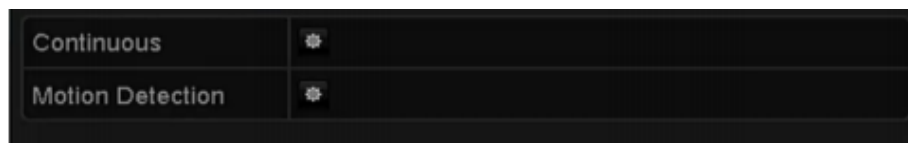


Figura 3.20: Grabación entre continua o por detección de movimiento.
Elaborado por: Autor

Esos son los primeros parámetros a configurar, ahora que ya se ingresó al equipo buscaremos los ajustes y escogeremos la opción configuración de sistema y se dejará establecido como se muestra en la figura 3.21, estos serán los parámetros como quedará el NRV vinculado a la red de internet.

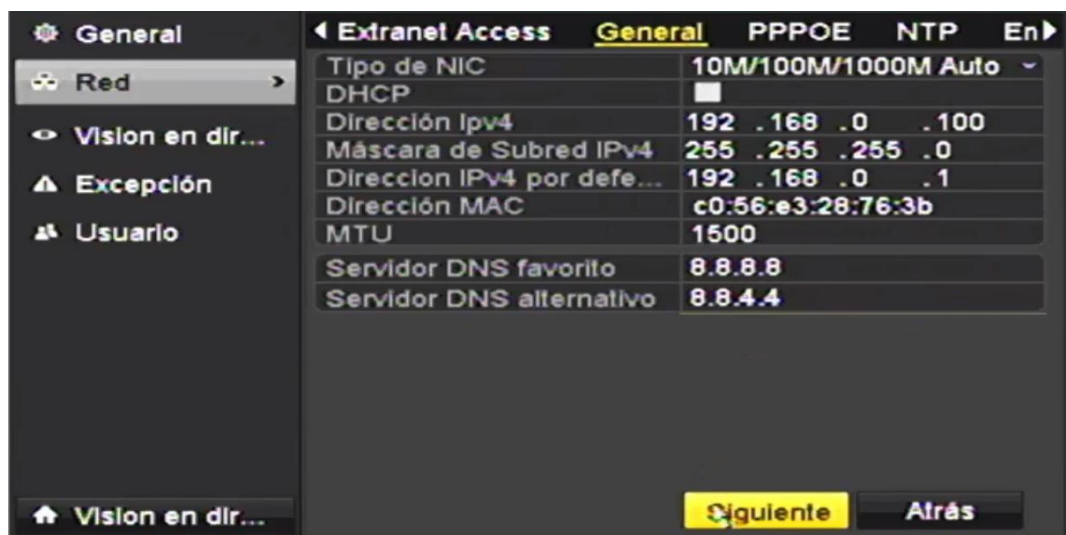


Figura 3.21: Configuración de parámetros del NVR.
Elaborado por: Autor


Luego procederemos a configurar las camaras agregandolas una a una, dandole click en el simbolo + de color verde , como se ve en la figura 3.22.



Figura 3.22: Configuración de cámara IP.
Elaborado por: Autor

Después nos aparecerá la interfaz de la cámara como se ve en la figura 3.23, en la cual le cambiaremos simplemente la dirección IP la cual sería 192.168.0.10, de esta forma estará vinculada a la misma de red.

IP Camera Address	10.9.6.7
Protocol	HIKVISION
Management Port	8000
Transfer Protocol	Auto
User Name	admin
Admin Password	
<input checked="" type="checkbox"/> Continue to Add	

Figura 3.23: Establecimiento de parámetros de cámaras IP.
Elaborado por: Autor

Una vez configurada la primera cámara se procederá con las 11 faltantes y lo único que se pondrá será la misma dirección IP de la anterior pero variando el último número como se muestra en la tabla 3.7. a continuación:

Tabla 3.7: Direcciones IP de cada cámara IP.

Dirección IP	Número de cámara IP
192.168.0.11	2
192.168.0.12	3
192.168.0.13	4
192.168.0.14	5
192.168.0.15	6
192.168.0.16	7
192.168.0.17	8
192.168.0.18	9
192.168.0.19	10
192.168.0.20	11
192.168.0.21	12

Elaborado por: Auto

Una vez que ya configuramos todos estos parámetros ya podremos visualizar las cámaras sin ningún problema como se ve en la figura 3.24, la cantidad de visualización de cámaras a la vez ya dependerá de la persona que este monitoreando.



Figura 3.24: Visualización de cámaras en el NVR.

Fuente: Autor

3.11. Esquema de equipos a implementar para abarcar el área total.

Teniendo en cuenta lo observado en el sitio para tener una cobertura todas se pondrán los equipos en lugares estratégico y poder tener cubierta toda la ciudadela de la red comunitaria mediante tecnología WI-FI y un sistema de video vigilancia IP.

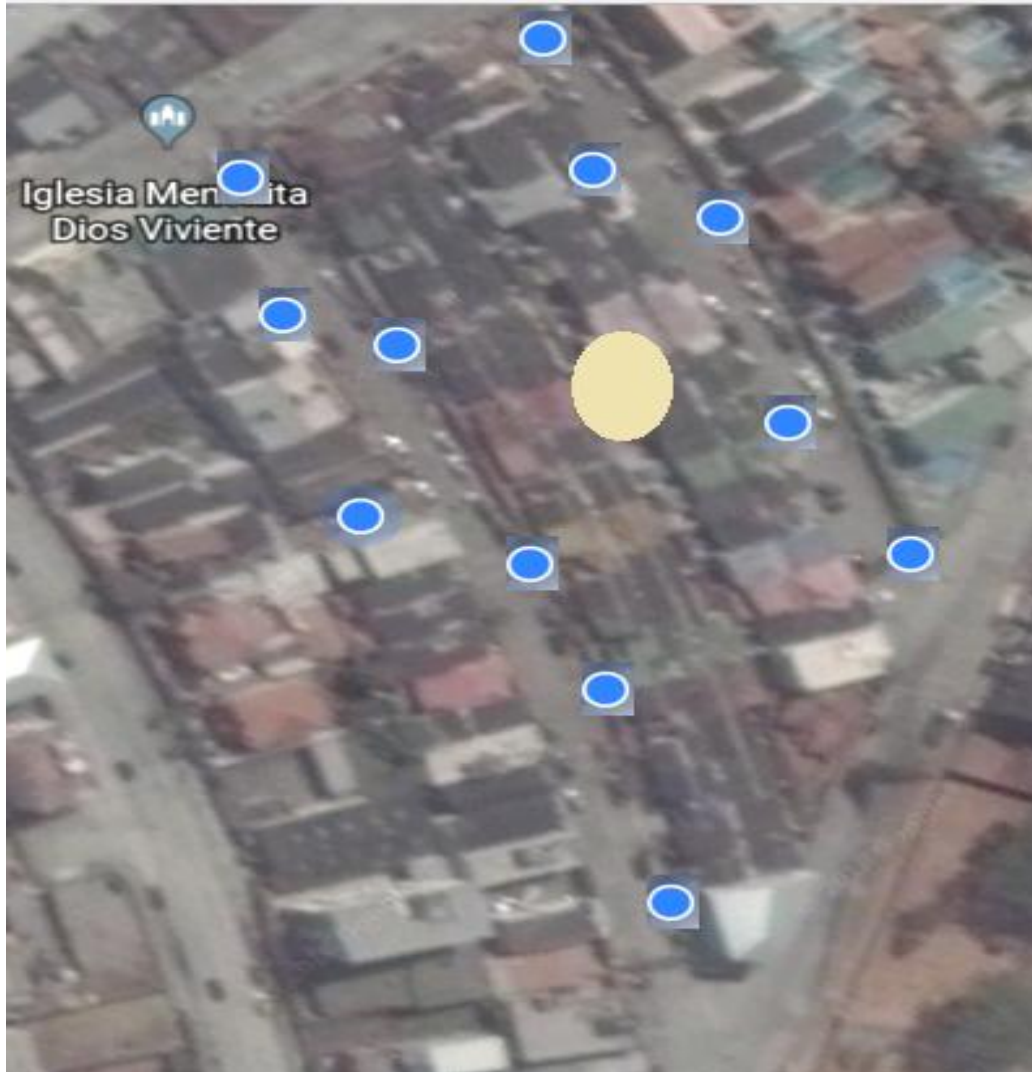




Figura 3.25: Ubicación estratégica de equipos.
Elaborado por: Autor

En la figura 3.25 se mostrará el esquema de cómo estarán ubicados los equipos, nos daremos cuenta de que para cubrir el área del sitio usaremos un total de 12 cámara IP, lo está representado por , por otro lado con la antena representada por , siendo ubicada en la parte central del área a cubrir, se podrá tener una cobertura total con la señal del internet comunitario.

Nos podemos dar cuenta en la figura 3.26 la cobertura que tendrá nuestra red teniendo en cuenta que el radio es el alcance que se tiene con la antena Tp-Link TL-ANT2415D, que en promedio rinde un alcance de máximo 800 m – 1000 m, para poder demostrar su cobertura se tomó como referencia un alcance aproximado a los 160 m, si tomamos como referencia este radio de esta circunferencia trazada nos daremos cuenta que el área a cubrir será de un aproximado de 80,204.91 m².

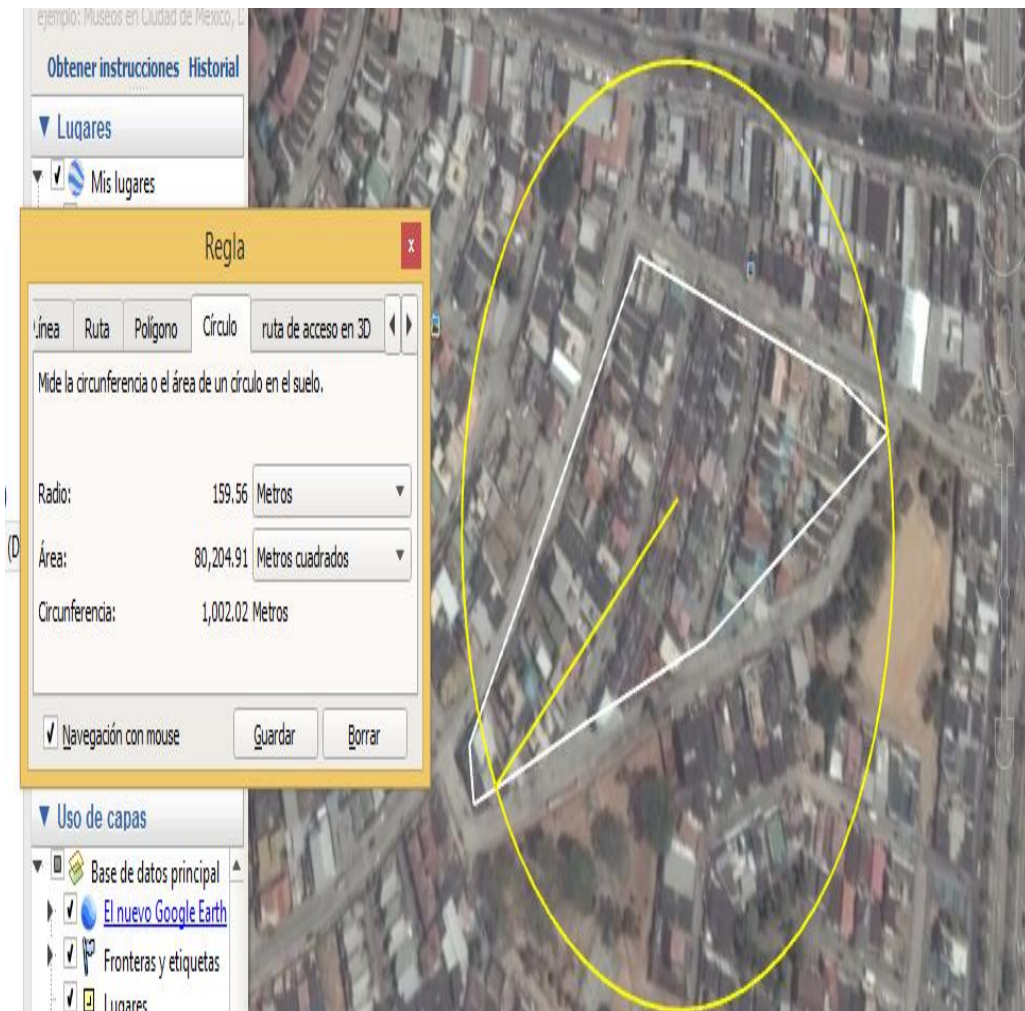


Figura 3.26: Cobertura total del área
Elaborado por: Autor

3.12. Diseño final de la Red comunitaria con camaras IP.

A continuación, en la figura 3.27 se puede observar el diseño final del sistema de video vigilancia IP con la red comunitaria de internet que se requiere para este proyecto, en la ciudadela Álamos Norte de Guayaquil.

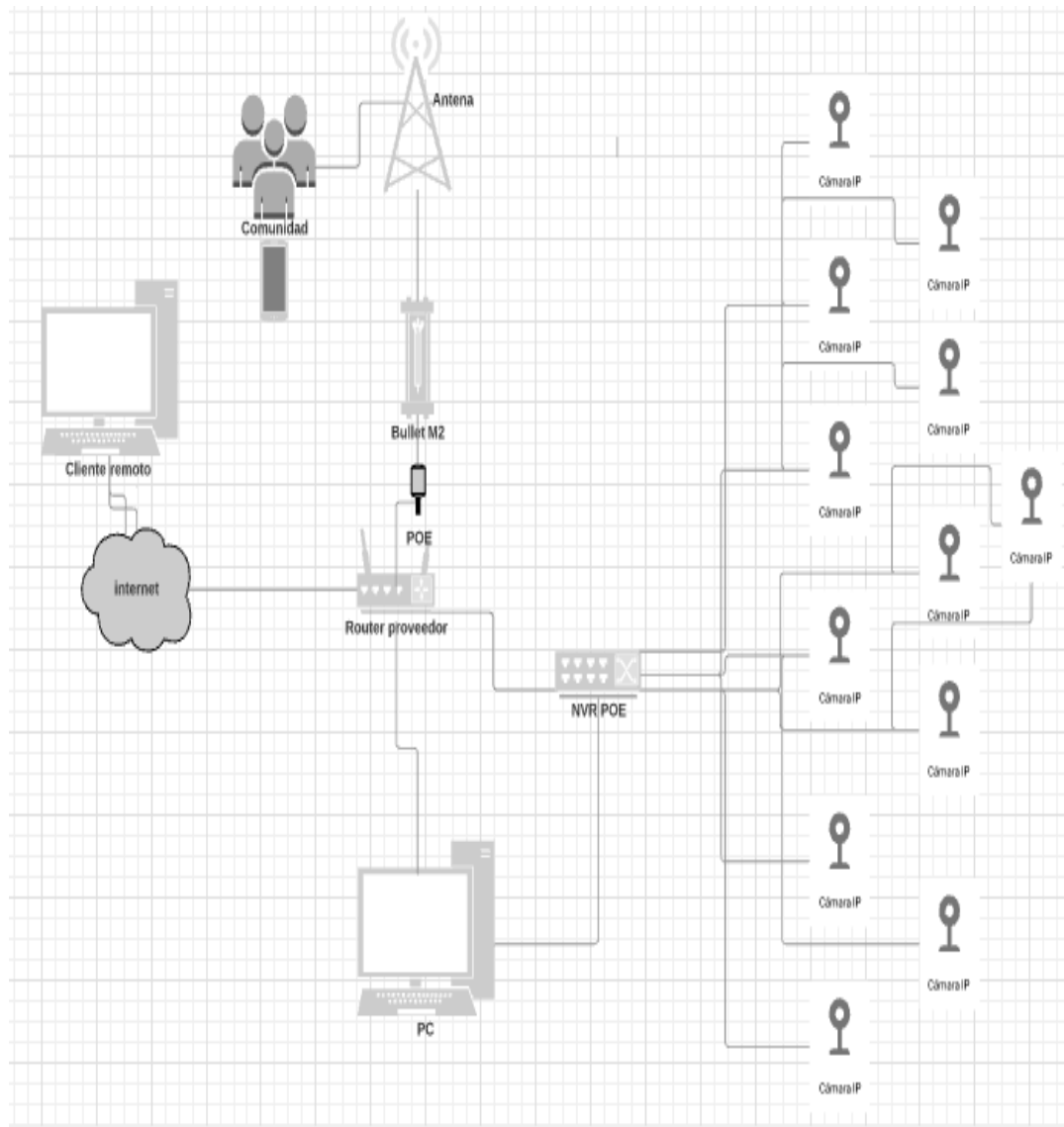


Figura 3.27: Diseño final de la Red comunitaria con cámaras IP
Elaborado por: Autor

En este esquema se muestra cómo queda finalmente todos los equipos implantados en este diseño para la red de internet comunitaria se pone un solo access point que el Bullet M2 complementado con una antena TP-link de 15dBm que trabaja en doble banda 2,4 Ghz y 5 Ghz los cuales se apegan a los protocolos 802.1 y son compatible con todos los aparatos electrónicos que hay en la actualidad. Así mismo cubrimos la ciudadela con la red de internet completamente ya que se pondrán los equipos en una parte estratégica (centro de la ciudadela), con lo que ganaremos cobertura con nuestra antena omnidireccional cubriremos 360°. En la parte de las cámaras se utilizará un total de 12 cámaras IP dos que estarán situadas en la entrada

y salida de la ciudadela, en la parte que resta usaremos 10 cámaras más con lo que cubriremos el total de la ciudadela, y como se mencionó antes el NVR nos ayudara a tener guardado toda la información con el total de 6Tb.

3.13. Aplicaciones para monitorear las cámaras online

Para tener un buen monitoreo de las cámaras desde cualquier parte usaremos la aplicación de Hikvision llamada IVMS-4500, la cual nos permitirá ver las cámaras en tiempo real desde cualquier dispositivo tales como Smartphone, tablet, PC, etc. Esta aplicación es totalmente compatible con todos los sistemas operativos ya sean ANDROID o IOS, para Android la encontraremos en PLAY STORE y para IOS en APP STORE, esta aplicación es gratis y la. Proporciona la misma empresa Hikvision para todos los usuarios que desean tener sus productos.

3.14. Procedimiento en caso de un robo.

En el caso que llegase a ocurrir un evento ya sea un robo, un accidente, etc. Se tiene que dar a conocer a las autoridades del suceso. También comunicar a la comunidad en general del percance. Las acciones principales a tomar se podrían resumir en tres.

La primera acción a tomar sería que el guardia se contacte con el UPC (Unidad de Policía Comunitaria) más cercano con el fin de comunicar sobre el evento ocurrido para que brinden su apoyo en el ámbito que les corresponde. En el caso de no poder comunicarse con el UPC debería llamar al 911 para que comunique al patrullero más cercano y se acerque lo más rápido a la ciudadela. En caso de accidente el 911 también brinda el servicio de ambulancia para asistir a los heridos. Actualmente hay un método en el cual se está coordinado con el UPC más cerca por medio del teléfono móvil marcado un solo número la llamada será directa al policía que este de turno.

La segunda acción a tomar por parte del guardia es alertar a la comunidad en este caso la Ciudadela Álamos Norte para que estén atentos a cualquier otro evento que pueda sucintarse. Una vez ya informadas las

familias se pueden comunicar por medio de WhatsApp o correos entre ellos por medio de la Red Comunitaria previamente instaladas. Así mismo puedan ingresar a las cámaras y darse cuenta de lo que está ocurriendo en la comunidad.

Por último, en el caso de que no se llegase a atrapar a los ladrones, hay que tener lista toda la información (Video), para que las autoridades puedan tomar las medidas necesarias y dar con el paradero de los responsables de los actos delincuenciales.

3.15. Costo aproximando de equipos a utilizarse.

Este tipo de proyecto saben ser financiados por empresas privadas o públicas que son las que tienen un gran capital, pero es este proyecto se trató de que pueda ser financiado por una comunidad que este preocupada por sus familias, por lo que se usaron quipos un poco costosos pero que van a dar las garantías de operación y durabilidad. A continuación, se mostrará una tabla de equipos con los materiales y los costos aproximados para su implementación.

Tabla 3.8: Costos aproximado de equipos para el proyecto

Cantidad	Descripción	Precio Unitario	Precio Total
1	Antena Omnidireccional TP-Link TL-ANT2415D	\$ 210.00	\$210.00
1	Bullet M2	\$75.00	\$75.00
1	POE	\$25.00	\$25.00
12	Cámara IP Hikvision DS-2CD2020F-I	\$50.00	\$600.00
1	NVR Hikvision DS-7600NI-I2	\$450.00	\$450.00
2	Rollo cables UTP categoría 6 (305mtrs)	\$250.00	\$500.00
30	Conectores tipo UTP categoría 6	\$0.25	\$7.50
1	Instalación proveedor de internet	\$100.00	\$100.00
1	Instalación red comunitaria	\$200.00	\$200.00
12	Servicio Instalación por punto de cámara	\$600.00	\$600.00
	TOTAL		\$2767.50

Elaborado por: Autor

Los costos serán asumidos por los moradores de las manzanas 18 y 19 de los Álamos, cuyas familias ascienden a 37, por el lapso de dos meses de la siguiente manera:

$$\text{\$ } 2767.50 / 37 \text{ Familias} = \text{\$ } 74.80$$

$$\text{Cuota 1} = \text{\$ } 37.40$$

$$\text{Cuota 2} = \text{\$ } 37.40$$

Dicho costo aumenta en \$ 17.40 dólares a su cuota mensual de \$20.00 dólares que están acostumbrado los moradores del sector a costear por concepto de guardianía. Luego de dos meses de recaudar dicho valor se procede a ejecutar la instalación del proyecto.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES.

4.1. Conclusiones.

- La ciudadela Los Álamos ha implementado diferentes alternativas para resolver el problema de la inseguridad en el sector, contratando seguridad privada y la implementación de una puerta eléctrica que permita controlar la entrada de los moradores, sin embargo, en las afueras de la ciudadela los actos delictivos no han disminuido y la poca efectividad del llamado a la Unidad Policial Comunitaria UPC, no han resuelto el problema.
- Una red WI-FI da niveles de señal de mayor alcance, pero con este sistema que se está proponiéndose tendrá una cobertura más significativa. Una red comunitaria de internet con los equipos Bullet M2 y TL-ANT2415D, tiene un rendimiento garantizado con una gran cobertura con lo que podrá brindarse el servicio sin ningún tipo de inconveniente.
- Con el equipo de alimentación inteligente como el POE se puede alimentar y enviar sin ningún tipo de fuente de alimentación al Bullet y a la antena. Al usar un total de 12 cámaras IP se llega a cubrir en su totalidad el área que se desea para poderle brindar seguridad a la comunidad de los Álamos Norte.
- Se deduce que el equipo DS-7600NI-I2 es el equipo idóneo por todas sus características ya que lo más importante es su capacidad para almacenar información.
- En cuanto al financiamiento del proyecto, se determina que su costo será asumido por los moradores del sector, en específico 37 familias, cuya aportación será de \$ 37.40 en dos pagos, valor que no altera en gran magnitud su presupuesto familiar, porque mensualmente ellos destinan \$20.00 para el tema de la seguridad.

4.2. Recomendaciones.

- Realizar el proyecto con una sola empresa que ofrezca el servicio tanto de internet como de seguridad para que haya equilibrio en el costo beneficio.

- Considerar la cantidad de familias que hay en la comunidad que se vaya a implementar este proyecto para poder aumentar o disminuir el número de equipos, decir replantear el proyecto, actualmente es de 37 familias, sin embargo, su grado de efectividad en cuanto a la atención de problemas delictivos puede ser el factor persuasivo para que más integrantes se unan al proyecto.

- Las autoridades fomenten a través de cursos el múltiple uso que se le puede dar al internet. Orientado a la seguridad mediante uso cámaras IP a través del internet. Además, que el sistema esté integrado a un software del UPC más cercano y de computadores que manejen la seguridad privada, de manera que el grado de respuesta inmediato del sistema, sea un factor decisivo a la captura de estos malos ciudadanos.

REFERENCIAS BIBLIOGRÁFICAS.

ACENS. (2012). Sistemas de seguridad en redes inalámbricas: WEP, WAP y WAP2. Recuperado 23 de febrero de 2018, a partir de <https://www.acens.com/wp-content/images/whitepaper-redes-seguridad-acens-julio-2012>

Camargo, J. (2014). *Modelo de cobertura para redes inalámbricas de interiores*. Escuela Superior de Ingenieros de Sevilla, Sevilla, España.

CEDATOS. (2011). La Inseguridad en el Ecuador. Obtenido de http://www.cedatos.com.ec/detalles_noticia.php?id=86

Encyclopædia Britannica. (2013). Telecommunications media. Recuperado 5 de enero de 2018, a partir de <https://global.britannica.com/topic/telecommunications-media>

Ferrando, M. (2014). *Parametros de Antenas* (p. 50). Valencia, España.: Universidad Politécnica de Valencia.

Flickenger, R. (2013). *Redes Inalámbricas en los Países en Desarrollo*.

Londres, Inglaterra: Limehouse Book Sprint Team.

Garreta, J. (2017). Historia y evolución de las redes WiFi: De tecnología inalámbrica a Aplicación ligera para retailers. Recuperado 8 de enero de 2018, a partir de <http://pleasenetworks.com/blog/post/13/historia-y-evolucion-de-las-redes-wifi-de-tecnologa-inalmbrica-a-aplicacin-ligera-para-retailers>

Grupo TCR. (2016). Cámaras IP, Ventajas Desventajas Aplicaciones. Recuperado 23 de febrero de 2018, a partir de <http://www.trc.es/Index.aspx>

- Hernández, J. (2012). *Antenas: Principios básicos, análisis y diseño*. UABC.
- Hikvision. (2018). DS-2CD201RF-I(W) - Hangzhou Hikvision Digital Technology Co. Ltd. Recuperado 23 de febrero de 2018, a partir de http://www.hikvision.com/es/Products_accessories_157_i37447.html
- Huidobro, J. (2013). Antenas de telecomunicaciones, *Acta* (15), 10.
- INEC. (2011). Ecuador en cifras: Inseguridad. Quito: Fascículo de la Provincia del Guayas.
- Instituto Federal de Telecomunicaciones. (2015). Glosario | Instituto Federal de Telecomunicaciones - IFT. Recuperado 6 de enero de 2018, a partir de <http://www.ift.org.mx/que-es-el-ift/glosario>
- Orange. (2016). ¿qué es una onda? Recuperado 6 de enero de 2018, a partir de <http://www.ondes-radio.orange.com/es/acerca-de-las-ondas/que-es-una-onda>
- Ramirez, J. (2008). *Las redes inalámbricas, más ventajas que desventajas*. (p. 18). Veracruz, Mexico: Universidad Veracruzana.
- Regalado, N. (2013). Introducción a las Telecomunicaciones.pdf. Recuperado 6 de enero de 2018, a partir de <https://es.scribd.com/doc/242629855/Libro-telecomunicaciones-completo-pdf>
- Romero, W. (2012). *Redes inalámbricas y simulación de WLAN mediante OPNET*. Universidad Oberta de Cataluña, Barcelona, España.
- sancegroup. (2017). NVR/DVR systems VS stand-alonewireless IP cameras. Recuperado 14 de febrero de 2018, a partir de <http://www.sancegroup.com/2017/06/nvr-dvr-systems-vs-stand-alone-wireless-ip-cameras.html>

TP-Link. (2018). TL-ANT2415D | 2.4GHz 15dBi antena omnidireccional para exteriores | TP-Link Ecuador. Recuperado 23 de febrero de 2018, a partir de https://www.tp-link.com/ec/products/details/cat-5691_TL-ANT2415D.html

Ubiquiti. (2018). Ubiquiti Networks - Bullet™ M. Recuperado 23 de febrero de 2018, a partir de <https://www.ubnt.com/airmax/bulletm/>

Villagomez, C. (2008). WiFi - Redes inalámbricas y seguridad. Recuperado 3 de enero de 2018, a partir de <http://es.ccm.net/faq/1160-wifi-redes-inalambricas-y-seguridad>

Weston, F., & Lewis, A. (2005). Física Universitaria, volumen 2. Madrid: Pearson Educación.

Yunquera, J. (2014). *Proyecto técnico despliegue de red inalámbrica para la Escuela Superior de Ingenieros de Sevilla*. Escuela Superior de Ingenieros de Sevilla, Sevilla, España.



DECLARACIÓN Y AUTORIZACIÓN

Yo, **Moncayo Quispe, Victor Emilio** con C.C: # 0928773746 Trabajo de Titulación: **DISEÑO TÉCNICO – ECONÓMICO DE UN SISTEMA DE VIDEO VIGILANCIA IP, MEDIANTE EL USO DE UNA RED DE INTERNET COMUNITARIA QUE UTILIZA TECNOLOGÍA DE ACCESO WI-FI EN LA CIUDADELA ÁLAMOS NORTE DE GUAYAQUIL** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 7 de marzo de 2018

f. _____

Nombre: Moncayo Quispe, Victor Emilio

C.C: 0928773746



Presidencia
de la República
del Ecuador



Plan Nacional
de Ciencia, Tecnología,
Innovación y Saberes



SENESCYT
Secretaría Nacional de Educación Superior,
Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Diseño técnico – económico de un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza tecnología de acceso WI-FI en la ciudadela Álamos Norte de Guayaquil.		
AUTOR(ES)	MONCAYO QUISPE, VICTOR EMILIO		
REVISOR(ES)/TUTOR(ES)	ALVARADO BUSTAMANTE, JIMMY SALVADOR		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TÍTULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	7 de Marzo de 2018	No. DE PÁGINAS:	81
ÁREAS TEMÁTICAS:	Sistemas de Comunicación, Informática y Comunicaciones Inalámbricas		
PALABRAS CLAVES/ KEYWORDS:	WI-FI, Red, Comunitaria, Inalámbrica, Video Vigilancia, IP.		
RESUMEN/ABSTRACT (150-250 palabras):	<p>La inseguridad en la ciudad de Guayaquil es una realidad que se vive el sector de Los Álamos, entre los delitos que destacan están robos, asaltos y asesinatos, siendo un tema de preocupación para la población, demandando un sistema de aviso efectivo en caso de que se produce el delito, capturando a los causantes y con ello bajar el índice delictivo en la zona. Este trabajo de titulación tiene el objetivo principal de diseñar un sistema de video vigilancia IP, mediante el uso de una red de internet comunitaria que utiliza la tecnología de acceso WI-FI para que la comunidad se sienta más segura en sus hogares y por medio de la red de internet este más comunicados, se abordaran temas como las redes inalámbricas, seguridad de las redes, cámara IP, equipos de almacenamiento, comparaciones, topología de redes y antenas. En este proyecto se decidió utilizar doce cámaras IP para monitoreo, una antena TP-Link con un equipo Bullet M2-HP el cual será nuestro punto de acceso una vez configurado, usaremos una red con un ancho de banda de 50 Mbps para que a su vez tenga la capacidad de soportar las cámaras IP a usar, el costo de la propuesta es asumido por los moradores del sector con una cuota por dos meses de \$ 37.40 con una participación de 37 familias.</p>		
ADJUNTO PDF:	<input checked="" type="checkbox"/>	<input type="checkbox"/> NO	
CONTACTO CON AUTOR/ES:	Teléfono: +593-4-2126104 +593-9-89490901	E-mail: victor.94.a@outlook.com	
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	Nombre: Palacios Meléndez Edwin Fernando		
	Teléfono: +593-9-68366762		
	E-mail: edwin.palacios@cu.ucsg.edu.ec		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			